MSSQL for Pentester: Discovery

August 24, 2021 By Raj Chandel

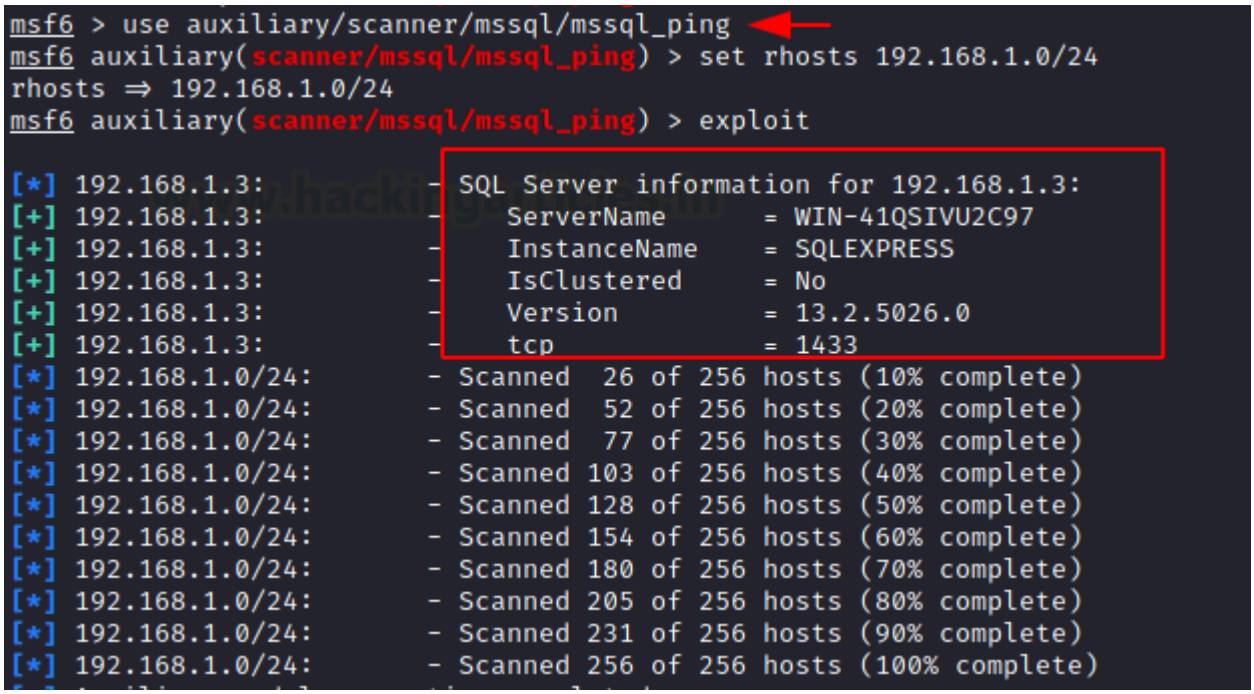
Microsoft SQL Server (MS-SQL) is a relational database manager created by Microsoft. Such management systems are used to engage databases with the user. Multiple databases are used in a large enterprise or organisation which leads to a problem of SQL Sprawl. There are various methods to identify these servers from both pentesting view and or to simply discover MS-SQL servers. In this article, we will explore such various methods in order to discover MS-SQL servers in the network, both locally and remotely.

Table of Content

Metasploit

Using Metasploit to determine the MS-SQL servers in the network is one of the best remote methods one can apply. Metasploit being a remarkable framework has an exploit to determine whether there are MS-SQL servers in your network or not.

```
use auxiliary/scanner/mssql/mssql_ping
set rhosts 192.168.1.0/24
exploit
```

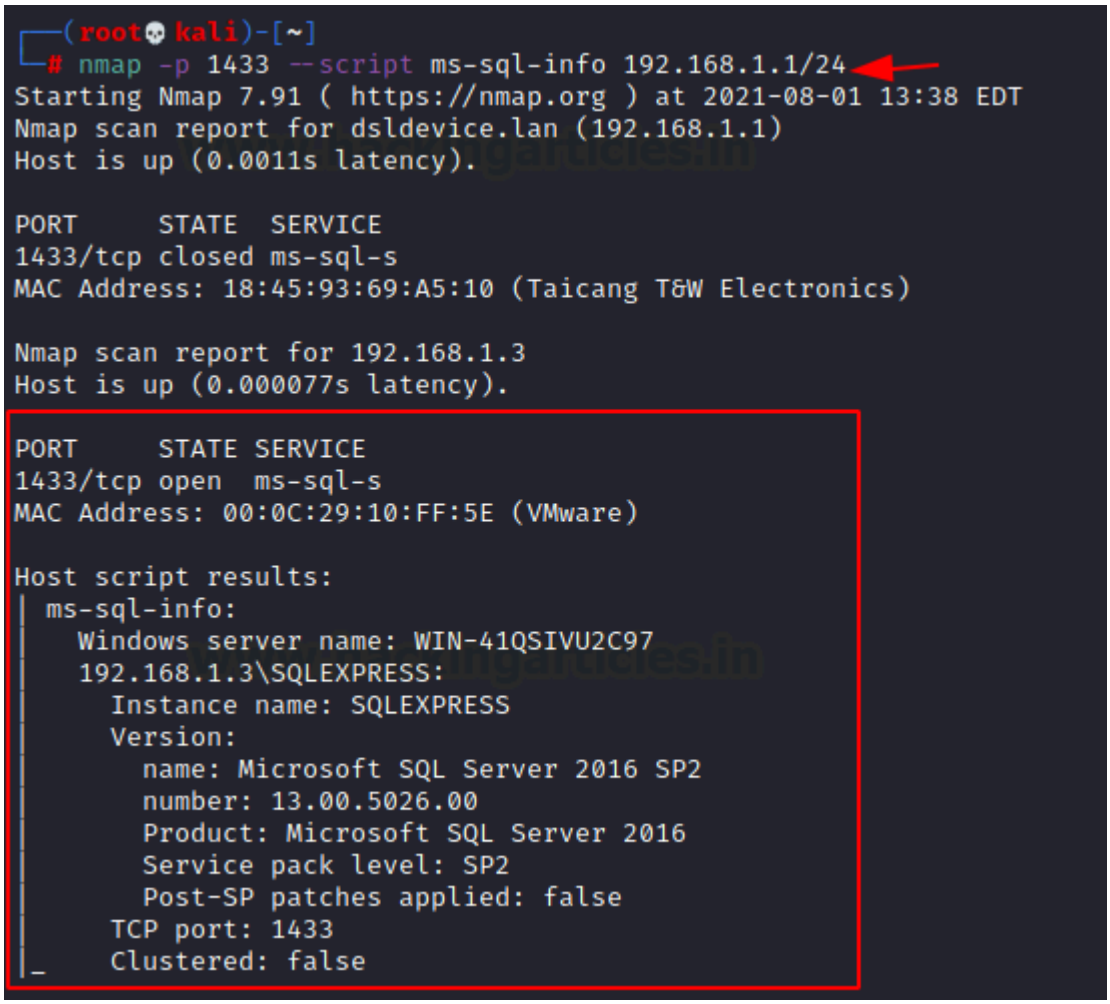


As you can observe in the above image the Metasploit exploit has the result for you and doesn't fail to inform you about the MS-SQL server and its port in the network.

Nmap

Our next method to identify the MS-SQL servers in the network is by using Nmap; the amazing network pentesting tool. This method is a remote method as well. To imply this method, just open your console in kali and type in the following command:

```
nmap -p 1433 -script ms-sql-info 192.168.1.1/24
```

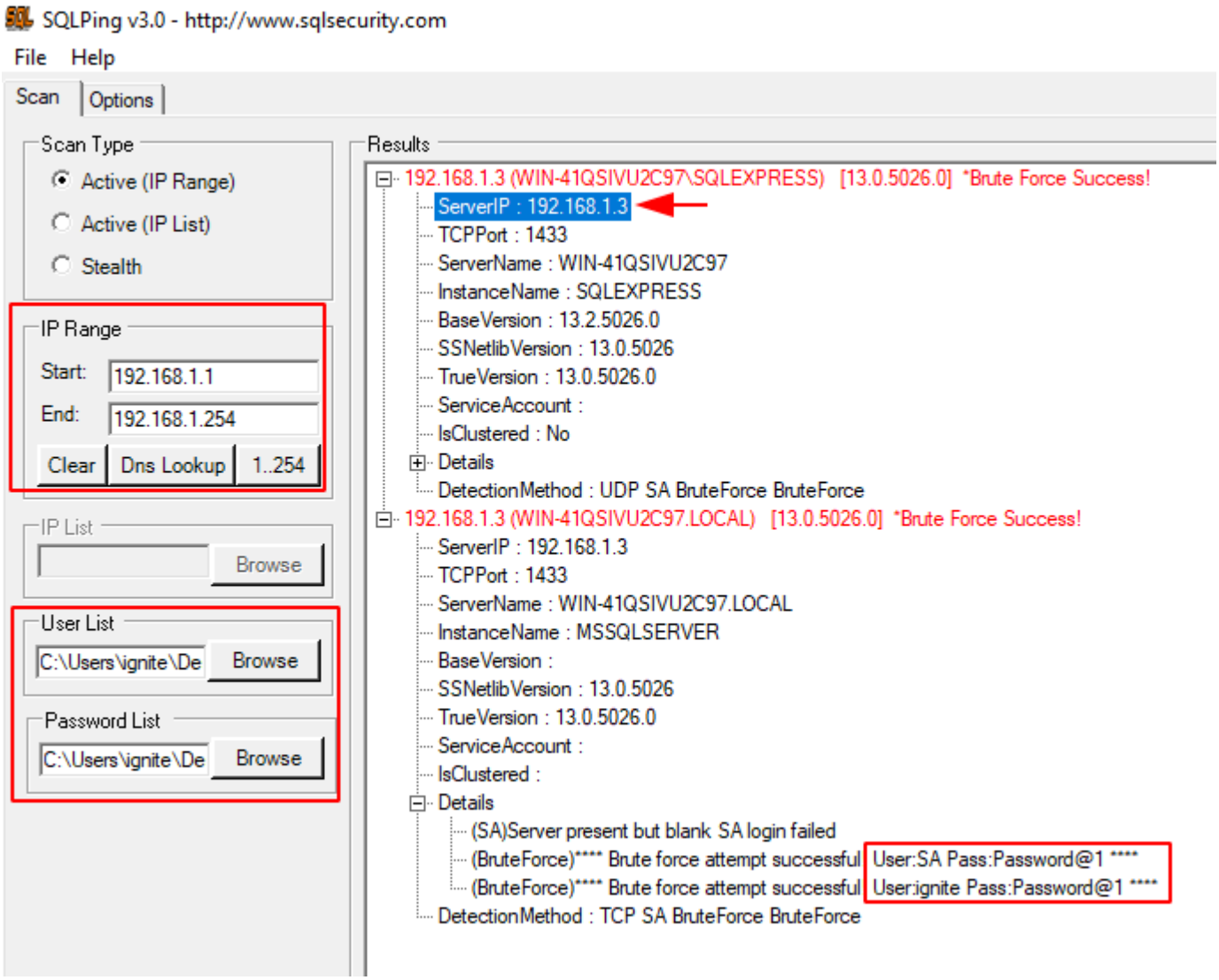


As Nmap is one of the best tools for NSPT, it can never fail to meet our needs. Such is proven in the image above; where you can see that the result of the command shows us the MS-SQL servers present in the network along with its details.

SQLPing

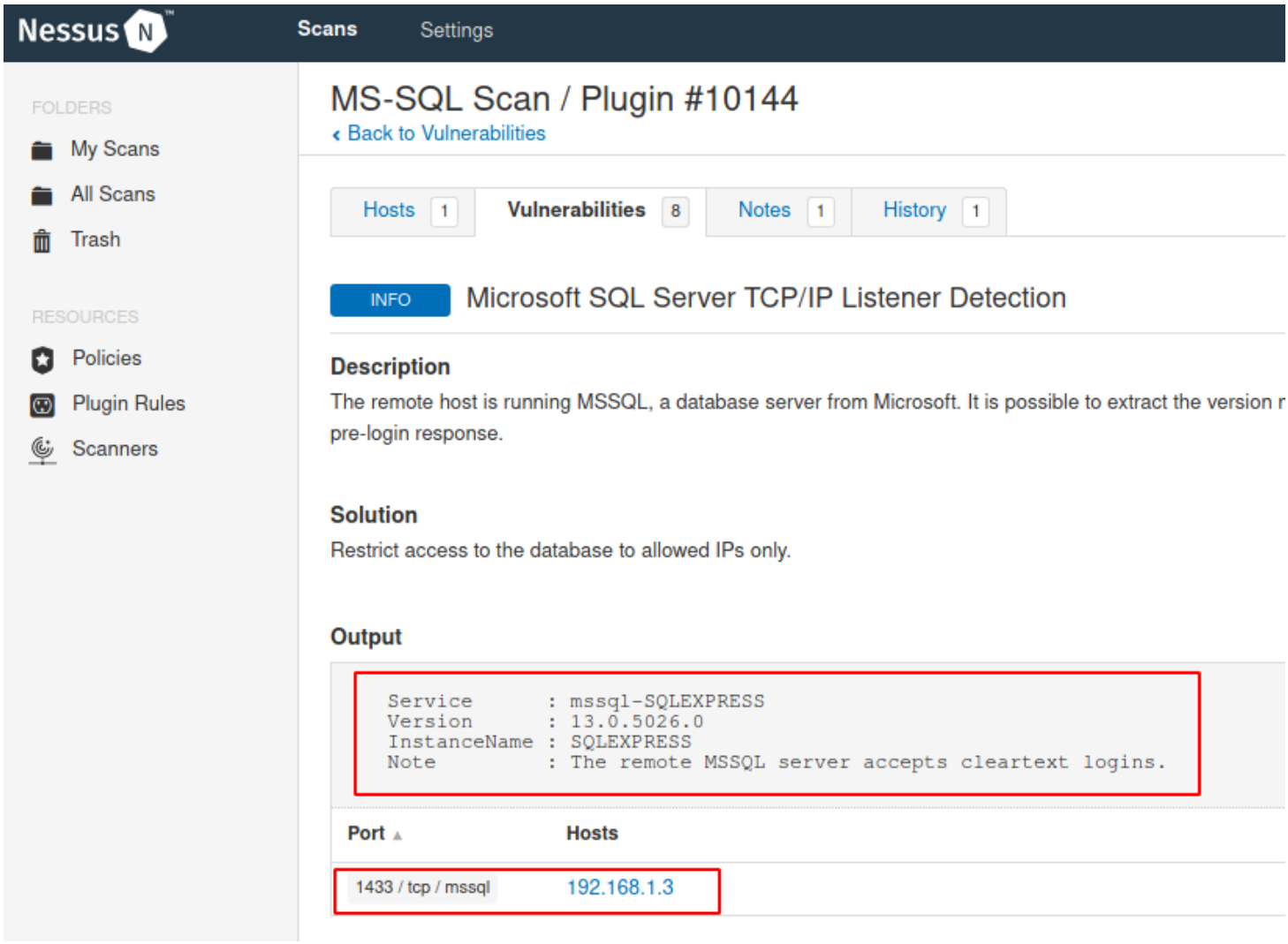
SQLPing is a tool for Windows that helps us to discover the MS-SQL server in the network. This tool is helpful for those who prefer testing through the windows operating system. It can be downloaded from **here**. Once the tool is downloaded, open the tool. In the left panel of the tool give the IP range of the network as shown in the image below. Also, this tool helps to brute force the username and password of the server through a dictionary. So, you can give the path of dictionaries at the bottom of the left panel as shown in the image below:

As you can see below the image, you can find the MS-SQL server in the network through the SQLPing tool.



Nessus

Nessus was developed by Renaud Deraison in 1998 in order to provide the security community with a free remote scanner. And so, this tool succeeded in its aim and made our lives easier. When you are specifically looking for MS-SQL servers in the network then start your Nessus scan, once the scan is complete; you can go to the vulnerabilities tab and put a filter for port 1433 as this is a default port for the Ms-SQL server.



And as you can see in the image above, it will show you all the said servers.

PowerUpSQL

Now, using PowerUpsql is a local method as this tool shows accurate results when it is well present in the network. To use this tool open Windows PowerShell and import the script of the tool and then type in the commands to identify the server. To do so, type the following set of commands:

```
cd .\Desktop\
powershell -ep bypass
Import-Module .\PowerUpSQL.ps1
Get-SQL-InstanceLocal -verbose
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd .\Desktop\
PS C:\Users\Administrator\Desktop> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\Desktop> Import-Module .\PowerUpSQL.ps1
PS C:\Users\Administrator\Desktop> Get-SQLInstanceLocal -Verbose


ComputerName       : WIN-41QSIVU2C97
Instance           : WIN-41QSIVU2C97\SQLEXPRESS
ServiceDisplayName : SQL Server (SQLEXPRESS)
ServiceName        : MSSQL$SQLEXPRESS
ServicePath        : "C:\Program Files\Microsoft SQL Server\MSSQL13.SQLEXPRESS\MSSQL\Binn\sqlservr.exe" -sSQLEXPRESS
ServiceAccount     : NT Service\MSSQL$SQLEXPRESS
State              : Running
```

And so, as you can see in the image above that following there above commands will produce the desired result.

Command Line

Using the command line is also a local method but it is quite useful. This is the easiest method to follow when you want to identify the MS-SQL servers in your network. One of the commands for the said is:

```
sqlcmd -L
```

```
C:\Users\Administrator>sqlcmd -L

Servers:
    WIN-41QSIVU2C97\SQLEXPRESS
```


And the other command for the same is the following:

```
osql -L
```

```
C:\Users\Administrator>osql -L

Servers:
    WIN-41QSIVU2C97\SQLEXPRESS
```


As you can observe from both of the images above, you have your desired result. These are the most effective ways to find out the MS-SQL database servers in the network both remotely and locally. Such methods go a long way in proving our testing to be effective.