# Apply filters to SQL queries

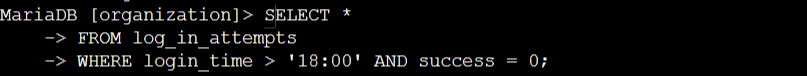
## Project description

The organization that I am working at is currently experiencing security issues involving the login attempts and the employee machines. Using SQL I will be examining organizations employee and log\_in\_attempts tables to retrieve relevant records and investigate the potential security issues within the organization’s databases.

I will be using SQL filtering tools such as AND, OR and NOT to complete this project.

## Retrieve after hours failed login attempts

To begin this investigation our team will be investigating failed login attempts that were made after office hours end, which is at 18:00.



To look at all columns we will be using SELECT \* which is a prefix for all columns. We are looking at the login\_in\_attempts table and using the conditions WHERE login\_time > '18:00' AND success = 0; . The AND operator allows us to filter data to show us all records that meet both conditions, which in this case is login times after 18:00 and all values in the success column that are 0 which means unsuccessful.

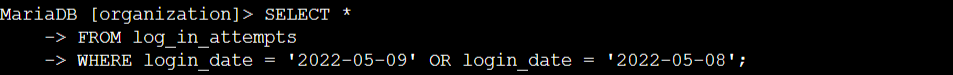


In this case 19 unsuccessful log in attempts were made after office hours.

## Retrieve login attempts on specific dates

Our team would also like to investigate suspicious events that occurred on 2022-05-09, we also want to retrieve login attempts that occurred the day before this too, 2022-05-08. To do this we will be looking at the log-in-attempts table, and using the OR filter to find all attempts made from those 2 dates.

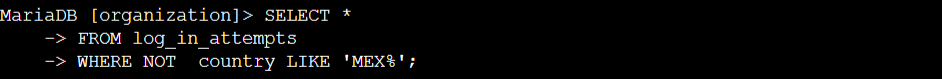
The OR operator connects both conditions and returns results where the first condition, the second condition, or both are met. 75 records were returned.





## Retrieve login attempts outside of Mexico

It was determined that the suspicious activity with login attempts didn’t originate in Mexico therefore we are going to look at all login attempts that did not come from Mexico. To do this, I will be using the NOT operator which negates conditions. This means that SQL returns all records that don’t match the condition specified in the query.



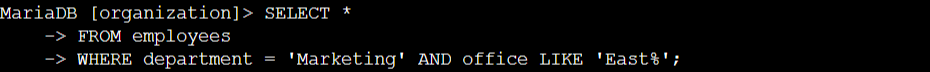
LIKE ‘MEX%’ was to select all records with a country that start with MEX. The data within country had ‘MEXICO’ and ‘MEX’ therefore the LIKE was needed to prevent the SQL query from being unnecessarily complicated.



144 login attempts were found that were not in Mexico.

## Retrieve employees in Marketing

Our team wanted to perform security updates on specific employee machines in the marketing department and specifically in the East offices.



Using the AND operator and the LIKE to specify all offices starting with East.

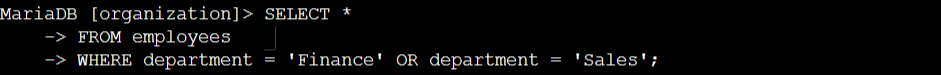
A screen shot of a computer

Description automatically generated

7 employees were found that matched our SQL query.

## Retrieve employees in Finance or Sales

Similar to before our team wanted to also perform a security update on machines for employees in the Sales and Finance departments.



Using the OR operator we can return all records that meet the Finance department condition or the Sales department condition or both.

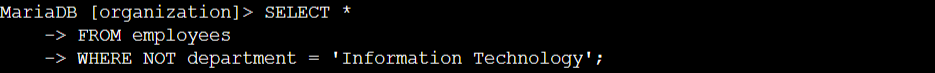
A black screen with white text

Description automatically generated



71 records were found that met that query.

## Retrieve all employees not in IT

The last update our team made separated the employees from the Information technology department from the other departments because the Information Technology department already had their security update completed. 

The Not operator was used to negate the condition and not return any records from the Information Technology department.



## Summary

In this project, I used SQL filtering tools (AND, OR, NOT) to investigate security issues in the organization’s databases. Key findings include:

* 19 failed login attempts occurred after office hours.
* 75 login attempts were identified on 2022-05-08 and 2022-05-09.
* 144 login attempts originated outside of Mexico.
* 7 employees in the Marketing department (East offices) were identified for security updates.
* 71 employees in the Finance or Sales departments required updates.
* Employees in IT were excluded, as their updates were already completed.