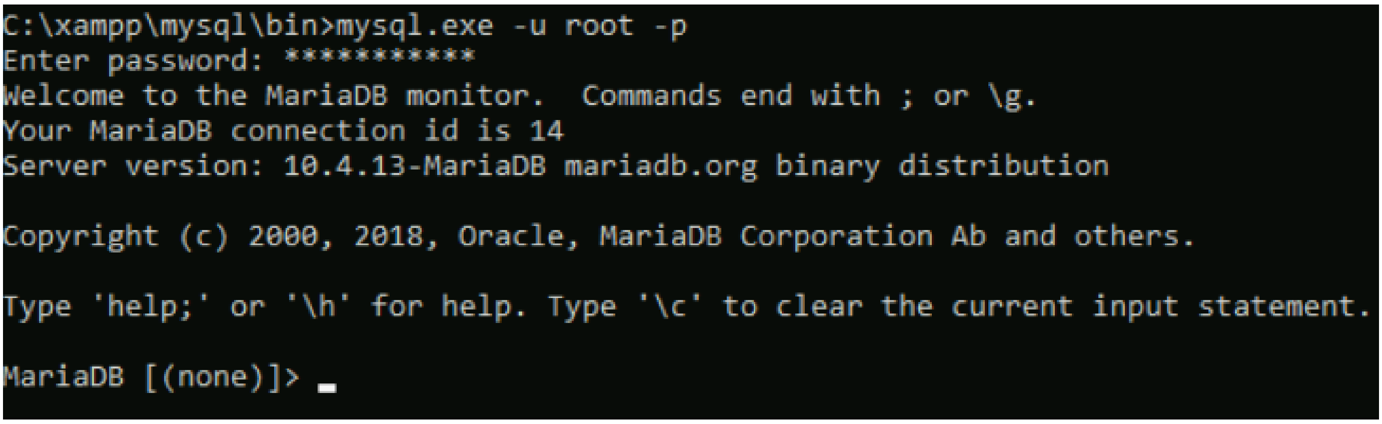
28

Now that we have a foothold onto the timekeep server we can being to enumerate what information we can find from the server. We can assume it is running a sql database somewhere because it had a login page. We also can assume that the web server is using xampp from the C:\ folder within the local disk. With this information we can easily find where the sql database is stored and how we can access it.

Understanding SQL Queries
SQL or structured query language is a database management language that uses queries to interact with various databases. In the Throwback lab, you will be interacting with a MariaDB through MySQL. SQL uses data definition, data manipulation, and data control to manage databases. The main operators used in queries are SELECT, FROM, and WHERE. SELECT, selects an object from a database. FROM, defines the database or table to query from. WHERE chooses the specific data from the object.
Examples of Queries

```
SELECT * FROM credentials WHERE id < 100;
SELECT * FROM table;
```

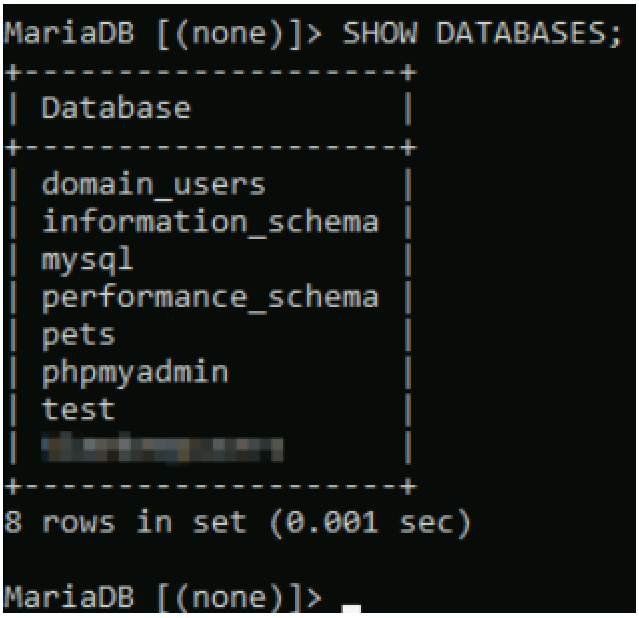
Using Queries to Enumerate Databases
We now the location of the database now and we can us mysql.exe to interact with the database but we dont have a password to login in. From here we could try the password that we got from THROWBACK-WS01 when kerberoasting the SQLService account.
1.) cd xampp/mysql/bin
2.) mysql.exe -u root -p



```
C:\xampp\mysql\bin>mysql.exe -u root -p
Enter password: ***********
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 14
Server version: 10.4.13-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> _
```

Accessing a local MySQL database on Windows

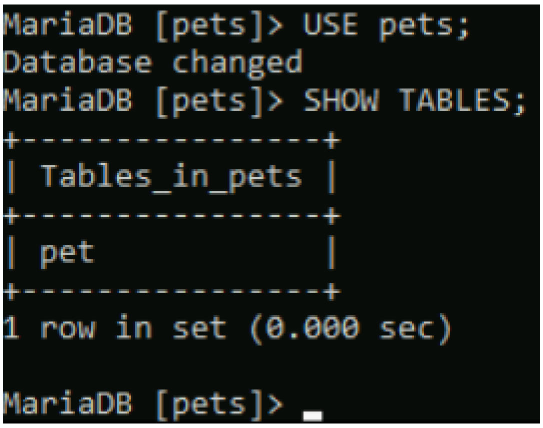
SUCCESS! Were now in the local database and can begin enumerating the contents of it.
3.) SHOW DATABASES;



```
MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| domain_users       |
| information_schema |
| mysql              |
| performance_schema |
| pets               |
| phpmyadmin         |
| test               |
| [redacted]         |
+--------------------+
8 rows in set (0.001 sec)

MariaDB [(none)]> _
```

Listing the databases present in the instance

4.) USE ;
5.) SHOW TABLES;



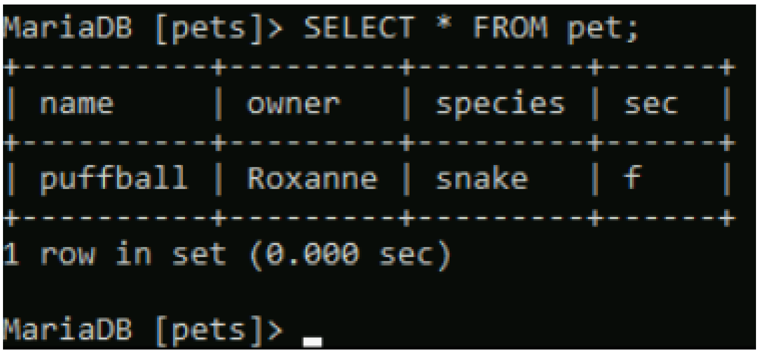
```
MariaDB [pets]> USE pets;
Database changed
MariaDB [pets]> SHOW TABLES;
+----------------+
| Tables_in_pets |
+----------------+
| pet            |
+----------------+
1 row in set (0.000 sec)

MariaDB [pets]> _
```

Selecting the 'pets' database and listing it's tables

Now that we know the databases and tables we can make a query to dump the tables and father the information that we need.

6.) SELECT * FROM

;



```
MariaDB [pets]> SELECT * FROM pet;
+----------+---------+---------+------+
| name     | owner   | species | sec  |
+----------+---------+---------+------+
| puffball | Roxanne | snake   | f    |
+----------+---------+---------+------+
1 row in set (0.000 sec)

MariaDB [pets]> _
```

Listing the contents of the 'pet' table

We have now successfully dumped the pet table from the pets database. These same step can be applied to any database or type of data.
Now that we have access to the database and know how to make queries we can look for potential databases that contain sensitive information. Look through the databases and see if there may any information relevant to the domain.

Answer the questions below

What database are the timekeep login users located?

Submit

What database are the domain users located in?

Submit

What table was located in the domain users database?

Submit

What is the first username in the table?

Submit

Submit flags for THROWBACK-TIME in Task 4.

Completed