# Lab: DB Pen Testing with Kali Linux

|  |
| --- |
| * This lab is worth 10 points. * The due date is Saturday, April 4 at midnight. * Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., DBPenTesting\_ImG.docx). |

# Tasks

## 1. Retrieving MS SQL server information

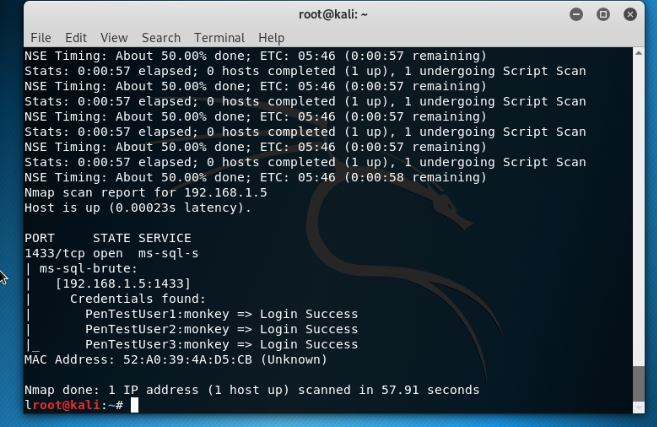
Task: Retrieve MS SQL server information like below. Explain how you were able to overcome the filtering. Also, provide the result like below in a screenshot (Screenshot #1).

I overcame the filtering by going into the Windows Server Machine and creating a rule to allow traffic to port 1433. I then rescanned and got the needed result for the screenshot. I made sure to delete the rule after I finished the lab to avoid leaving an open port.



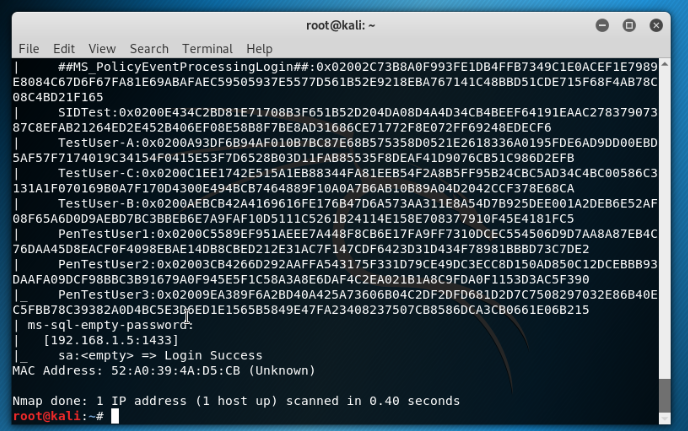
## 2. Brute forcing MS SQL passwords

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



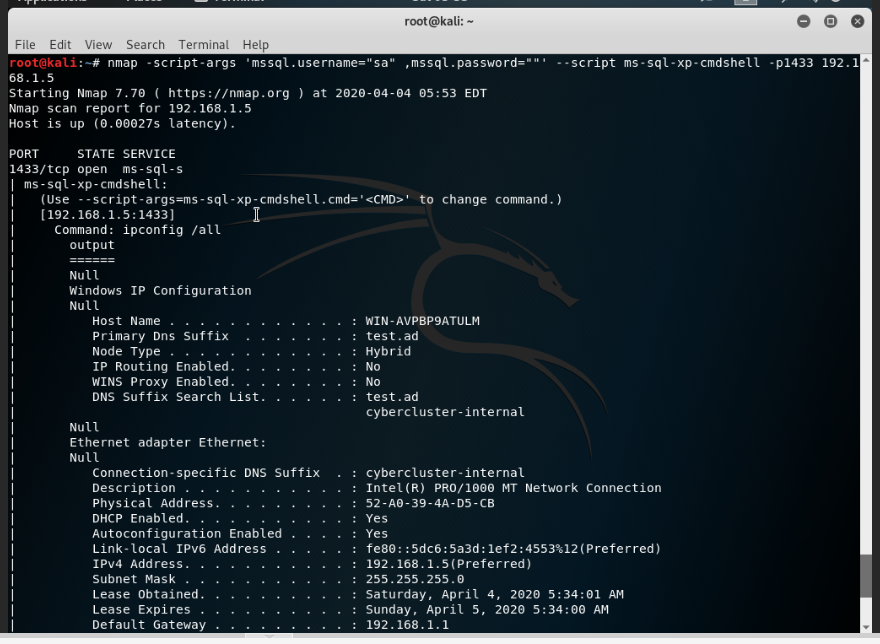
## 3. Dumping the password hashes of MS SQL

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

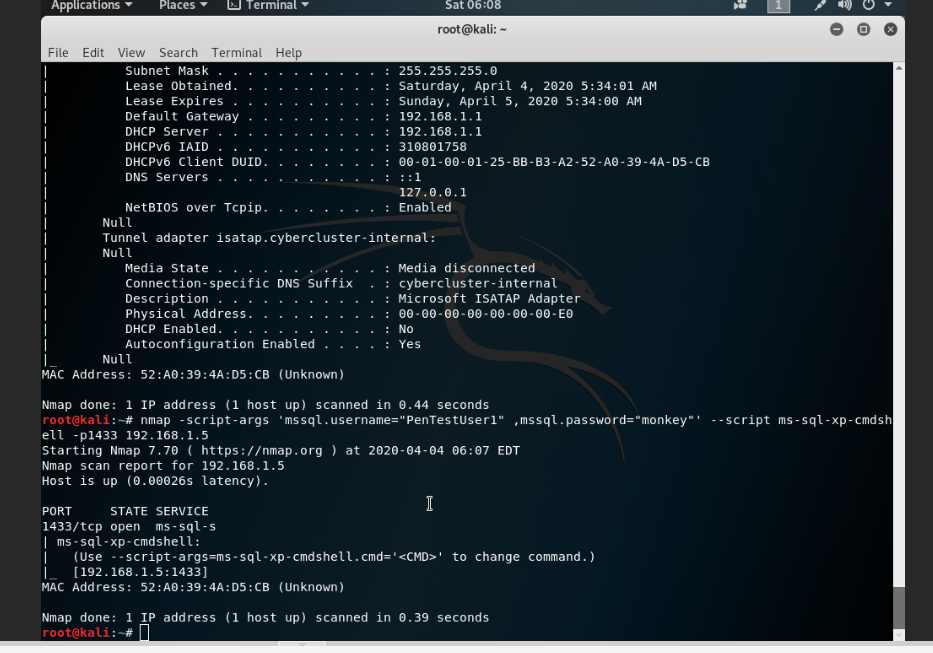


## 4. Running commands through the command shell on MS SQL

Task: run the above command using ‘sa’ account with empty password. Display the result in a screenshot (Screenshot #4A).



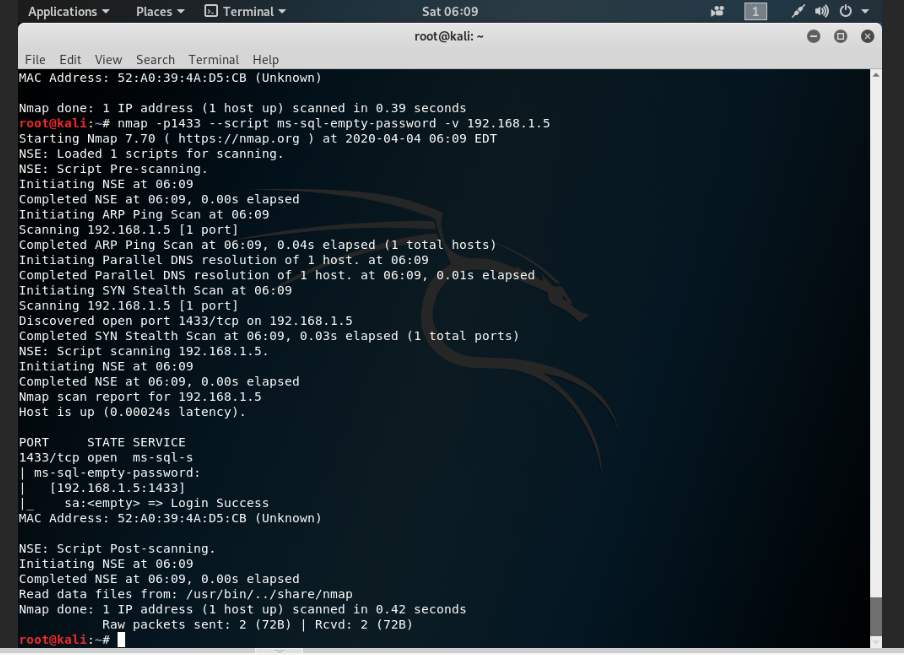
Task: run the above command using ‘PenTestUser1’ account. Display the result in a screenshot (Screenshot #4B). Why are the results from 4A and 4B different?



The results are different due to the different privileges and attributed to each account.

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

Task: Display the result with ‘sa’ account in a screenshot (Screenshot #5).



I made sure to delete the open port rule and disable xp\_cmd after finishing the lab.