Descripción

Esta máquina es ideal para personas que están empezando en el mundo del hacking o personas que buscan practicar para la certificación eJPTv2.

Herramientas que emplearemos en esta máquina

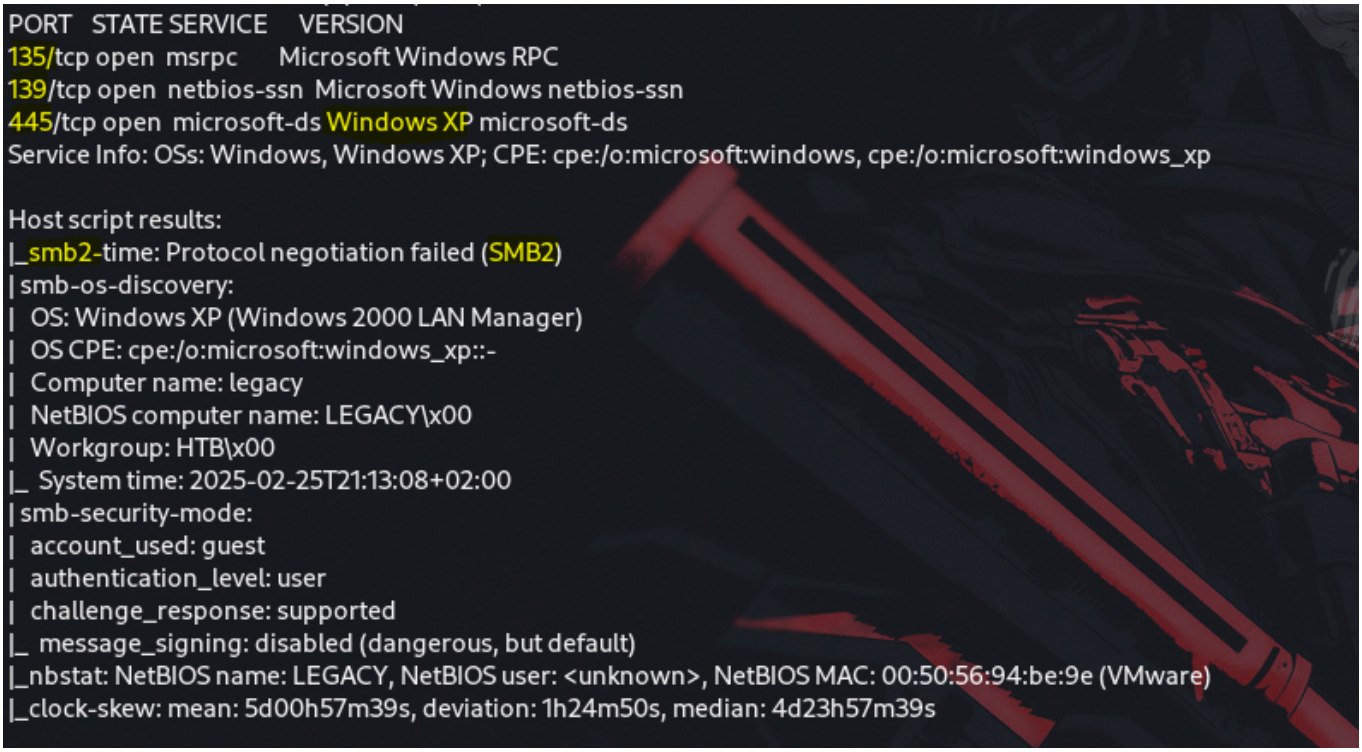
- NMAP Y NMAP SCRIPTS
- METASPLOIT

Enumeración

Vamos a realizar un escaneo de puertos para ver los servicios que están activos en la máquina víctima

```
sudo nmap -p- --min-rate 5000 -sCV 10.10.10.4 -oN Legacy
```

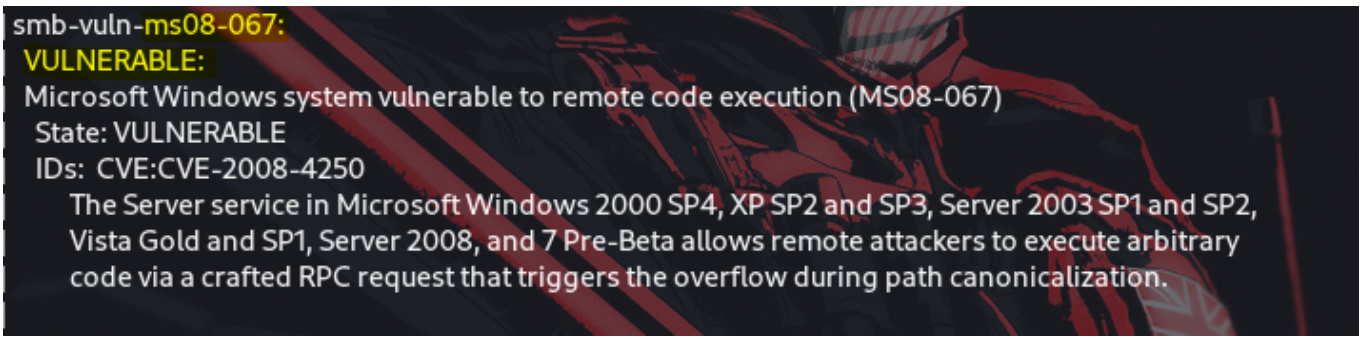
Resultados del escaneo



En este escaneo podremos ver 3 puertos abiertos pero vamos a fijarnos en el **445** que tiene el servicio **smb** activo

Vamos a ejecutar el siguiente script de NMAP para enumerar posibles vulnerabilidades de **SMB**

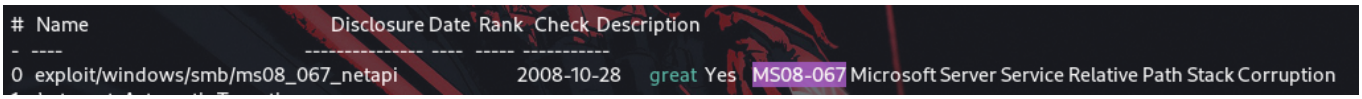
```
sudo nmap --script=smb-vuln* 10.10.10.4
```



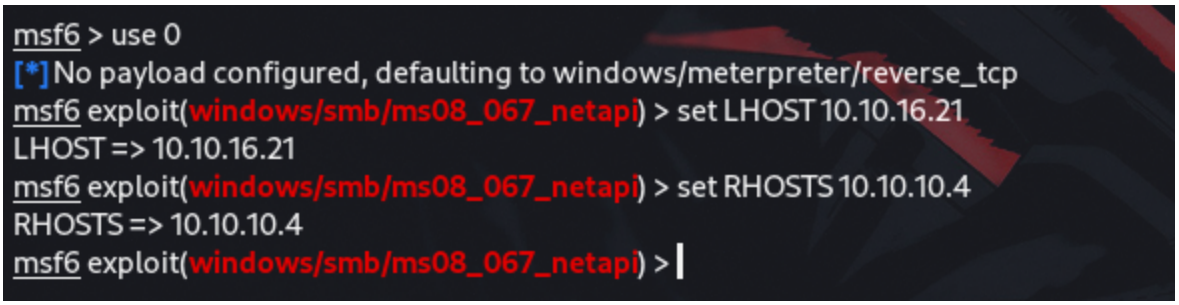
Podemos ver que estamos ante la vulnerabilidad **ms08-067**

Explotación

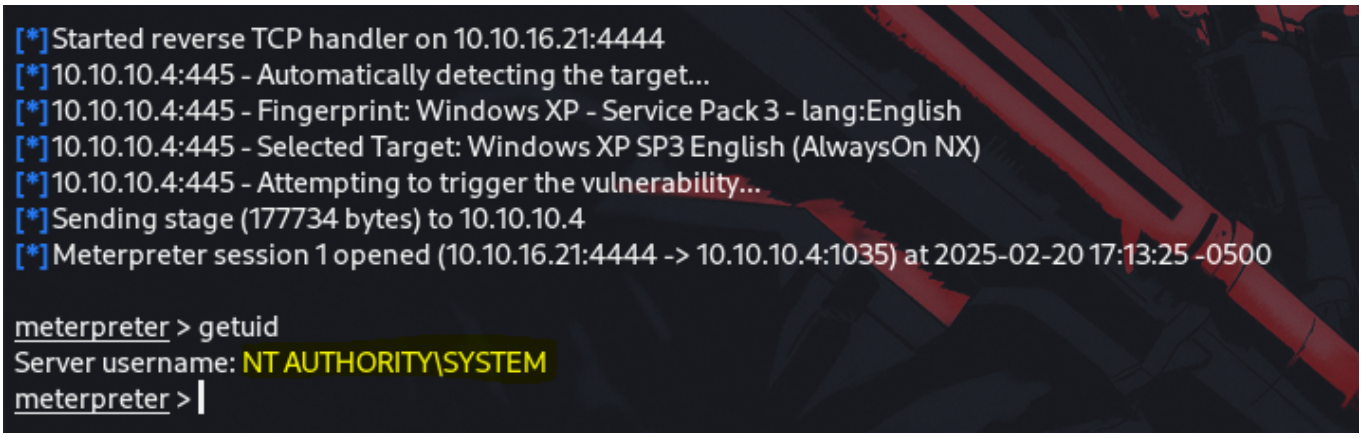
Si buscamos la vulnerabilidad **ms08-067** en metasploit, encontraremos un módulo para explotar esta vulnerabilidad



Lo configuramos y lo lanzamos



Después de lanzar el módulo tendremos una sesión privilegiada de **meterpreter**



Ahora solo nos quedará buscar la rootflag y la userflag