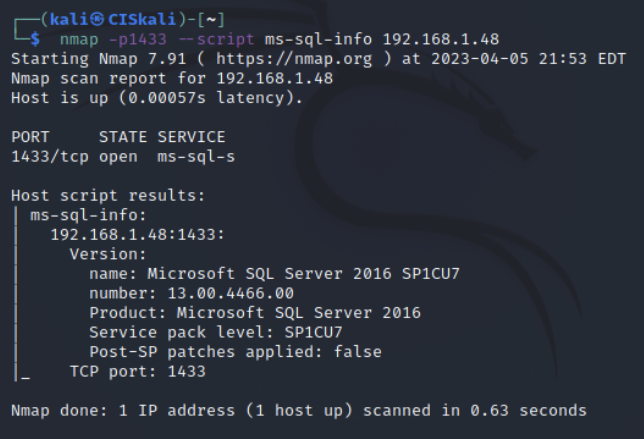
# Lab: DB Pen Testing with Kali Linux

***Daniel Hutchins – CIS 483-75***

# Tasks

## 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). 

**The firewall was disabled on the Windows SQL Server, which allowed for port 1433 to be exploited and had an nmap scan successfully complete.**

## 2. Brute forcing MS SQL passwords

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

Graphical user interface, text

Description automatically generated

**The brute force attack was able to impersonate the 3 logins we added to the usernames.lst.**

## 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).

Text

Description automatically generated A picture containing text

Description automatically generated

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?

Graphical user interface, text

Description automatically generated

**carduser1 does not have the same permissions as the sa account on the SQL Server, hence why the 2nd attempt to pull info from the server was not successful and stopped at the initial login. The sa user’s permissions allow for ipconfig commands and server-wide functions to execute.**