# Apply filters to SQL queries

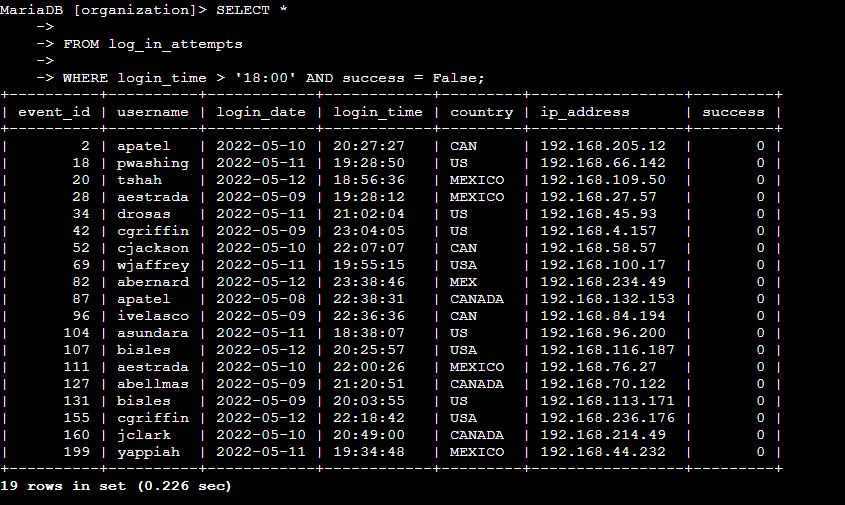
## **Project description**

As a security professional at an IT organization. Part of my job is to investigate security issues to help keep the system secure. I have recently discovered some potential security issues that involve login attempts and employee machines. The following steps provide examples of how I used SQL with filters to perform security-related tasks.

## **Retrieve after hours failed login attempts**

## I have discovered that there was a potential security incident after business hours (after 18:00). We need to investigate all after hours login attempts.

I created a SQL query to filter for failed login attempts that occurred after business hours as below:

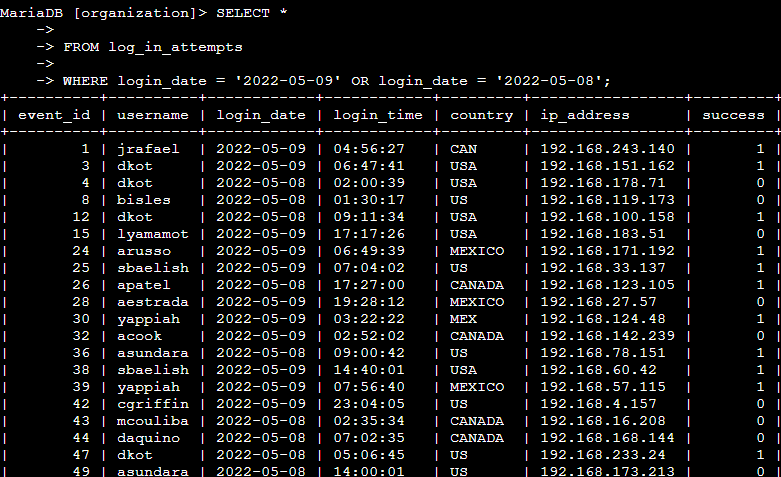


I started by selecting all data from the log\_in\_attempts table. Then, I used a WHERE clause with an AND operator to filter my results to output only login attempts that occurred after 18:00 and failed.

## **Retrieve login attempts on specific dates**

We discovered that a suspicious event occurred on 2022-05-09. I need to investigate all login activity that occurred on the day and the day before.

I created a SQL query to filter for login attempts that occurred on the specific dates.



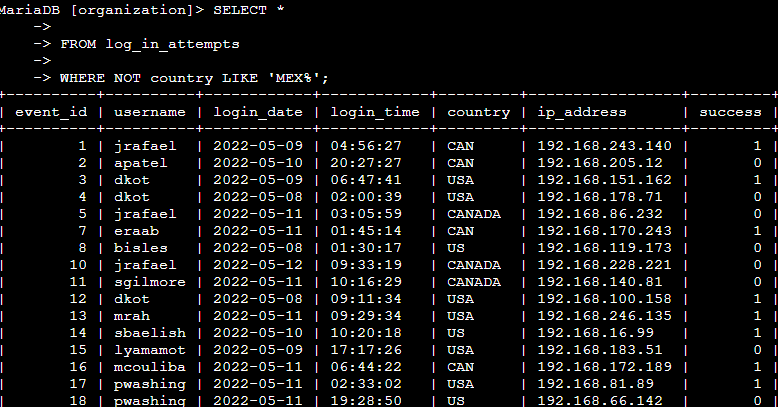
I started by using a SELECT statement to retrieve all data from the log\_in\_attempts table. Then, I used a WHERE clause with an OR operator to filter my results to output only login attempts that occurred on either 2022-05-09 or 2022-05-08.

## **Retrieve login attempts outside of Mexico**

After investigating the organization’s data on login attempts, I believe there is an issue with the login attempts that occurred outside of Mexico. These login attempts should be investigated.

I discovered from investigating the login attempts that the suspicious activity didn’t originate in Mexico. Therefore, I need to investigate login attempts that occurred outside of Mexico.

I created a SQL query to filter for login attempts that occurred outside of Mexico.

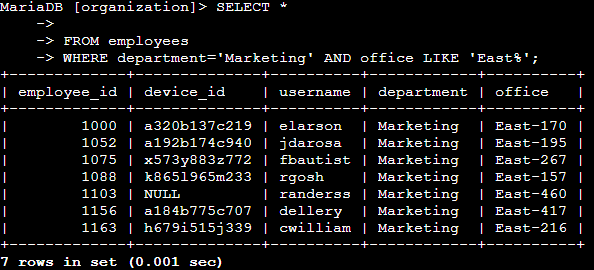


I started by using a SELECT statement to retrieve all data from the log\_in\_attempts table. Then, I used a WHERE clause with NOT to filter for countries other than Mexico. I used LIKE with MEX% as the pattern to match because the dataset represents Mexico as MEX and MEXICO. The percentage sign (%) represents any number of unspecified characters when used with LIKE.

## **Retrieve employees in Marketing**

We would like to perform security updates on specific employee machines in the Marketing department. We must retrieve information on which employee machines to update.

I created a SQL query to filter for employee machines from employees in the Marketing department in the East building.

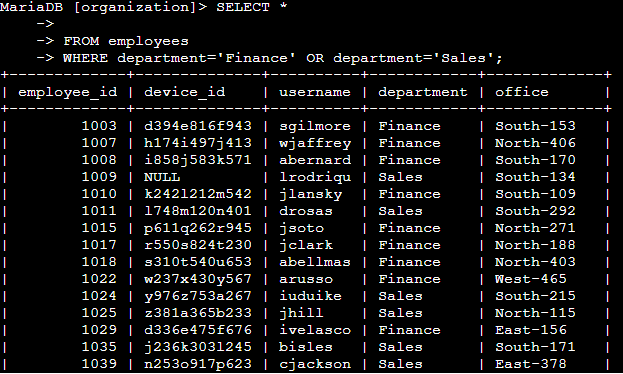


I started by using a SELECT statement to retrieve all data from the employees table. Then, I used a WHERE clause with AND to filter for employees who work in marketing and in the East building. The pattern office LIKE 'East%' filters for employees in the East building.

## **Retrieve employees in Finance or Sales**

We would like also to update the machines for employees in the Finance and Sales departments. We would like to retrieve employee information only from these two departments

I created a SQL query to filter for employee machines from employees in the Finance or Sales departments.

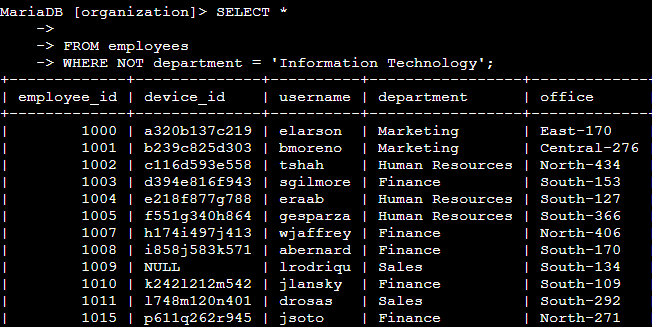


I started by using a SELECT statement to retrieve all data from the employees table. Then, I used a WHERE clause with an OR operator to filter my results to output from either Finance or Sales.

## **Retrieve all employees not in IT**

My team needs to make one more security update on employees who are not in the Information Technology department. To make the update, I first have to get information on these employees.

The following demonstrates how I created a SQL query to filter for employee machines from employees not in the Information Technology department.



I started by using a SELECT statement to retrieve all data from the employees table. Then, I used a WHERE clause with an NOT operator to filter for employees who don’t belong to the Information Technology department

## Summary

I applied filters to SQL queries to get specific information on login attempts and employee machines. I used two different tables, log\_in\_attempts and employees. I used the AND, OR, and NOT operators to filter for the specific information needed for each task. I also used LIKE and the percentage sign (%) wildcard to filter for patterns.