Mysql

Note:
Default port of Mysql is 3306

- Mysql is RDBMS
- It uses SQL language
- Stores data in tables which can be accessed by clients

Enumeration :

- Inorder to connect to the remote mysql server, mysql-client is need to install on the system.
- To install mysql client – sudo apt install default-mysql-client

Here, we can enumerate by manually or using automated tools like Nmap scripts and Metasploit modules.

i) First scan the target ip & find the service version of it
ii) Find if any exploit available for the version. (In this example, Mysql server version is 5.7, There is a exploit available for 4.x & 5.x version, which states that when someone try to log in with wrong password, sql server returns different message than access denied. by using this we can get the possible users)
iii) Then, use NSE scripts mysql-enum we can get the possible username (You can also use metasploit module mysql_sql).
iv) Then using different Tools bruteforce the password.
v) Finally, try to log in into mysql server using mysql-client which we installed above.

This comes under exploitation

Exploitation :

Here, we already did it above, but there may be more than one way to do it. Lets see,

There is the another metasploit module named mysql_schemadump. which dumps the schema of the entire database

Again, Another metasploit module named mysql_hashdump it extracts the username & password hashes and displays it which is used later in cracking.

Here, we crack password using Hydra.

↳ Copy the password hash with usernames (i.e) user:axx5cdxx
(user = username, axx5cdxx = hash)

↳ Then use John to crack by john hash.txt

↳ Then we got the password.

Sometimes, Same password is used to multiple services, In THM eg:) we use mysql password for user carl & try to log on into another services running on system which is nothing but SSH & Then we able to pwn the machine & got access.