Thursday September 23, 2021
TryHackMe - Task8 - Understanding MySQL
https://tryhackme.com/room/networkservices2

INTRODUCTION

MySQL is a relational database management system (RDBMS) based on Structured Query Language (SQL). Other database management systems such as PostgreSQL and Microsoft SQL server use slightly different SQL syntax. MySQL can run on various platforms, whether it's Linux or windows. It is commonly used as a back end database for many prominent websites and forms an essential component of the LAMP stack, which includes: Linux, Apache, MySQL, and PHP. Facebook is a major social networking site that uses MySQL.

Client - Server Model:

MySQL, as an RDBMS, is made up of the server and utility programs that help in the administration of MySQL databases. The server handles all database instructions like creating, editing, and accessing data. It takes and manages these requests and communicates using the MySQL protocol. This whole process can be broken down into these stages:

1. MySQL creates a database for storing and manipulating data, defining the relationship of each table.
2. Clients make requests by making specific statements in SQL.
3. The server will respond to the client with whatever information has been requested.

ASSUMPTIONS

Assumption: Assume that the credentials: "root:password" have been found while enumerating subdomains of a web server.

REQUIREMENTS

Requirements: MySQL client.
To install the default mysql client on the AttackBox the following command was run in the terminal:

sudo apt install default-mysql-client

```
root@ip-10-10-59-225:~# sudo apt install default-mysql-client

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following additional packages will be installed:

  libaio1 mysql-client-5.7 mysql-client-core-5.7

The following NEW packages will be installed

  default-mysql-client libaio1 mysql-client-5.7 mysql-client-core-5.7

0 to upgrade, 4 to newly install, 0 to remove and 377 not to upgrade.

Need to get 8,582 kB of archives.

After this operation, 61.2 MB of additional disk space will be used.

Do you want to continue? [Y/n] Y

Get:1 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libaio1
amd64 0.3.110-5ubuntu0.1 [6,476 B]

Get:2 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64
mysql-client-core-5.7 amd64 5.7.35-0ubuntu0.18.04.1 [6,627 kB]

Get:3 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64
mysql-client-5.7 amd64 5.7.35-0ubuntu0.18.04.1 [1,944 kB]

Get:4 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu bionic/universe amd64
default-mysql-client all 1.0.4 [3,508 B]

Fetched 8,582 kB in 0s (27.5 MB/s)

Selecting previously unselected package libaio1:amd64.

(Reading database ... 353162 files and directories currently installed.)

Preparing to unpack .../libaio1_0.3.110-5ubuntu0.1_amd64.deb ...

Unpacking libaio1:amd64 (0.3.110-5ubuntu0.1) ...
```

```
Selecting previously unselected package mysql-client-core-5.7.
Preparing to unpack .../mysql-client-core-5.7_5.7.35-0ubuntu0.18.04.1_amd64.deb ...
Unpacking mysql-client-core-5.7 (5.7.35-0ubuntu0.18.04.1) ...
Selecting previously unselected package mysql-client-5.7.
Preparing to unpack .../mysql-client-5.7_5.7.35-0ubuntu0.18.04.1_amd64.deb ...
Unpacking mysql-client-5.7 (5.7.35-0ubuntu0.18.04.1) ...
Selecting previously unselected package default-mysql-client.
Preparing to unpack .../default-mysql-client_1.0.4_all.deb ...
Unpacking default-mysql-client (1.0.4) ...
Setting up libaio1:amd64 (0.3.110-5ubuntu0.1) ...
Setting up mysql-client-core-5.7 (5.7.35-0ubuntu0.18.04.1) ...
Setting up mysql-client-5.7 (5.7.35-0ubuntu0.18.04.1) ...
Setting up default-mysql-client (1.0.4) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for libc-bin (2.27-3ubuntu1.2) ...
root@ip-10-10-59-225:~#
```

EXPLOIT

A variable targetIP was set to the target vulnerable machine IP address using the command:

$targetIP=10.10.236.138

root@ip-10-10-59-225:~# targetIP=10.10.236.138

root@ip-10-10-59-225:~# echo $targetIP

10.10.236.138

nmap can be used to scan all of the ports on the target IP 10.10.236.138 using the -p- flag. A scan of the services on those ports can also be run at the same time using the -sV flag. The output of the scan can be sent to a file named nmap_10.10.236.138. The command to do this is:

nmap -sV -p- $targetIP >> nmap_$targetIP

```
nmap -sV -p- $targetIP >> nmap_$targetIP
```

However, this scan takes a long time. So, first I checked if MySQL service was running on the default port 3306. The command to do this is:

nmap -sV -p 3306 $targetIP

As a result, I found that indeed MySQL was running on the default port 3306.

```
root@ip-10-10-59-225:~# nmap -sV -p 3306 $targetIP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-23 23:17 BST
Nmap scan report for ip-10-10-236-138.eu-west-1.compute.internal (10.10.236.138)
Host is up (0.00020s latency).

PORT  STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.7.29-0ubuntu0.18.04.1
MAC Address: 02:C8:0C:B8:1C:77 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
root@ip-10-10-59-225:~# ^C
```

I confirmed I was able to manually connect to the MySQL database using the given credentials of username: root and password: password.

The command was:

mysql -h $targetIP -u root -p

at the password prompt, password was entered.

```
root@ip-10-10-59-225:~# mysql -h $targetIP -u root -p
Enter password:    ← password was entered here
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.7.29-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql>
```

and from there forward I used metasploit. I have to go back and redo this using other tools since my goal is the OSCP and metasploit use is restricted for that exam.