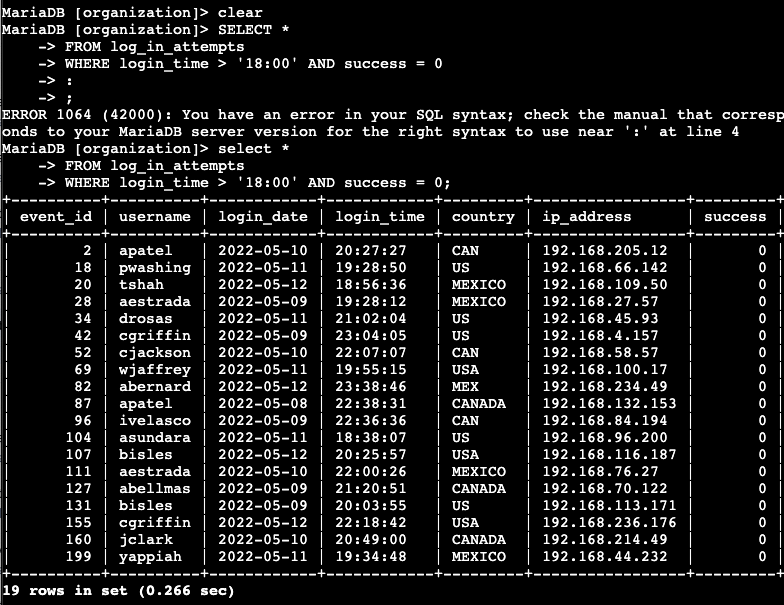
# Apply filters to SQL queries

## Project description

In this project I acted as a security professional investigating potential security issues within an organization. I focused on suspicious login activity and employee machine data by analyzing the log\_in\_attempts and employee tables. Using SQL, I applied filters such as AND, OR, NOT, and LIKE to retrieve targeted records that revealed failed logins, activity outside of work hours, non-local access, and department specific data. This process helped identify users or machines that may pose a security risk and supported the team’s efforts to take preventive actions.

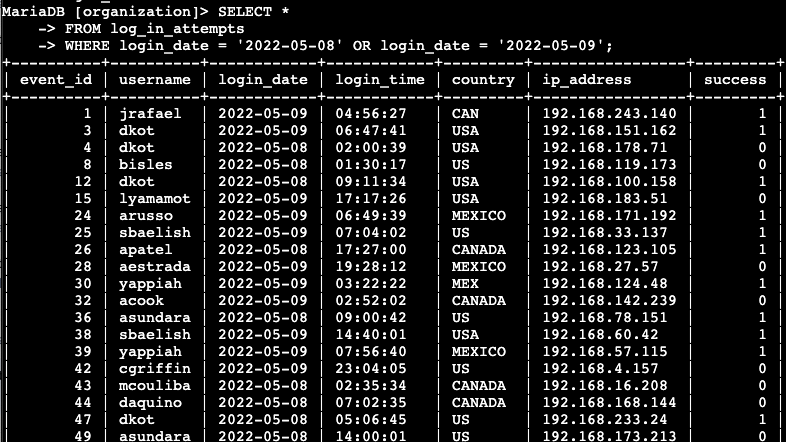
## Retrieve after hours failed login attempts

* The task is to find all failed login attempts that happened after 18:00
  + I’m retrieving ALL columns SELECT \*
  + FROM log\_in\_attempts table
  + I’m filtering using the WHERE login\_time is > than ’18:00’
  + AND success = 0
  + The “success = 0 is used to filter for failed login attempts, 0 indicates failure in the success column and 1 represents true success in the login attempts.
* Based on the results, there were a total of 19 failed login attempts after 18:00



## Retrieve login attempts on specific dates

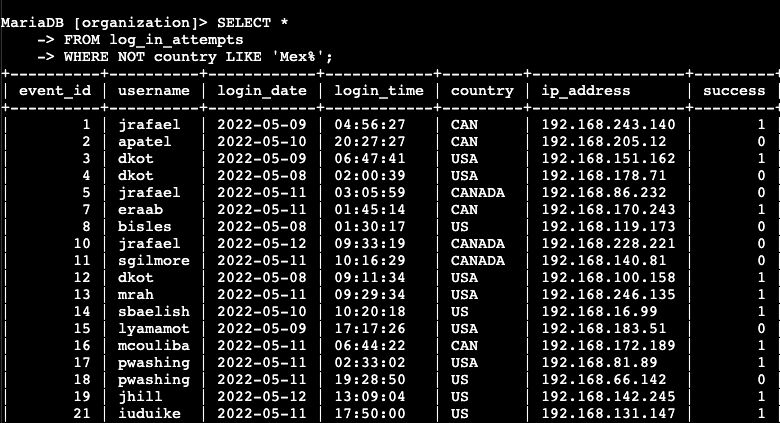
* A suspicious event occurred on 2022-05-09 and I’m tasked to investigate. I also want to include the day before 2022-05-08 to see what led up to it.
  + I’m retrieving ALL columns SELECT \*
  + FROM log\_in\_attempts
  + WHERE login\_date = ‘2022-05-08’ OR login\_date = ‘2022-05-09’;
* Based on the results there were a total of 75 attempts that were made on 8 May, 2022 and May 9, 2022.





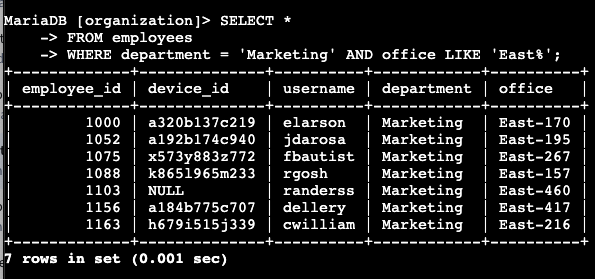
## Retrieve login attempts outside of Mexico

* The next task is to retrieve all login attempts that did NOT originate from Mexico however, based on results for country, we get both Mexico and Mex for country.
  + I retrieved all columns SELECT \*
  + FROM log\_in\_attempts
  + WHERE NOT country LIKE ‘Mex%’;
* When filtering WHERE I used the operator NOT to remove any results with Mexico as the country. This allowed me to capture all login attempts that originated outside of Mexico.
* I also used the LIKE operator with first three letters of Mexico followed by wildcard % to remove any results with the words Mexico or Mex (‘Mex%’).
* There was a total of 144 attempts that were made outside of Mexico.



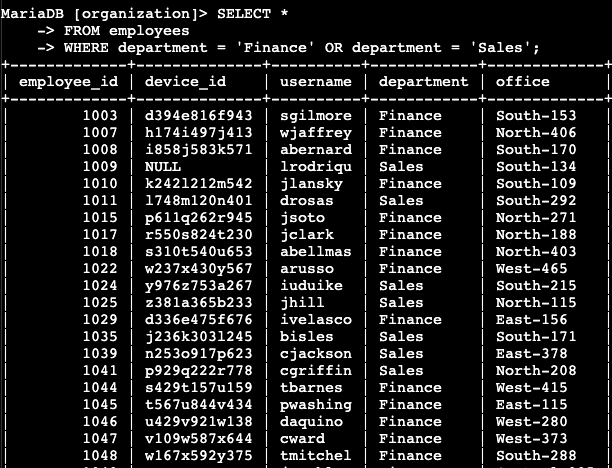
## Retrieve employees in Marketing

* The next task is to perform security updates on specific employee machines. The task is to retrieve information on employees who work in the marketing department and that are located in any office within the East building
  + I’m retrieving all columns SELECT \*
  + FROM employees table
  + WHERE department = ‘Marketing’ AND office LIKE ‘East%’;
  + Dsf
* Retrieved all columns from the employees table and filtered using the marketing department. I also used the operator AND to add an additional filter along with a secondary operator LIKE to retrieve data for office that began with East and a wildcard % to retrieve all the offices that started with East followed by any number.
* We have a total of 7 employees that belong to the Marketing department and are located in any office within the East building.



## Retrieve employees in Finance or Sales

* The next task is to perform security updates on machines for employees in the Sales and Finance departments.
  + I’m retrieving all SELECT \*
  + FROM employees table
  + WHERE department = ‘Finance’ OR department = ‘Sales’;
* I retrieved all columns from the employees table. I then filtered through departments equal to Finance OR operator Sales department. As I want either Finance or Sales or both to show on the results.
* There are 71 total employees that need the security update on their machines.





## Retrieve all employees not in IT

* The last task is to conduct more updates on employee machines. The task is to identify employees not in the Information Technology department so the team can perform security updates.
  + I retrieved all columns SELECT \*
  + FROM employees
  + WHERE NOT department = ‘Information Technology’;
* I selected all columns from the employees table. I then filtered by department but also used the operator NOT to exclude those in the Information Technology department since those machines have already been updated.
* There are a total of 161 total machines that need to be updated and this excludes those in the Information Technology department.

## 

## Summary

To summarize this activity, I analyzed the organizations log\_in\_attempts and employees table to investigate potential security issues. I applied SQL filters such as AND, OR, NOT, and LIKE to retrieve records that revealed failed login attempts, after-hours activity, non-local access, and machines requiring updates. These tasks completed supported efforts to reduce organizational risk and strengthen the overall security posture.