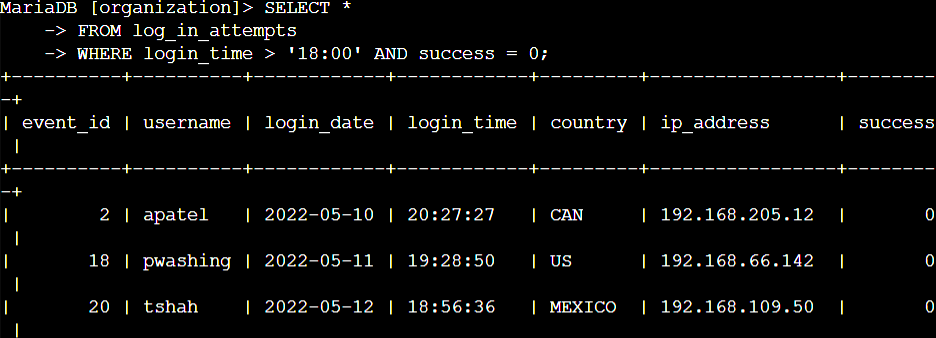
# Apply filters to SQL queries

## Project description

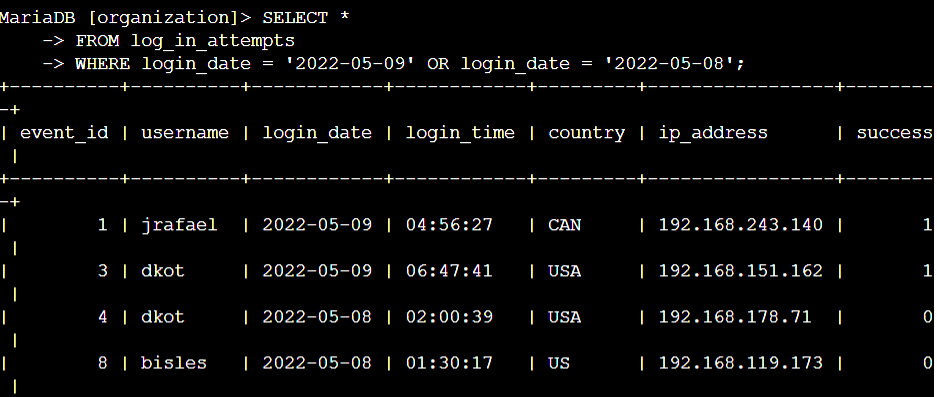
In this scenario, a potential security incident might have occurred in the organization after business hours. My role is to investigate this incident by analyzing data from two tables, “log\_in-attempts” and “employees”. By using SQL queries, I am to filter the data and retrieve relevant data such as after-hours login attempts, login attempts on specific dates, login attempts outside of a specified country and details of employees based on their department and location.

## Retrieve after hours failed login attempts

To examine potential security incidents that occurred outside of regular business hours, I will apply SQL filters to the “log\_in\_attempts” table. Specifically, I’ll retrieve all entries related to unsuccessful login attempts that happened after 18:00 (6:00 PM).The first part of the screenshot is my query, and the second part is a portion of the output.

This query filters for login attempts that failed and occurred after 6:00 PM. First, I selected all data from the log\_in\_attempts table. Then, I used a WHERE clause with an AND operator to show only login attempts that happened after 6:00 PM and were unsuccessful. The first condition, login\_time > '18:00', filters for attempts after 6:00 PM. The second condition, success = 0, filters for attempts that failed.

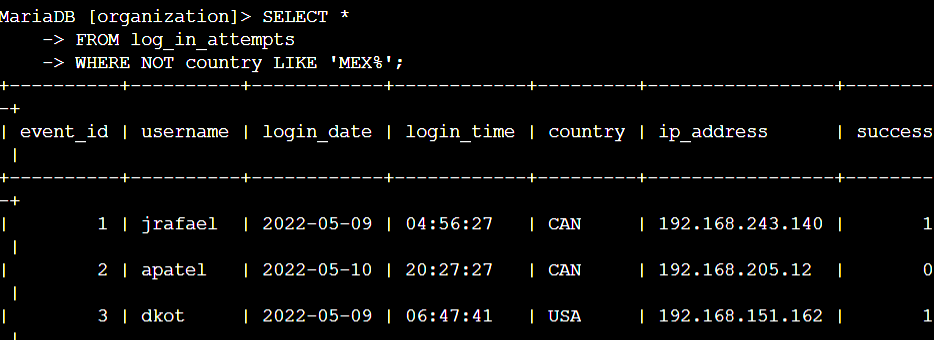
## Retrieve login attempts on specific dates

To investigate a specific event, I will query the "log\_in\_attempts" table to retrieve login attempts that occurred on 2022-05-09 or 2022-05-08

This query retrieves all login attempts that occurred on either 2022-05-09 or on 2022-05-08. I began by selecting all data from the log\_in\_attempts table. Then, I used a WHERE clause with an OR operator to filter the results. The first condition is login\_date = '2022-05-09', which filters for logins on 2022-05-09. The second condition is login\_date = '2022-05-08', which filters for logins on 2022-05-08.

## Retrieve login attempts outside of Mexico

To retrieve suspicious login attempts that occurred outside of Mexico, I will use SQL filters to retrieve records from the "log\_in\_attempts" table where the country is not Mexico.

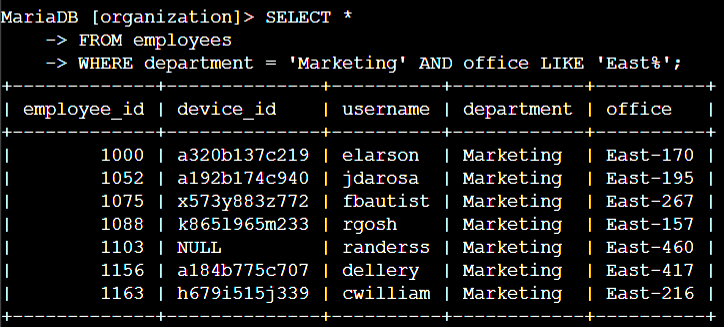


This query retrieves all login attempts that occurred in countries except Mexico. I began by selecting all data from the log\_in\_attempts table. Then, I used a WHERE clause with NOT to filter out countries other than Mexico. I used LIKE with the pattern 'MEX%' to match both 'MEX' and 'MEXICO', as the dataset represents Mexico in different formats. The percentage sign (%) in LIKE represents any number of unspecified characters.

## Retrieve employees in Marketing

My team wants to update the computers for certain employees in the Marketing department. To do this, I have to get information on which employee machines to update.

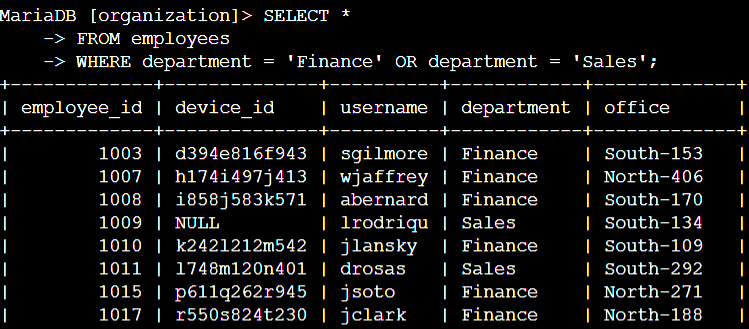
To gather information about employees in the Marketing department located in the East building, I will query the "employees" table and apply SQL filters.



I began by selecting all data from the employees table. Then, I used a WHERE clause with AND to filter for employees working in the Marketing department and situated in offices within the East building. To match the office location, I used LIKE with 'East%' as the pattern because the office column specifies the East building with various office numbers. The first condition, department = 'Marketing', filters for Marketing department employees. The second condition, office LIKE 'East%', filters for employees based in the East building.

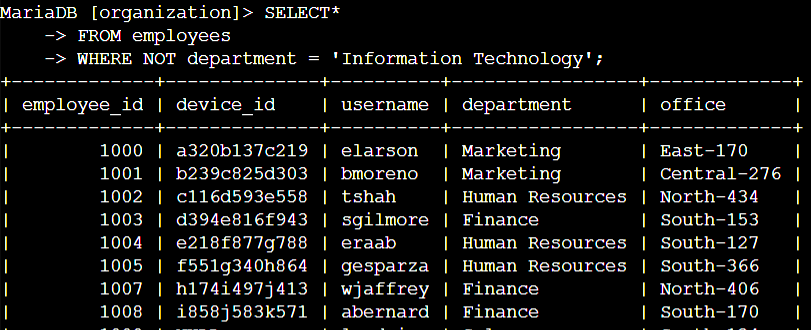
## Retrieve employees in Finance or Sales

The machines for employees in the Finance and Sales departments also need to be updated. Since a different security update is needed, I have to get information on employees only from these two departments.To identify the employees in the Finance or Sales departments, I will query the "employees" table using SQL filters.

Initially, I selected all data from the employees table. Using a WHERE clause with OR, I filtered for employees in either the Finance or Sales departments. I used the OR operator instead of AND to include all employees from either department. The first condition, department = 'Finance', selects employees from the Finance department. The second condition, department = 'Sales', selects employees from the Sales department.

## Retrieve all employees not in IT

My team needs to make one more security update on employees who are not in the Information Technology department. To make the update, I first have to get information on these employees.To get all employees not belonging to the IT department, I will query the "employees" table using SQL filters.



First, I started by selecting all the data from the employees table. Then, I used a WHERE clause with NOT to filter for employees not in this department. Thus getting all the employees who are not from the information technology department.

## Summary

Using SQL queries, I've thoroughly investigated potential security concerns such as after-hours login attempts, suspicious logins on specific dates, logins from outside Mexico, and employee details based on department and location. These queries helped improve organizational security by identifying and addressing potential vulnerabilities and risks.