# Lab: DB Pen Testing with Kali Linux

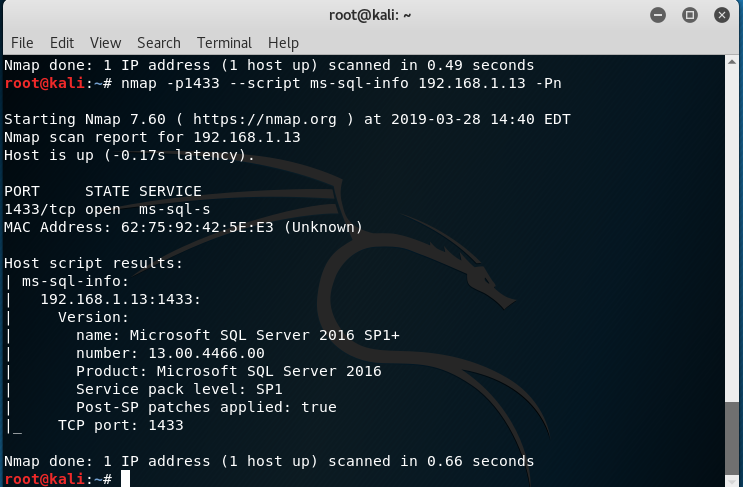
|  |
| --- |
| * This lab is worth 10 points. * The due date is Saturday midnight (March 30). * Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., DBPenTesting\_ImG.docx). |

# Tasks

## 1. Retrieving MS SQL server information

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

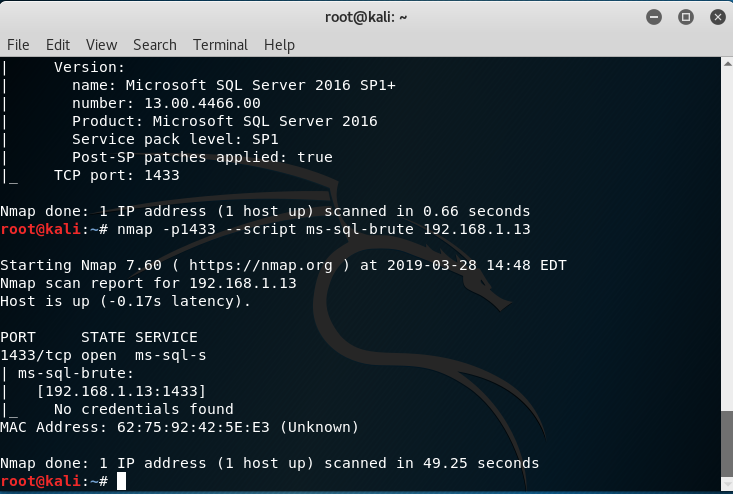
I turned off all of the firewalls in windows vm.



## 2. Brute forcing MS SQL passwords

Run the following command:

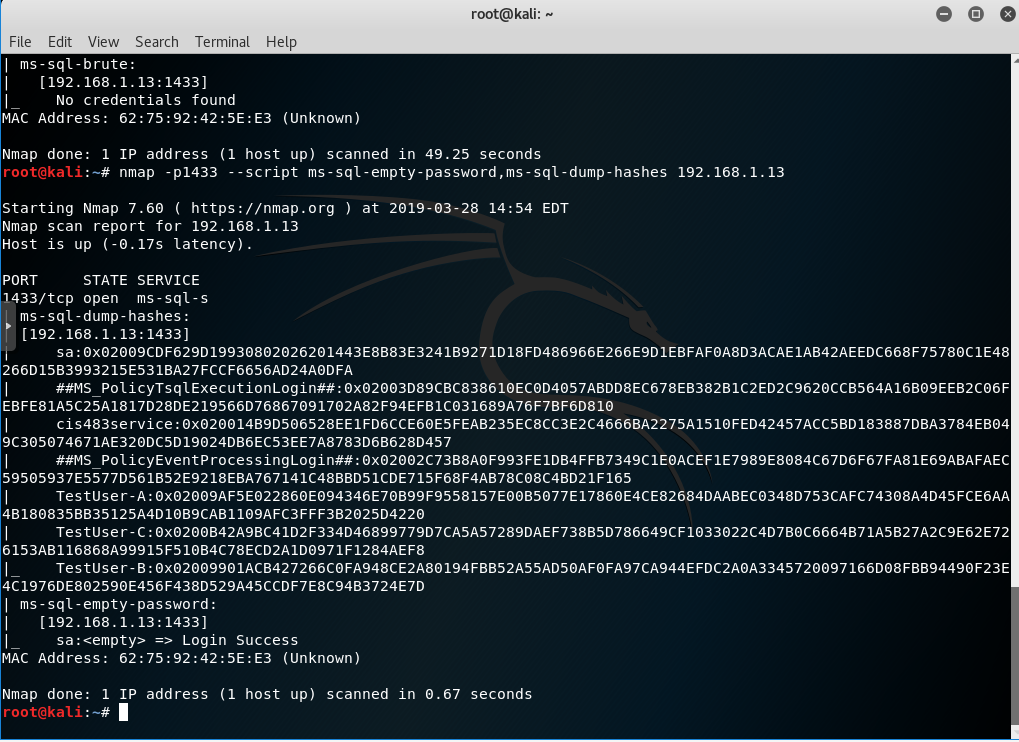
Task: Display the result in a screenshot (Screenshot #2).



## 3. Dumping the password hashes of MS SQL

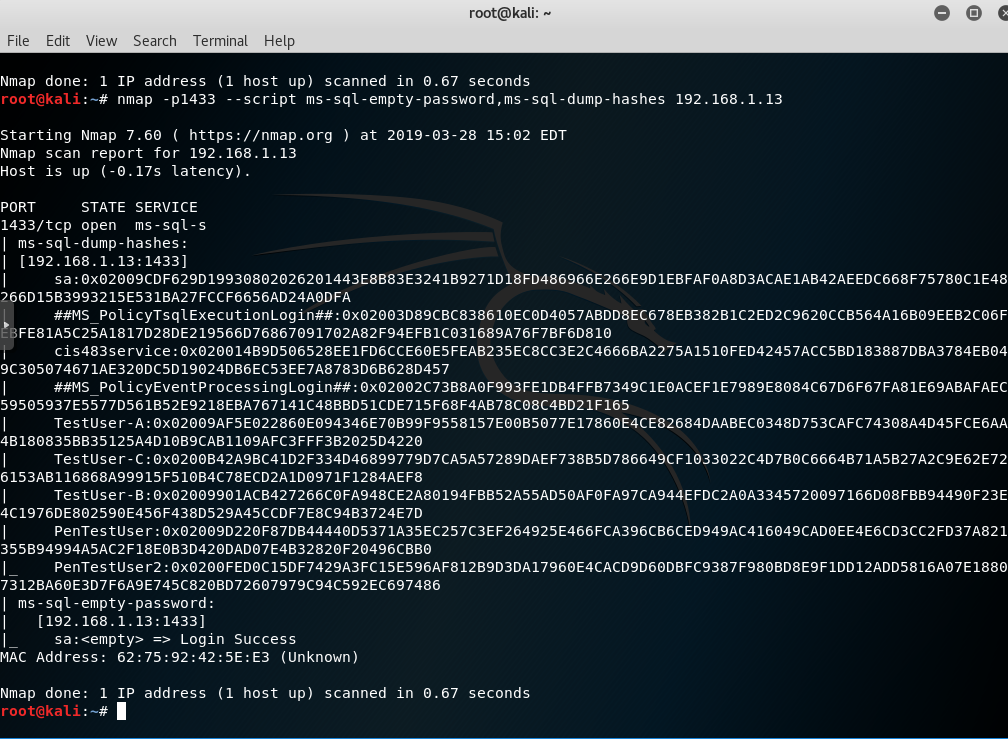
Run the following command:

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



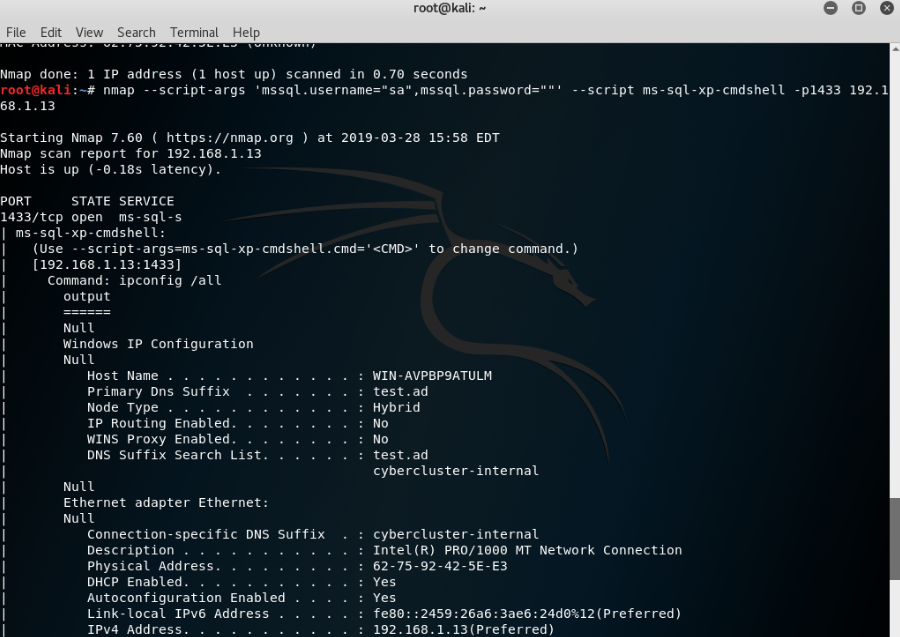
After this, run the following command in MS SQL and run the above Nmap script.

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



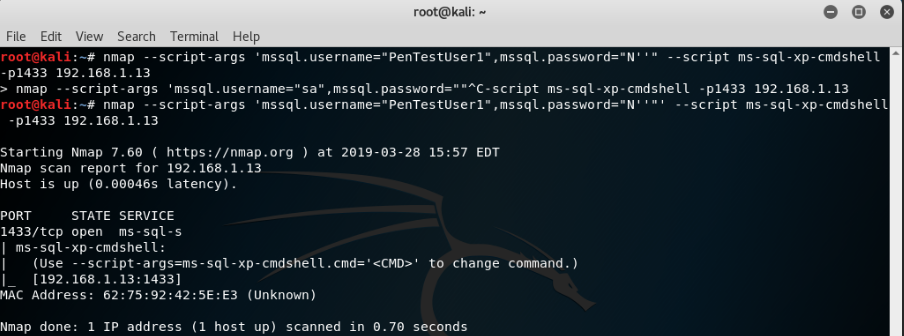
## 4. Running commands through the command shell on MS SQL

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?

SA has permission to run ipconfig and PenTestUser1 is just a login. No permissions have been attached to it.



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

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

