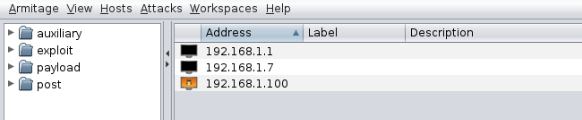
# Lab: MySQL Hacking with Metasploit

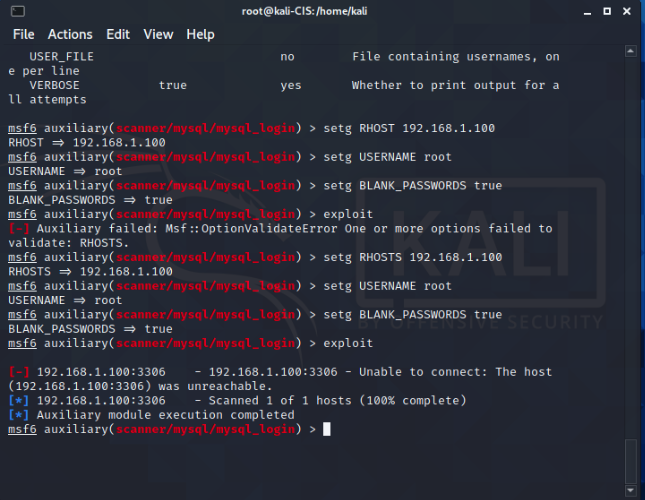
|  |
| --- |
| * This lab is worth 2 points. * The due date is Tuesday midnight. * Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., MySQLHacking\_ImG.docx). |

## Task 1: Brute-forcing logins

1. msf > use **auxiliary/scanner/mysql/mysql\_login**

* Take a screenshot of the outcome. Explain what you have done and accomplished.



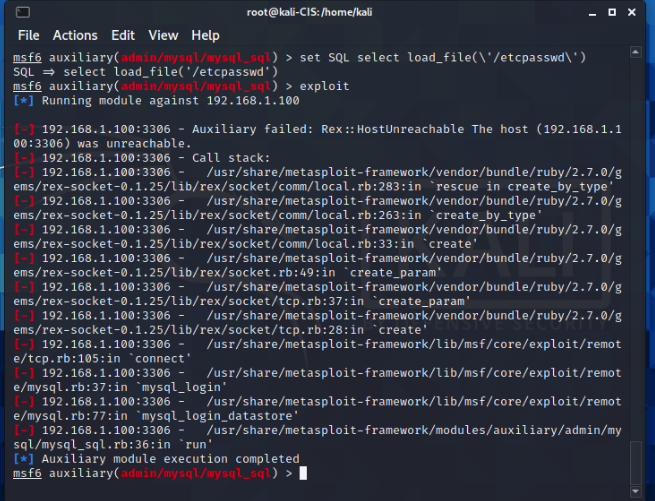


In this task I used a brute force attack, I first located the target which is the ip address for the machines using armitage, and then ran the exploit, then I set the username to root and made the password blank in the sql database.

## Task 2: Dumping /etc/passwd from MySQL

1. msf auxiliary(mysql\_sql) > use **auxiliary/admin/mysql/mysql\_sql**
2. msf auxiliary(mysql\_sql) > set **SQL select load\_file(\'/etc/passwd\')**

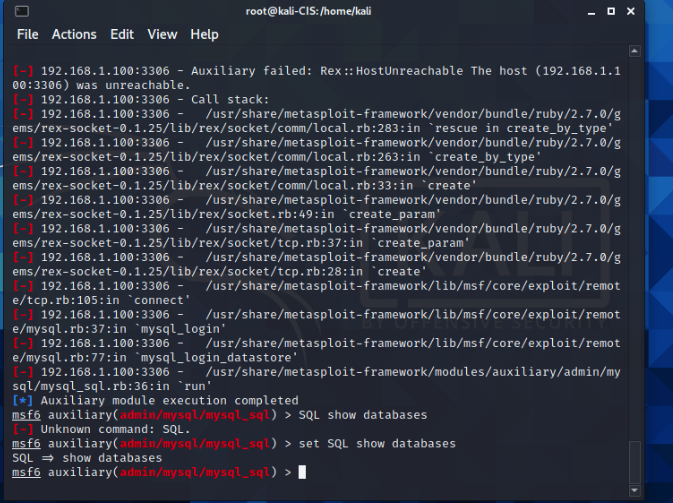
* Take a screenshot of the outcome. Explain what you have done and accomplished.



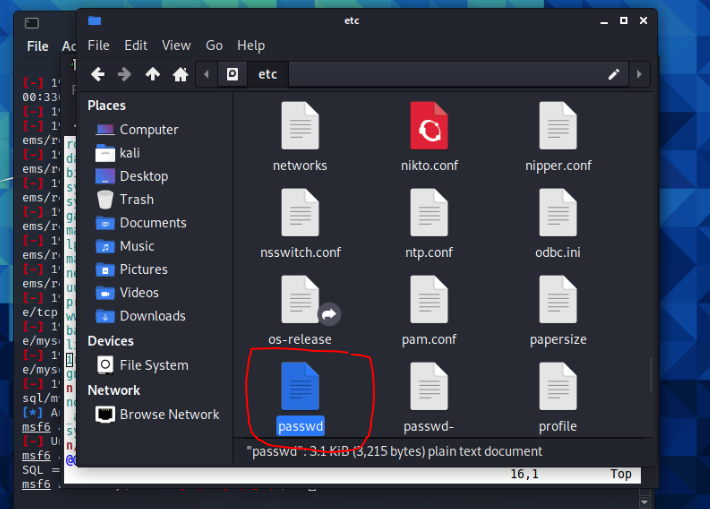
In this set after running the exploit, and managed to gain access to mysql, I’ve taken the passwords stored in mysql database and made file this method is called data collection.

1. msf auxiliary(mysql\_sql) > set **SQL show databases**

* Take a screenshot of the outcome. Explain what you have done and accomplished.



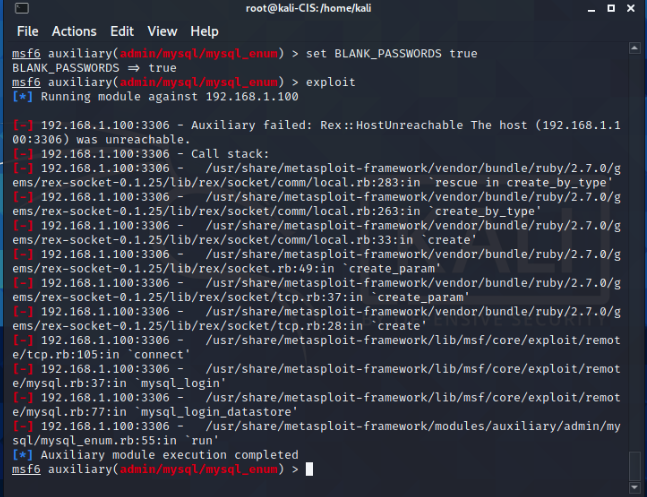
After finind the target, executing the payload we gained access to SQL database, in which we dumb the password into a local file, and it is as seen below



## Task 3: Enumerating MySQL Users

1. msf auxiliary(mysql\_enum) > use **auxiliary/admin/mysql/mysql\_enum**

* Take a screenshot of the outcome. Explain what you have done and accomplished.



In this step I reverted everything back to what it was which is “cleaning up” and next I can deliver.