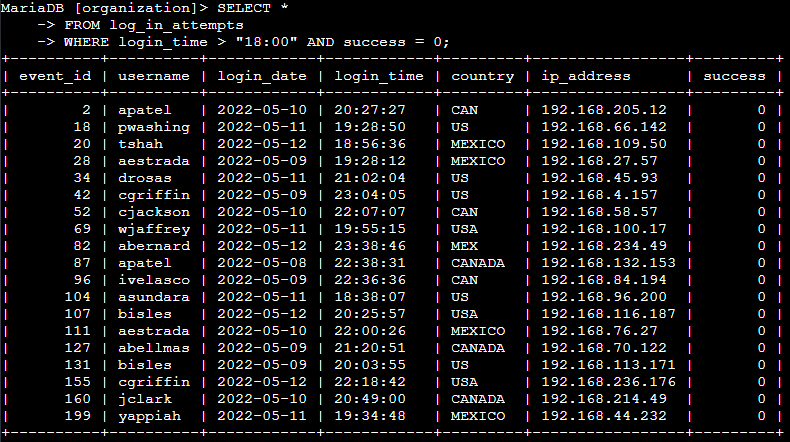
# Apply filters to SQL queries

## Project description

The goal of this project is to investigate security issues to keep this organization’s system secure. For that, we are going to use SQL to look up some potential security issues that involve login attempts and employee machines. Using SQL will allow us to check on all the tables the company has and search through them to investigate potential security issues.

## Retrieve after hours failed login attempts

We recently discovered a potential security incident that occurred after business hours. So, we are going to check on the log\_in\_attempts table to review all the activity.



We select all the data with \*, and we want to extract this data from a specific table called log\_in\_attempts. Then, we have to specify that we want login attempts after 18:00 using login\_time > “18:00” and the attempts that were unsuccessful using success = 0 or FALSE. We use the operator AND to add another function to the query.

## Retrieve login attempts on specific dates

A suspicious event took place on 2022-05-09, for this we want to review all login attempts which occurred on this and the day before.



In order to investigate this, we need to select all the data with SELECT \*. Then, we put FROM log\_in\_attempts because that’s the table we want to use. Finally, to get specific data we want to know what happened with logins, so we add login\_date = “2022-05-09” to know what attempts happened in this day, and we add login\_date = “2022-05-08” to get the data from the day before. In this case we use OR to reach information of this two specific days.

## Retrieve login attempts outside of Mexico

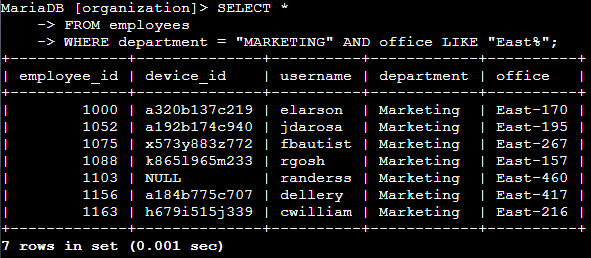
Now we want to retrieve data from the logins outside of Mexico, because the team has determined that this suspicious activity doesn’t come from Mexico.



In this one, the parts of SELECT and FROM stay the same because we are using the same operator for the same things but the conditions change. We want to know about the attempts that had been occurring outside Mexico, so we put WHERE NOT country LIKE “MEX%”; NOT to exclude Mexico from the query, country to specify we want to exclude this country, LIKE to extract from the table the values that have something to do with Mexico, and “MEX%” to find all the concepts alike Mexico.

## Retrieve employees in Marketing

Our team wants to perform security updates on specific employee machines in the Marketing department, so for this we are going to continue using SQL to extract that info.



In this case we use SELECT \* to select all the data. We use FROM employees because now we want to search through the employees table. Now, with the query of WHERE department = “MARKETING”, we are trying to find marketing employees and with AND office LIKE “East%” we specify that we are looking for employees on the offices of the East side. We use AND to add another function to the query.

## Retrieve employees in Finance or Sales

Apart from the marketing employees, now we want to retrieve sales and finance staff, to have an update on machines for them.



As we continue using the same SELECT and FROM operators, we may change the following one because our goal is to extract finance or sales data. In the operator of WHERE we specify the department of sales with department = “SALES” and we do the exact same thing with the finance one. We use OR to include one or the other one.

## Retrieve all employees not in IT

Our team need to make one more update to employee machines, but as the IT department already has this update we have to find the ones that don’t.



For this, we need to exclude the department of Information Technology using the NOT operator. It follows with department = “INFORMATION TECHNOLOGY”; to let the machine know that we are excluding that department.

## Summary

So, to sum up, our currently completed tasks are the following ones: we have been checking failed login attempts after hours, on specific dates and outside of Mexico. We retrieved employees in Marketing, Sales and Finance to look for un updated machines and we checked that the IT department was updated so we looked for the departments that weren’t updated.