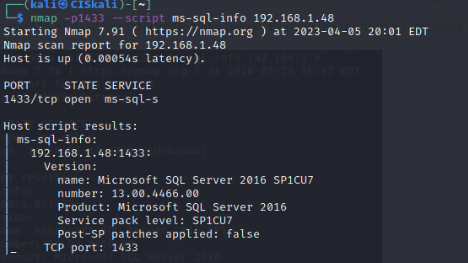
# Lab: DB Pen Testing with Kali Linux

# Tasks

## 1. Retrieving MS SQL server information

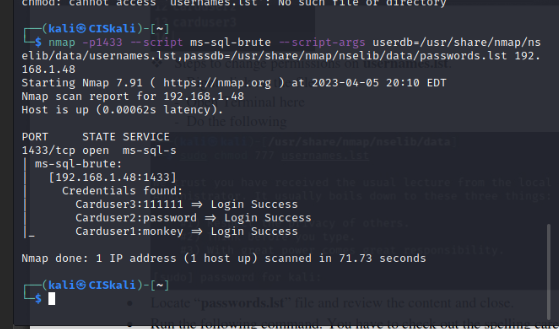
Task: Retrieve MS SQL server information like below. Explain how you were able to overcome the filtering. Also, provide the result like below in a screenshot (Screenshot #1).



I was able to bypass filtering by turning off the firewall.

## 2. Brute forcing MS SQL passwords

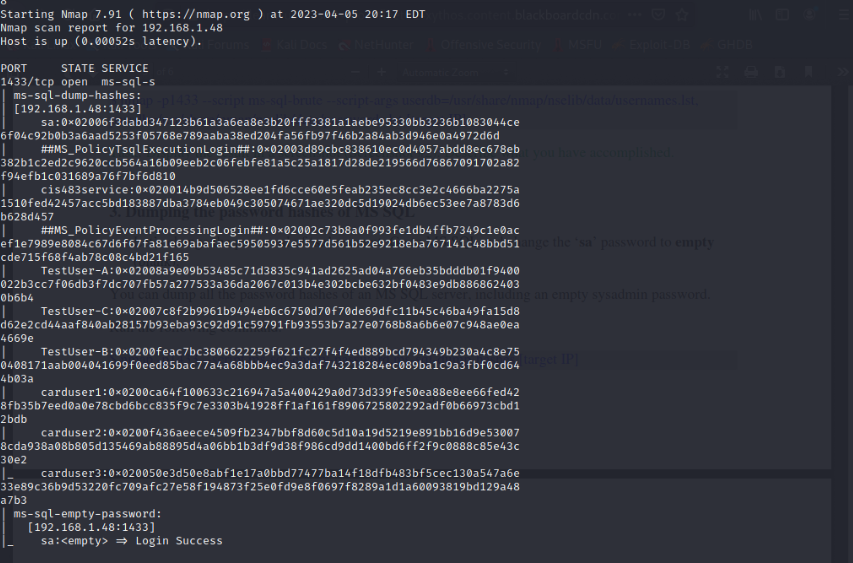
Task: Display the result in a screenshot (Screenshot #2). Describe what you have accomplished.

\

I just accessed the three accounts by brute forcing into each.

## 3. Dumping the password hashes of MS SQL

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



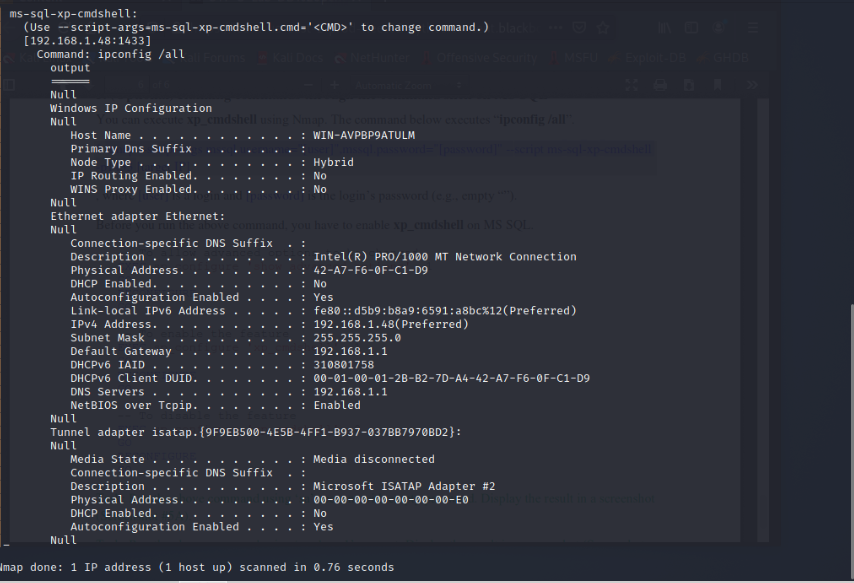
## 4. Finding sysadmin accounts with empty passwords on MS SQL

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

## 

## 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).



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?

