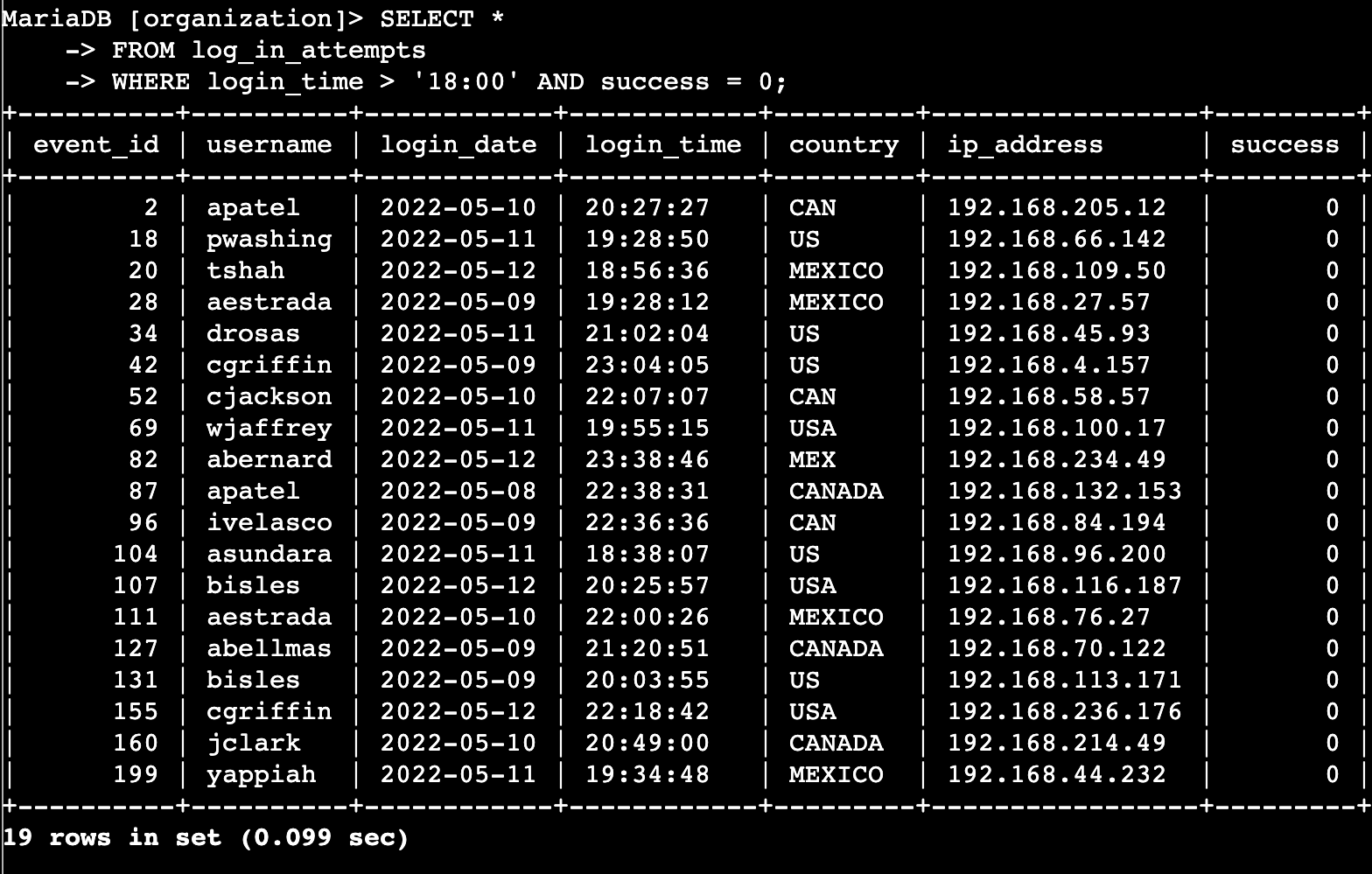
# Apply filters to SQL queries

## Project description

In this project I am using SQL in order to investigate some potential security issues that were recently uncovered. These potential issues involve login attempts and employee machines so I will use SQL filters to retrieve records from different datasets.

## Retrieve after hours failed login attempts

Since the potential security incident occurred after hours (which is 18:00) I used the query below to find all the failed login attempts after 18:00. Since this system recognizes a successful login attempt as 1 and a failed login attempt at 0, I searched the login attempts table to find all the failed login times that occurred after 18:00. Since I needed the login time to be after 18:00 and I only wanted to see the failed login attempts, I used the AND filter to make sure the query would only show me data from the login attempts table where both were true.



## Retrieve login attempts on specific dates

For this query I needed to investigate a suspicious event that occurred on 2022-05-09 and 2022-05-08. Since I needed to see all login attempts on both these dates I utilized the OR filter in the below query to show me all the login attempts made on both those dates. I also made sure to write login date before inserting the value of each date to ensure it would only show me data where login date was equal to either of the values I entered.

## 

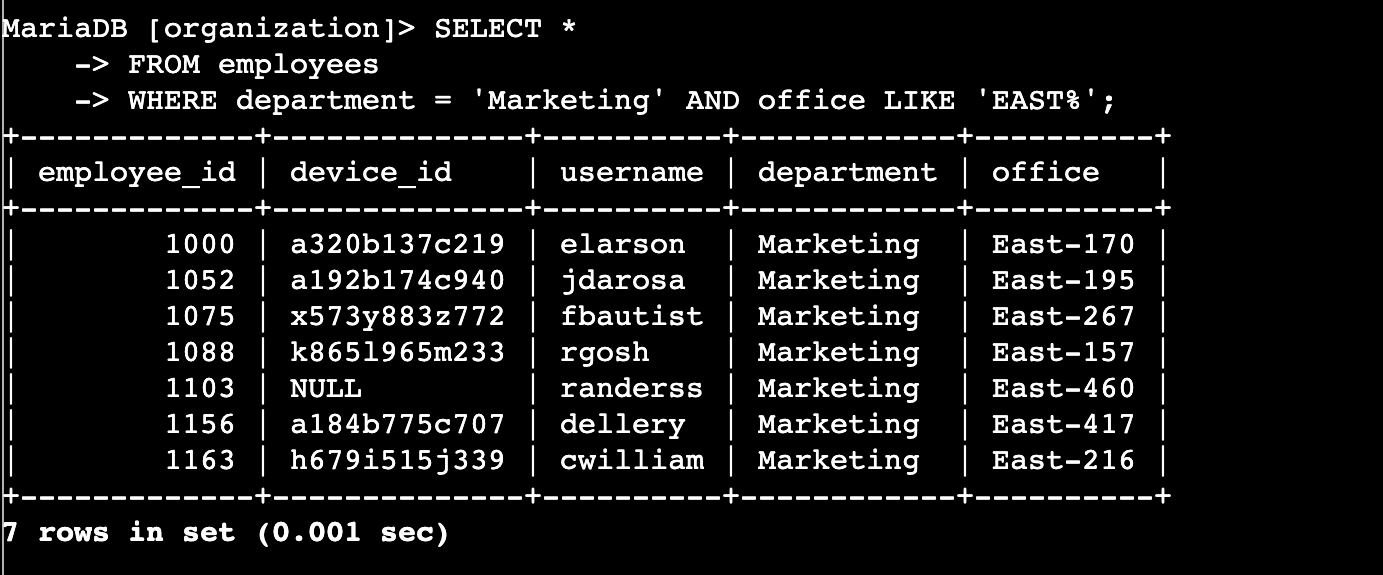
## Retrieve login attempts outside of Mexico

In this query I needed to see all the login attempts that didn’t occur in Mexico because the security team had determined that the suspicious activity didn’t originate in Mexico. I used the below query to see all login attempts outside of Mexico by using the NOT filter. The NOT filter will show me all other values that are don’t fit the criteria of the value I enter. I also had to use the LIKE operator since this company utilizes MEX or MEXICO in the country column to represent Mexico. To ensure I include both of these I typed in ‘MEX%’ so that the query wouldn’t show me anything in the country column that started with “MEX”.

## 

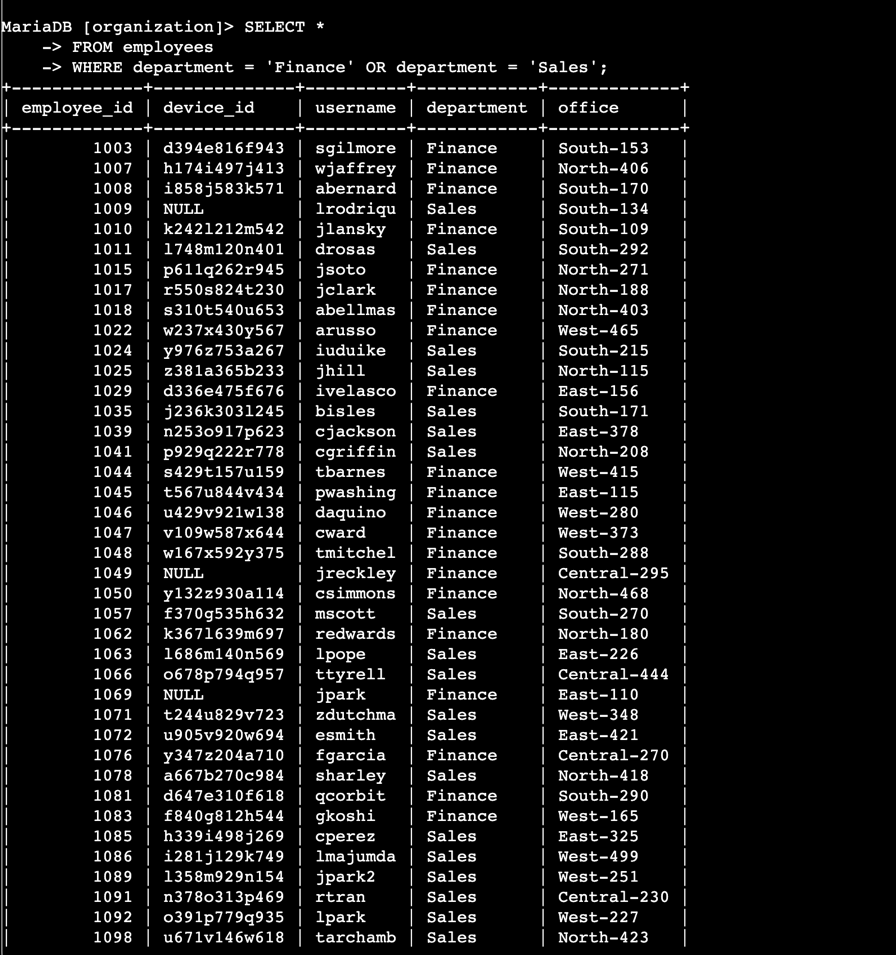
## Retrieve employees in Marketing

In this query I was tasked with finding out all the employees in the Marketing department that work in the East building. The security team wanted to perform security updates on their machines. Since we only needed to update the machines of these people I needed to enter a query that would show me only those employees. By using the AND filter I was able to have the query show me data from the employee table where the department value was only “Marketing” and the office value was only for the East building. Since this company writes office building locations as “East-xxx” or “North-xxx” I used the LIKE operator as well to type in “EAST%” so that the office value would return anything starting with “EAST”.



## Retrieve employees in Finance or Sales

In this query I needed to find information on all the employees in the Sales and Finance department so the security team could update their machines. In the below query I used the OR function so that it would return me data from the employee table where the department value was either Sales or Finance. I didn’t use AND because that would mean the employee would have to work in Sales and Finance. Using OR and making sure to put department for both ensures that the query returns data where the department value is equal to either one.



## Retrieve all employees not in IT

In this final query the security team needed to make an update for all the employees outside the IT department. Since this company only lists IT as “Information Technology” I used that as the value for department. Instead of typing all the other departments I just used the NOT filter so that the employee data table would only give me data on employees where their department value did not equal “Information Technology”.

## 

## Summary

In summary, I utilized different filters in these SQL queries to get specific information on employee machines and login attempts. Using the log\_in\_attempts and employees table as well as AND, OR, and NOT filters I was able to retrieve the information needed. I also used the LIKE operator and % to uncover the desired information.