**Activity 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.

Common operators for working with numeric or date and time data will help you accurately filter data. These are some of the operators you'll use:

* = (equal)
* > (greater than)
* < (less than)
* <> (not equal to)
* >= (greater than or equal to)
* <= (less than or equal to)

In this lab activity, you’ll apply these operators to accurately filter for specific numbers and dates!

***Note:****The terms****row****and****record****are used interchangeably in this lab activity.*

**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.

Here’s how you’ll do this task: **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.

It's time to get started and use operators to filter data from a table!

***Note:****In this lab you’ll be working with the organization database and the tables it contains.*

*The lab starts with the organization database in the MariaDB shell that is already open. This means you can start with the tasks as soon as you click the****Start Lab****button.*

*If you unintentionally exit the organization database in the MariaDB shell, you can reconnect by running the sudo mysql organization command.*

**Disclaimer:** For optimal performance and compatibility, it is recommended to use either **Google Chrome** or **Mozilla Firefox** browsers while accessing the labs.

**Start your lab**

Before you begin, you can review the instructions for using the Qwiklabs platform under the **Resources** tab in Coursera.

If you haven't already done so, click **Start Lab**. This brings up the terminal so that you can begin completing the tasks!

When you have completed all the tasks, refer to the **End your Lab** section that follows the tasks for information on how to end your 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'. Replace X with the correct operator:

SELECT \*

FROM log\_in\_attempts

WHERE login\_date X '2022-05-09';

The correct query to solve this step:

SELECT \* FROM

log\_in\_attempts

WHERE login\_date > '2022-05-09';

Copied!

content\_copy

How many login attempts were made after 2022-05-09?

134

185

111

check125

Submit

**Answer**: The number of login attempts made after the 2022-05-09 is 125.

**Now**, based on your first query, you find a need to expand the date range to include 2022-05-09 in your search.

1. Complete the SQL query to retrieve data for login attempts that were made on or after '2022-05-09'. Replace X with the correct operator:

SELECT \*

FROM log\_in\_attempts

WHERE login\_date X '2022-05-09';

The correct query to solve this step:

SELECT \*

FROM log\_in\_attempts

WHERE login\_date >= '2022-05-09';

Copied!

content\_copy

How many login attempts were made on or after 2022-05-09?

check165

190

143

186

Submit

**Answer**: The number of login attempts made from 2022-05-09 onward is 165.

Click **Check my progress** to verify that you have completed this task correctly.

You have completed this task and returned the necessary login attempts.To achieve this, you filtered the data in the log\_in\_attempts table by login date (login\_date).

Retrieve login attempts after a certain date

Check my progress

*You have completed this task and returned the necessary login attempts.To achieve this, you filtered the data in the log\_in\_attempts table by login date (login\_date).*

**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. You must insert the required dates X and Y:

SELECT \*

FROM log\_in\_attempts

WHERE login\_date BETWEEN 'X' AND 'Y';

The correct query to solve this step:

SELECT \*

FROM log\_in\_attempts

WHERE login\_date BETWEEN '2022-05-09' AND '2022-05-11';

Copied!

content\_copy

How many login attempts were made between 2022-05-09 and 2022-05-11?

157

134

160

check123

Submit

**Answer**: 123 login attempts were made between 2022-05-09 and 2022-05-11.

Click **Check my progress** to verify that you have completed this task correctly.

You have completed this task and retrieved logins in a date range. You achieved this by using the correct operators in SQL to return results in a date range.

Retrieve logins in a date range

Check my progress

*You have completed this task and retrieved logins in a date range. You achieved this by using the correct operators in SQL to return results in a date range.*

**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'.

***Note:****Place time data in single quotation marks.*

The correct query to solve this step:

SELECT \*

FROM log\_in\_attempts

WHERE login\_time < '07:00:00';

Copied!

content\_copy

What is the username of the fifth record returned from this query?

jrafael

bisles

checkeraab

acook

Submit

**Answer**: The username in the fifth record returned from this query is eraab.

The query in the previous step returned more results than required.

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

The correct query to solve this step:

SELECT \*

FROM log\_in\_attempts

WHERE login\_time BETWEEN '06:00:00' AND '07:00:00';

Copied!

content\_copy

What time was the earliest login attempt between 06:00:00 and 07:00:00?

check06:01:31

06:04:34

06:15:41

06:03:41

Submit

**Answer**: The earliest login attempt was at 06:01:31.

Click **Check my progress** to verify that you have completed this task correctly.

You have completed this task and retrieved logins at certain times. You achieved this by using the correct operators in your filter.

Investigate logins at certain times

Check my progress

*You have completed this task and retrieved logins at certain times. You achieved this by using the correct operators in your filter.*

**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.

***Note:****The event\_id column contains numeric data; do not place numeric data in quotation marks.*

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

The correct query to solve this step:

SELECT event\_id, username, login\_date

FROM log\_in\_attempts

WHERE event\_id >= 100;

Copied!

content\_copy

What is the login date of the third result returned by your query?

2022-05-08

2022-05-10

check2022-05-09

2022-05-11

Submit

**Answer**: The login date of the third result returned is 2022-05-09.

The query in the previous step returned more data than required.

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

The correct query to solve this step:

SELECT event\_id, username, login\_date

FROM log\_in\_attempts

WHERE event\_id BETWEEN 100 AND 150;

Copied!

content\_copy

What is the username of the seventh result returned by your query?

bisles

gesparza

mabadi

checktmitchel

Submit

**Answer**: The username of the seventh result is tmitchel.

Click **Check my progress** to verify that you have completed this task correctly.

You have completed this task and filtered login attempts based on the event\_id field from the log\_in\_attempts table. You did this by writing a SQL query and modifying the query to return logins between certain parameters.

Investigate logins by event ID

Check my progress

*You have completed this task and filtered login attempts based on the event\_id field from the log\_in\_attempts table. You did this by writing a SQL query and modifying the query to return logins between certain parameters.*

**Conclusion**

Great work!

You 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, =, >, >=)

to filter data from a table.

You’re now ready to filter for numbers and dates to extract all sorts of useful data!