# Ryan Foster

CIS 483-01

# Lab: DB Pen Testing with Kali Linux

# Tasks CISSecureS23

## 1. Retrieving MS SQL server information

Task: Retrieve MS SQL server information like below. Explain how you were able to overcome the filtering. Also, provide the result like below in a screenshot (Screenshot #1).

Overcame the filtering because there was no filtering in the first place. The firewall was turned off.

A screenshot of a computer

Description automatically generated

## 2. Brute forcing MS SQL passwords

Task: Display the result in a screenshot (Screenshot #2). Describe what you have accomplished.

Looks like we were able to brute force the passwords for the three users that we just created in the SQl server on the windows server. We were able to run the list of passwords in the password file through the three carduser users and login to each one as shown below.

Graphical user interface, text

Description automatically generated

## 3. Dumping the password hashes of MS SQL

Task: Display the result in a screenshot (Screenshot #3).

Text

Description automatically generated

## 4. Finding sysadmin accounts with empty passwords on MS SQL

Task: Display the result with ‘sa’ account in a screenshot (Screenshot #4).

Text

Description automatically generated

## 5. Running commands through the command shell on MS SQL

Task: Run the above command using ‘sa’ account with empty password. Display the result in a screenshot (Screenshot #5A).

A screenshot of a computer

Description automatically generated with medium confidence

Task: Run the above command using ‘carduser1’ account. Display the result in a screenshot (Screenshot #5B). Why are the results from 5A and 5B different?

A screenshot of a computer

Description automatically generated with medium confidence