# Apply filters to SQL queries

## Project description

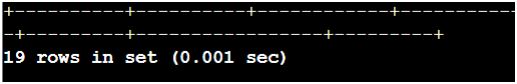
As a security analyst, it is my job to analyze data. In terms of data-related tasks, SQL is the most efficient tool that I can able to use, especially for huge chunks of data. The data obtained came from specific information about employees, the machines they are using, and the departments they belong to. All of these information are stored in a database. To identify specific information needed during the investigation, I need to filter the database by utilizing SQL queries.

## Retrieve after hours failed login attempts

To identify all uncsuccessful attempts after 6:00 p.m., I utilized the SQL query below. This is to further investigate failed login attempts that we made after the said business hour above.



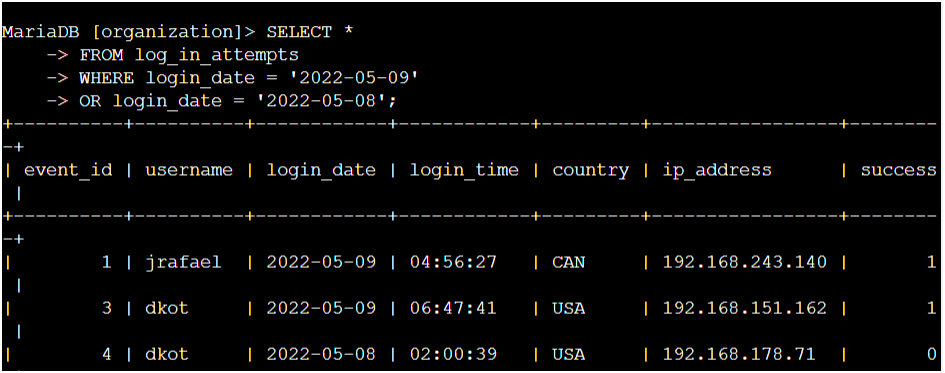
I selected all columns in the table name log\_in\_attempts by using **SELECT** and **FROM** commands. For a more specified filtering information, I used the **WHERE** clause to indicate that the needed information by the team are the failed log-in attempts, specified by the clause **‘success = FALSE’** or number 0, done before **6:00 p.m**.

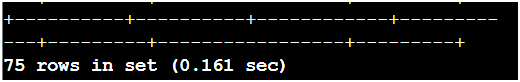


Based on the output, there was 19 failed login attempts occurred after 6:00 p.m.

## Retrieve login attempts on specific dates

The team is investigating a suspicious event that occurred on ‘2022-05-09’. To retrieve all login attempts that occurred on this day and the day before ‘2022-05-08’. I selected all columns FROM log\_in\_attempts table, where the login\_date is either ‘2022-05-09’ or ‘2022-05-08’ using the SQL query below.

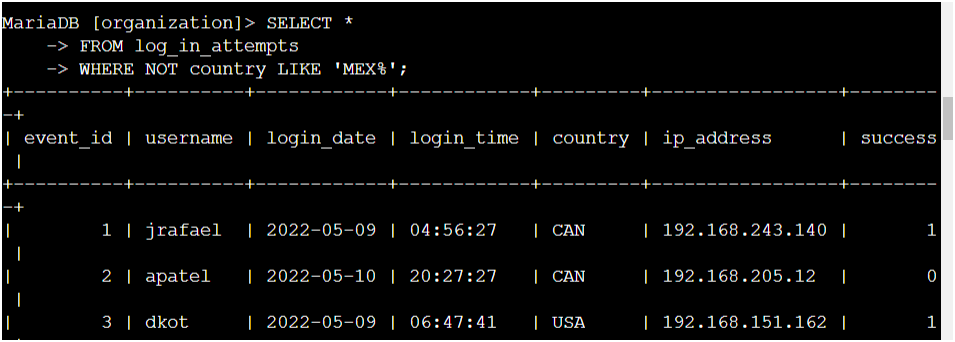


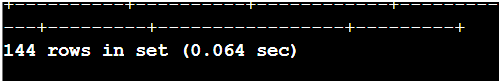


Based on the output above, there were 75 login attempts made on those days.

## Retrieve login attempts outside of Mexico

The team also investigated logins that did not originate in Mexico. To retrieve those information, I used the SQL query below.

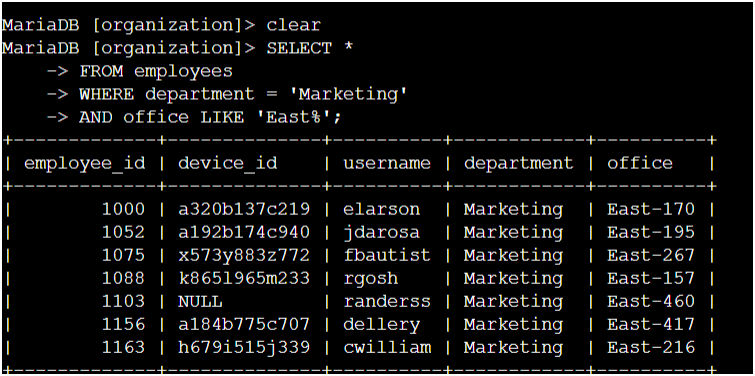




Based on the output above, there were 144 login attempts made outside of Mexico.

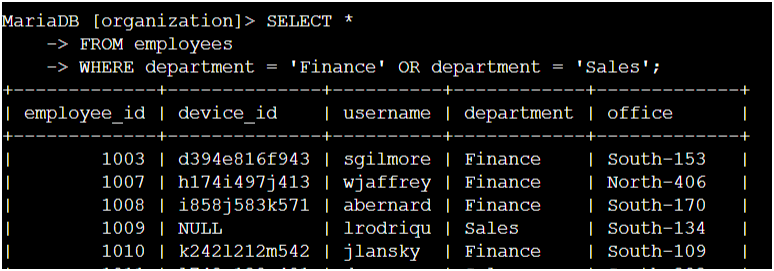
## Retrieve employees in Marketing

The team needs to update employee machines, and the information from employees in the Marketing department located at East buildings will be needed.



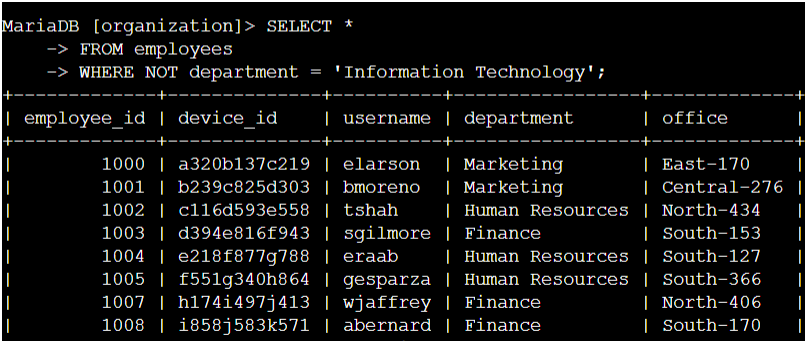
## Retrieve employees in Finance or Sales

To perform a different update to the computers of all employees in the Finance or the Sales department, the information about those employees need to be located. To do that, I utilized the SQL query below. I used the OR operation to indicate that the department where the employee belongs should be either in Finance or Sales.



## Retrieve all employees not in IT

The team needs to make on more update. Since the update was already made to employee computers in the Information Technology department, the team needs information about employees who are not in that department. To do that, I include a NOT operation before the department variable in the WHERE clause. I utilized the SQL query below.





The output shows that there are 161 employees that are not in the Information Technology department.

## Summary

I was able to gain practical experience in using SQL to run SQL queries to retrieve information from a database, and apply AND, OR, and NOT operators to filter SQL queries.