**Activity overview**

Previously, you learned how to use basic SQL queries to retrieve information from a database. You have also learned about using the ORDER BY keyword to sort data returned in an ascending or a descending order.

In this lab activity, you’ll use SELECT and FROM in SQL to return the information you need from a database. You’ll also use the ORDER BY keyword to sequence the information returned by a query based on a specified column.

It's important to know how to query information from a database because this is a common task you might encounter as a security analyst. You should know how to get the information you need to improve security and keep data safe.

With that in mind, it's time to explore the scenario.

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

**Scenario**

In this scenario, you have to determine which employee devices must be updated. You also need to investigate user login activity to explore if any unusual activity has occurred.

The information you need is located in the machines and login\_attempts tables in the organization database.

Here’s how you’ll do this task: **First**, you’ll obtain information on the employee devices that must be updated. **Next**, you’ll examine the login attempts for unusual activity. **Finally**, you’ll use the ORDER BY keyword to sort the data returned by your SQL queries.

OK, let’s get ready to practice running your very first SQL queries!

***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 employee device data**

In this task, you need to obtain information on employee devices because your team needs to update them. The information you need is in the machines table in the organization database.

**First**, you need to retrieve all the information about the employee devices.

1. Run the following query to select all device information from the machines table:

SELECT \*

FROM machines;

Copied!

content\_copy

***Note:****Using the asterisk (\*) returns all data from the specified table. Also, table names in MySQL are case-sensitive.*

The output returns all the contents of the machines table:

+--------------+------------------+----------------+---------------+-------------+

| device\_id | operating\_system | email\_client | OS\_patch\_date | employee\_id |

+--------------+------------------+----------------+---------------+-------------+

| a184b775c707 | OS 1 | Email Client 1 | 2021-09-01 | 1156 |

| a192b174c940 | OS 2 | Email Client 1 | 2021-06-01 | 1052 |

| a305b818c708 | OS 3 | Email Client 2 | 2021-06-01 | 1182 |

| a317b635c465 | OS 1 | Email Client 2 | 2021-03-01 | 1130 |

| a320b137c219 | OS 2 | Email Client 2 | 2021-03-01 | 1000 |

|... | | | | |

+--------------+------------------+----------------+---------------+-------------+

200 rows in set (0.356 sec)

**Next**, you want to focus on the email client running on various devices.

1. Run the following query to select only the device\_id and email\_client columns from the machines table. Replace X with device\_id and Y with email\_client:

SELECT X, Y FROM machines;

The correct query to solve this step:

SELECT device\_id, email\_client

FROM machines;

Copied!

content\_copy

The output should return only the selected columns of the machines table:

+--------------+----------------+

| device\_id | email\_client |

+--------------+----------------+

| a184b775c707 | Email Client 1 |

| a192b174c940 | Email Client 1 |

| a305b818c708 | Email Client 2 |

| a317b635c465 | Email Client 2 |

| a320b137c219 | Email Client 2 |

|... | |

+--------------+----------------+

200 rows in set (0.015 sec)

What email client is returned in the third row?

Email Client 4

Email Client 3

checkEmail Client 2

Email Client 1

Submit

**Answer**: The email client returned in the third row is Email Client 2.

**Now**, you need information on the operating systems used on various devices and their last patch date.

1. Complete the query to return only the device\_id, operating\_system, and OS\_patch\_date columns from the machines table. Replace X, Y, and Z with the columns that you need to return:

SELECT X, Y, Z FROM machines;

The correct query to solve this step:

SELECT device\_id, operating\_system, OS\_patch\_date

FROM machines;

Copied!

content\_copy

What is the patch date of the first entry?

2021-06-01

2021-03-01

2021-12-01

check2021-09-01

Submit

**Answer**: The patch date of the first entry is 2021-09-01.

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

You have completed this task and retrieved the needed information from the machines table.

Retrieve employee device data

Check my progress

*You have completed this task and retrieved the needed information from the machines table.*

**Task 2. Investigate login activity**

In this task, you need to analyze the information from the log\_in\_attempts table to determine if any unusual activity has occurred.

**First**, you need to investigate the locations where login attempts were made to ensure that they’re in expected areas (the United States, Canada, or Mexico).

1. Write a SQL query to select the event\_id and country columns from the log\_in\_attempts table.

The correct query to solve this step:

SELECT event\_id, country

FROM log\_in\_attempts;

Copied!

content\_copy

Were any login attempts made from Australia?

Yes

checkNo

Submit

**Answer**: No. Login attempts were not made from Australia.

**Next**, you need to check if login attempts were made outside of the organization's working hours.

1. Write a SQL query that selects the username, login\_date, and login\_time columns from the log\_in\_attempts table.

The correct query to solve this step:

SELECT username, login\_date, login\_time

FROM log\_in\_attempts;

Copied!

content\_copy

What username is returned in the fifth row?

checkjrafael

mrah

dkot

apatel

Submit

**Answer**: The username returned in the fifth row is jrafael.

**Now**, you need to get a complete picture of all login attempts.

1. Write a SQL query that selects all columns from the log\_in\_attempts table, using a single symbol after the SELECT keyword.

The correct query to solve this step:

SELECT \*

FROM log\_in\_attempts;

Copied!

content\_copy

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

You have completed this task and retrieved the needed information from the log\_in\_attempts table.

Investigate login activity

Check my progress

*You have completed this task and retrieved the needed information from the log\_in\_attempts table.*

**Task 3. Order login attempts data**

In this task, you need to use the ORDER BY keyword. You'll sequence the data that your query returns according to the login date and time.

**First**, you need to sort the information by date.

1. Run the following query, which orders log\_in\_attempts data by login\_date:

SELECT \*

FROM log\_in\_attempts

ORDER BY login\_date;

Copied!

content\_copy

What are the username and login date of the first record returned?

mabadi on 2022-05-10

checkivelasco on 2022-05-08

sbaelish on 2022-05-10

daquino on 2022-05-08

Submit

**Answer**: The first record returned contains a username of ivelasco and a login date of 2022-05-08.

**Now**, you need to further organize the previous results by ordering them by login\_time.

1. Modify the query from the previous step by adding the login time to the ORDER BY clause. You must replace X with the appropriate column name:

SELECT \*

FROM log\_in\_attempts

ORDER BY login\_date, X;

The correct query to solve this step:

SELECT \*

FROM log\_in\_attempts

ORDER BY login\_date, login\_time;

Copied!

content\_copy

What are the username and login time of the first record returned by the above query?

wjaffrey at 00:15:55

gesparza at 00:40:00

pwashing at 00:36:12

checkbsand at 00:19:11

Submit

**Answer**: The first record returned contains a username of bsand and a login time of 00:19:11.

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

You have completed this task and used the ORDER BY keyword to sort the data returned from the log\_in\_attempts table.

Order login attempts data

Check my progress

*You have completed this task and used the ORDER BY keyword to sort the data returned from the log\_in\_attempts table.*

**Conclusion**

Great work!

You have completed this activity, and you now have practical experience in running basic SQL queries to

* select specific columns from a table,
* select all columns from a table by using an asterisk (\*), and
* sort query results using the ORDER BY keyword.

These basic queries form the foundation for running more advanced queries and applying filters later.