**Activity: Apply more filters in SQL**

Overview: As a security analyst, you’ll often need to query numbers and dates. For example, you may need to filter patch dates to find machines that need an update. Or you might filter login attempts made during a certain period of time to investigate a security incident.

Scenario: In this scenario, you’re investigating a recent security incident. You need to gather information about login attempts for certain dates and times. This will help in resolving a security incident. **First**, you’ll retrieve login events made after a certain date. **Second**, you’ll narrow the focus of the search to filter logins in a date range. **Third**, you’ll investigate logins that were made at certain times. **Finally**, you’ll filter login attempts based on their event IDs.

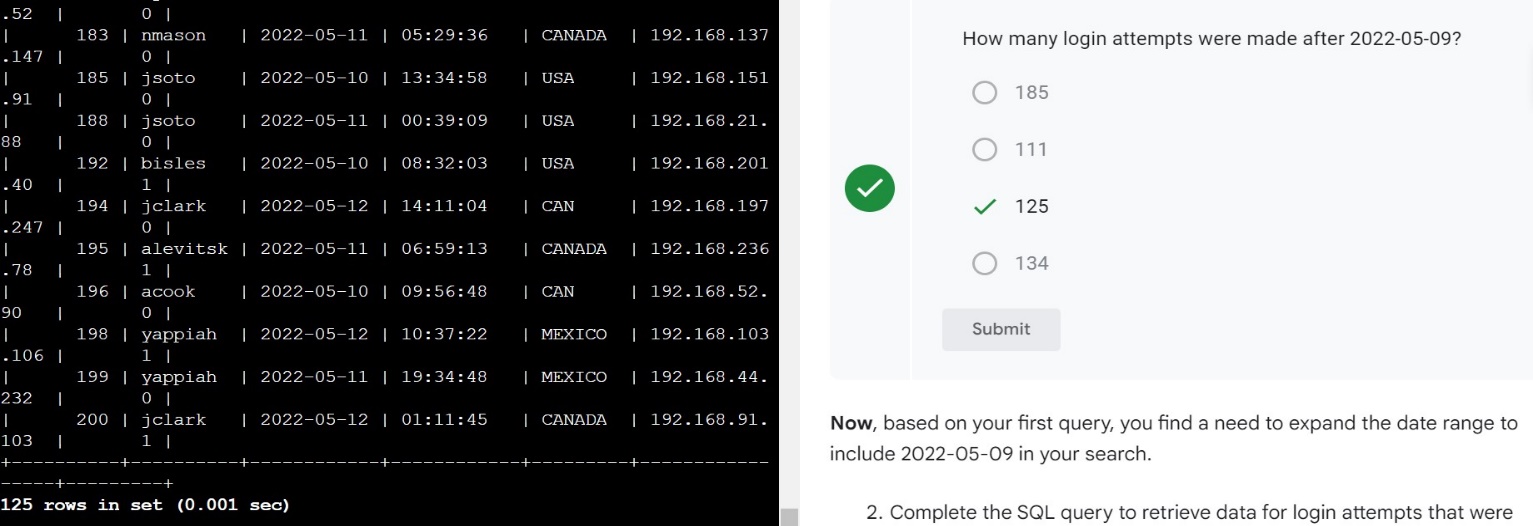
**Start your lab:** click on “start lab” to start the lab.

**Task 1. Retrieve login attempts after a certain date**

In this task, you need to investigate a recent security incident. To do this, you need to gather information about login attempts made after a certain date.

1. Complete the SQL query to retrieve data for login attempts made after '2022-05-09'.

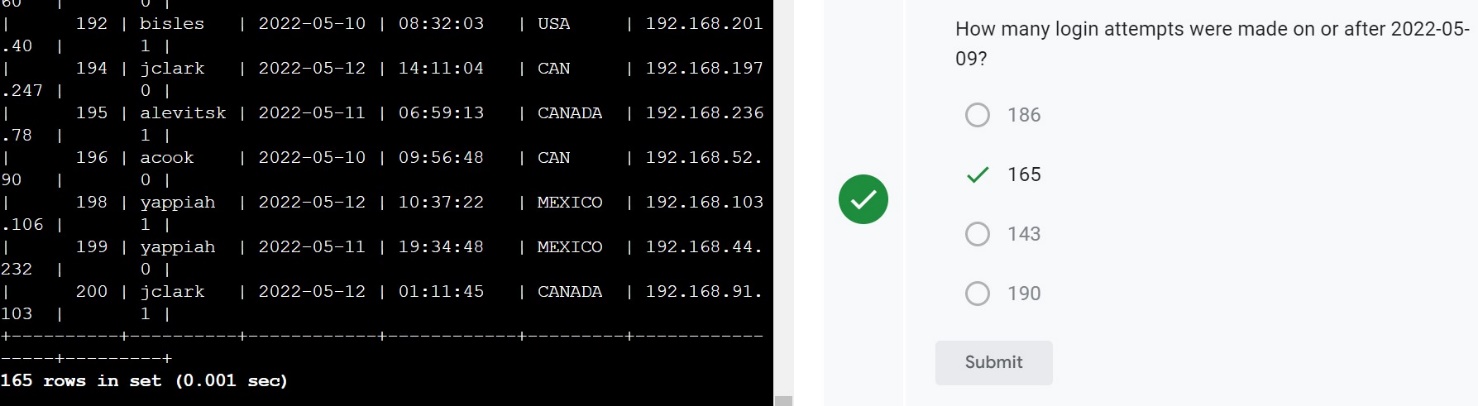
**>SELECT \* FROM log\_in\_attempts WHERE login\_date > ‘2022-05-09’ ;**



1. Complete the SQL query to retrieve data for login attempts that were made on or after '2022-05-09'.

**>SELECT \* FROM log\_in\_attempts WHERE login\_date >= ‘2022-05-09’ ;**

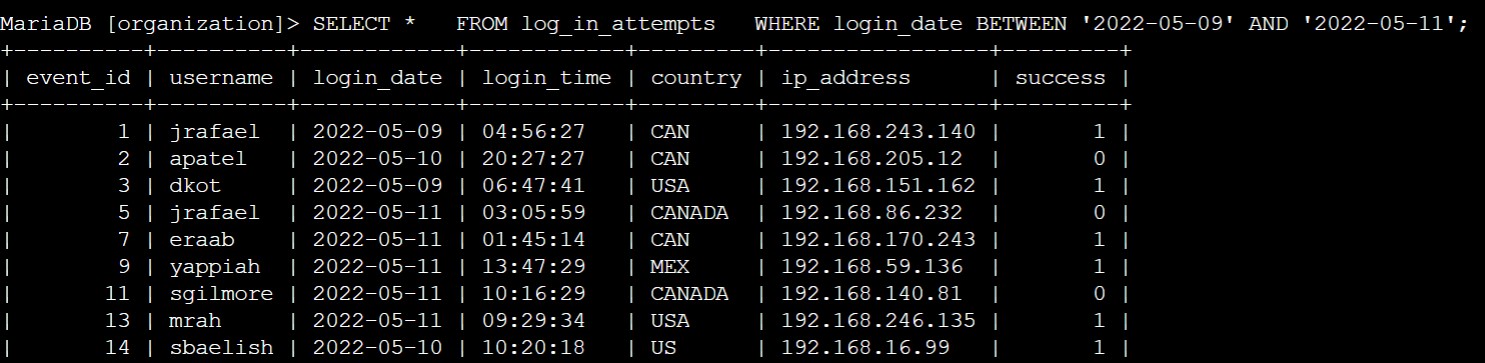


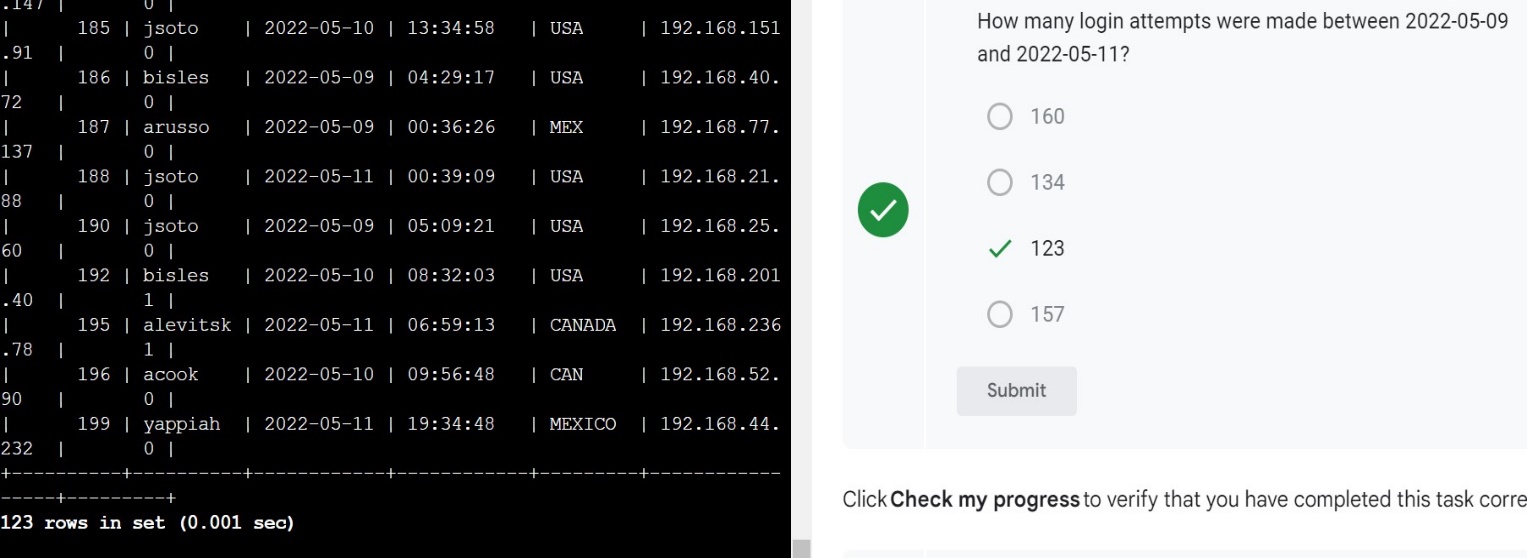


**Task 2. Retrieve logins in a date range**

In this task, you need to narrow the focus of the search. Login attempts made after 2022-05-11 shouldn't be included. Use the BETWEEN and AND operators to return results between '2022-05-09' and '2022-05-11'.

* Run the query to retrieve the required records.

**>SELECT \* FROM log\_in\_attempts WHERE login\_date BETWEEN ‘2022-05-09’ AND ‘2022-05-11’ ;**

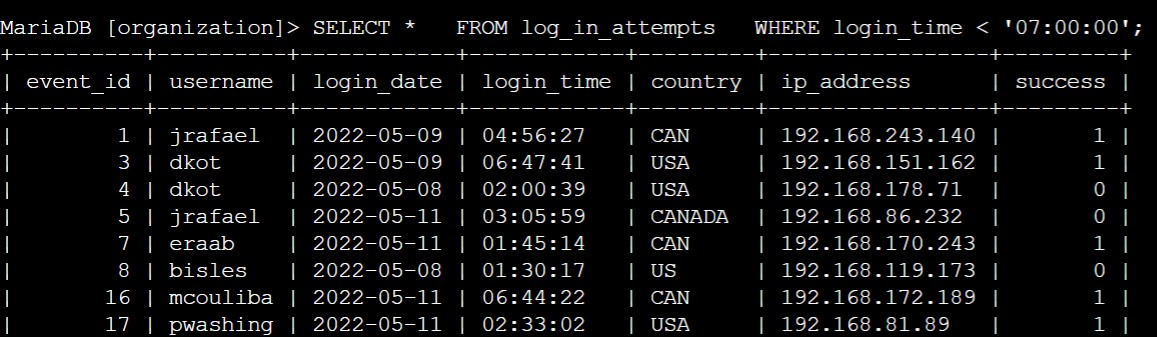


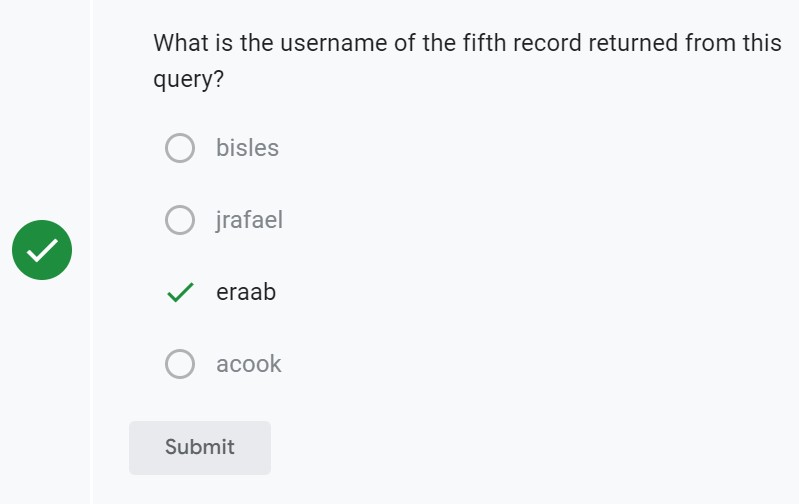
**Task 3. Investigate logins at certain times**

In this task, you need to investigate logins that were made at certain times. To do this, filter the data in the log\_in\_attempts table by login time (login\_time). **First**, your organization's typical work hours begin at 07:00:00. Retrieve all login attempts made before 07:00:00 to learn more about the users who are logging in outside of typical hours.

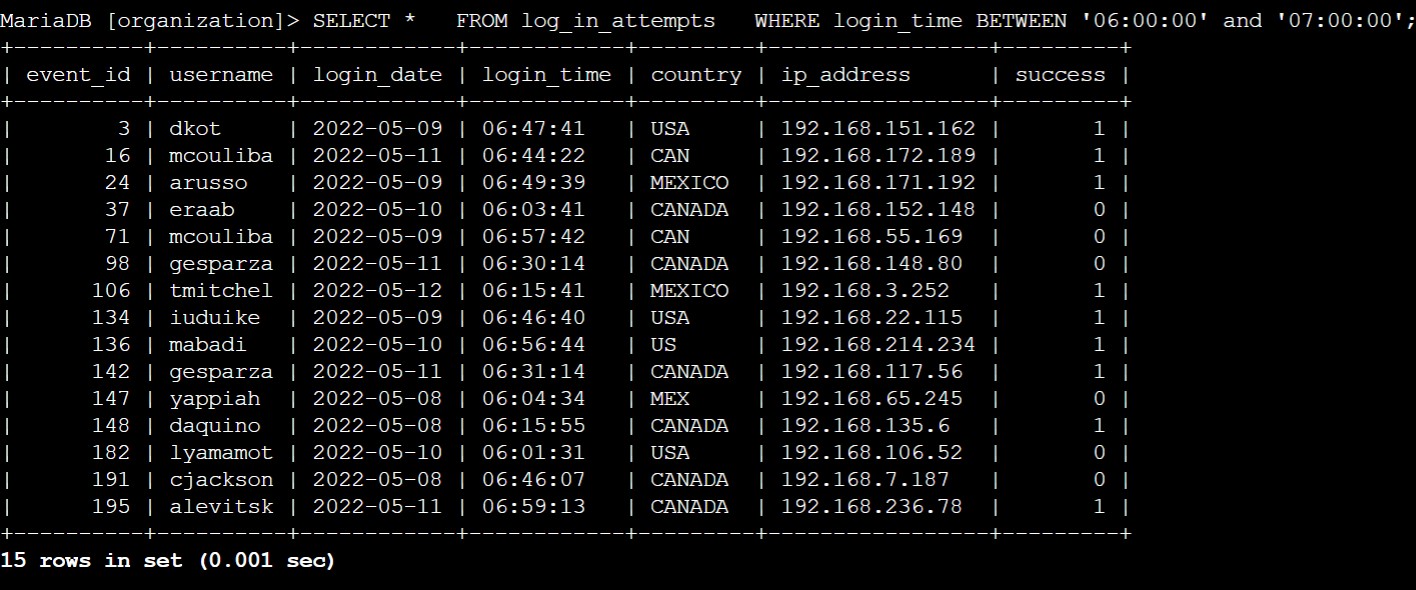
1. Write a SQL query to retrieve data for login attempts made before '07:00:00'.

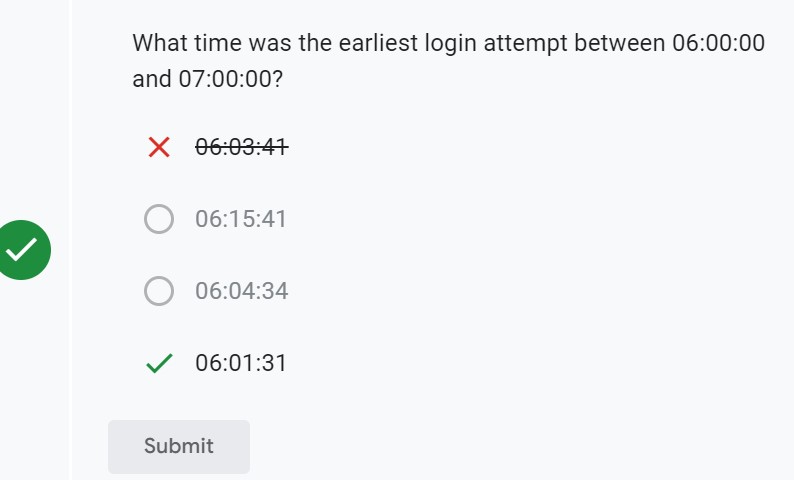
**>SELECT \* FROM log\_in\_attempts WHERE login\_time < ’07:00:00’ ;**





1. Modify the query to return logins between '06:00:00' and '07:00:00'.

**>SELECT \* FROM log\_in\_attempts WHERE login\_time BETWEEN ’06:00:00’ and ’07:00:00’ ;**



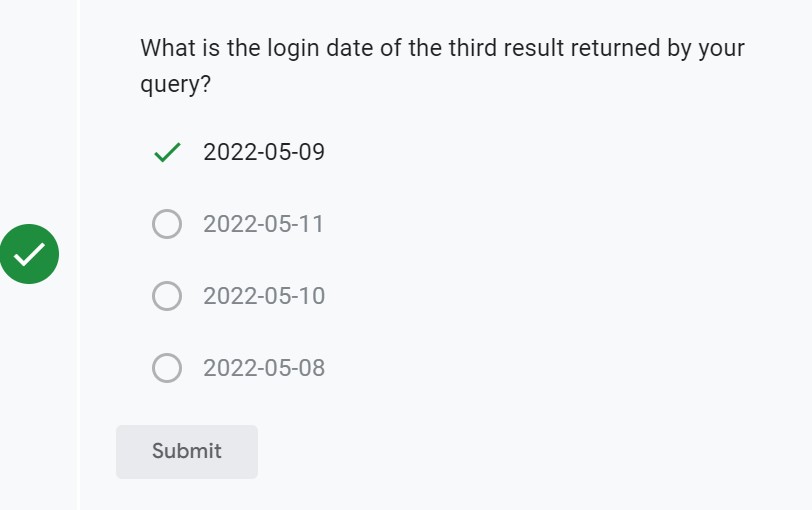
**Task 4. Investigate logins by event ID**

In this task, you need to investigate login attempts based on event ID numbers. With this query, you want to return only the event\_id, username, and login\_date fields from the log\_in\_attempts table.

1. Write a query to return login attempts with event\_id greater than or equal to 100.

**>SELECT \* FROM log\_in\_attempts WHERE event\_id >= 100 ;**

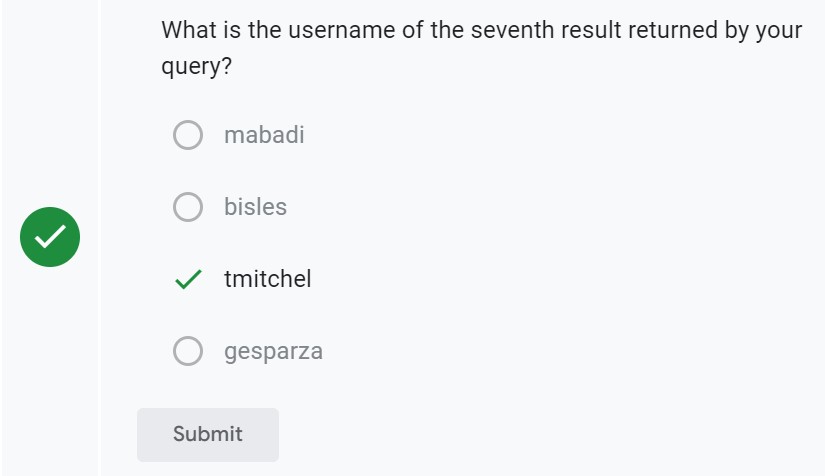




1. Modify the query to return only login attempt with event\_id between 100 and 150.

**>SELECT\* FROM log\_in\_attempts WHERE event\_id BETWEEN 100 and 150 ;**





**Conclusion:**

I have completed this activity and practiced applying

* the WHERE keyword
* the BETWEEN and AND operators, and
* operators for working with numeric or date and time data types (for example, =, >, >=).