## **Scenario**

# 

# Review the scenario below. Then complete the step-by-step instructions.

# You are a security professional at a large organization. Part of your job is to investigate security issues to help keep the system secure. You recently discovered some potential security issues that involve login attempts and employee machines.

# Your task is to examine the organization’s data in their **employees** and **log\_in\_attempts** tables. You’ll need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

# Note: This scenario involves the same queries as the ones the [Filter with AND, OR, and NOT](https://www.coursera.org/learn/linux-and-sql/ungradedLti/wVReS/activity-filter-with-and-or-and-not) lab. You can revisit the lab to get screenshots to include in your portfolio document. If you choose, it's also possible to complete this activity without revisiting the lab by typing your queries in the template.

# 

# Apply filters to SQL queries

## Project description

To keep my organization’s and users’ data safe I am using SQL with filters to perform security related operations as follows.

## Retrieve after hours failed login attempts

Your team is investigating failed login attempts that were made after business hours. You want to retrieve this information from the login activity. You’ll identify all unsuccessful attempts after 18:00.

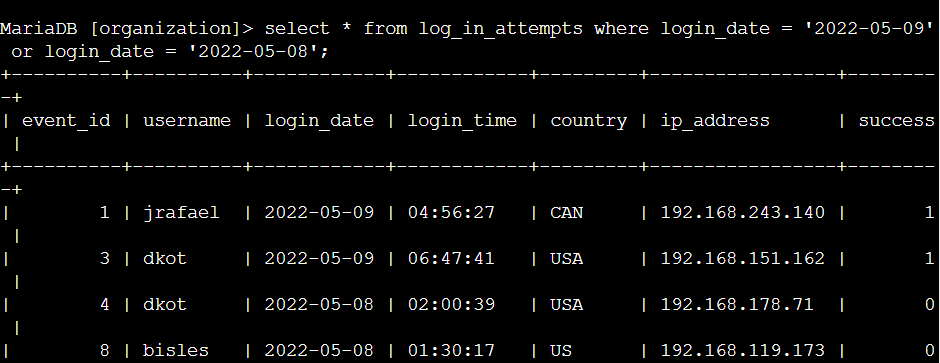


Above command depicts that we are selecting all columns from log\_in\_attempts where login\_time > 18:00:00 and success = 0. This basically means that we are searching for all the login attempts after 18:00 and which have failed.

Here success = 0 means that the login attempts failed while success = 1 means that login attempt is successful. Here we received a total of 19 rows.

## Retrieve login attempts on specific dates

Your team is investigating a suspicious event that occurred on '2022-05-09'. You want to retrieve all login attempts that occurred on this day and the day before ('2022-05-08').



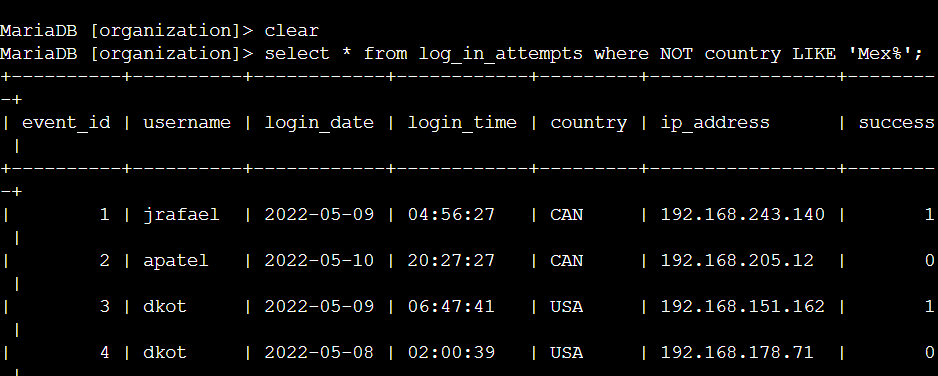
In this query, we are requesting all columns from log\_in\_attempts which occured on 2022-05-09 or 2022-05-08.

The result of this query is 75.

## 

## Retrieve login attempts outside of Mexico

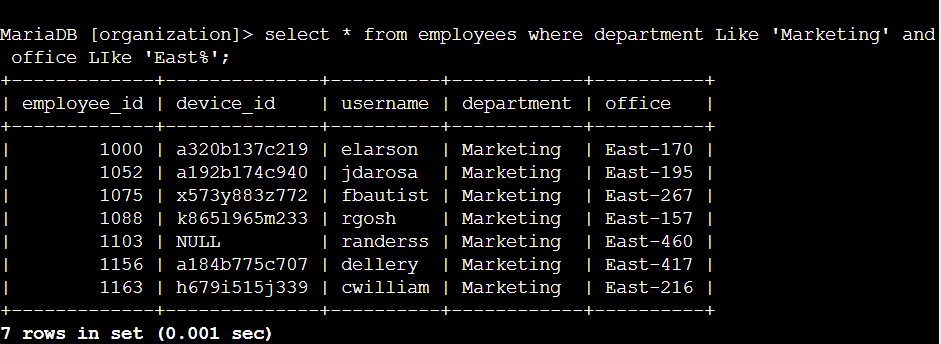
Now, your team is investigating logins that did not originate in Mexico, and you need to find this information. Note that the country field includes entries with 'MEX' and 'MEXICO'. You should use the NOT and LIKE operators and the matching pattern 'MEX%'.



The above command helps to filter the record in which country of login was not starting with name “Mex”. The ‘%’ is called a wildcard which depicts that there can be any number of any kind of string after the word ‘Mex’.

## Retrieve employees in Marketing

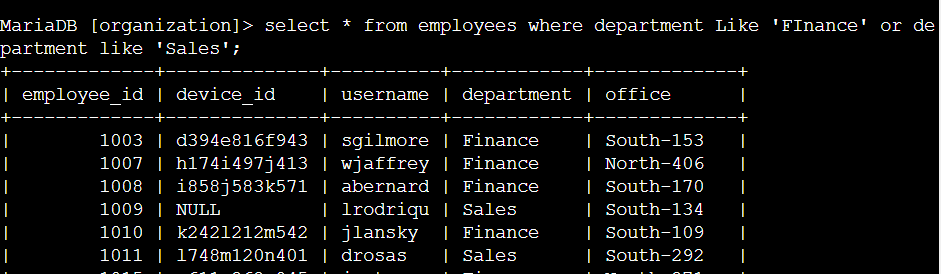
Write a SQL query to retrieve this information from the employees table. Select all columns and include filters on the department and office columns to return only the needed records.



To get employees from the marketing department and working in an office whose name starts with ‘East’.’%’operator used after East will ensure that every office name starting with ‘East’ will be considered for checking whether its department is Marketing or not.

## Retrieve employees in Finance or Sales

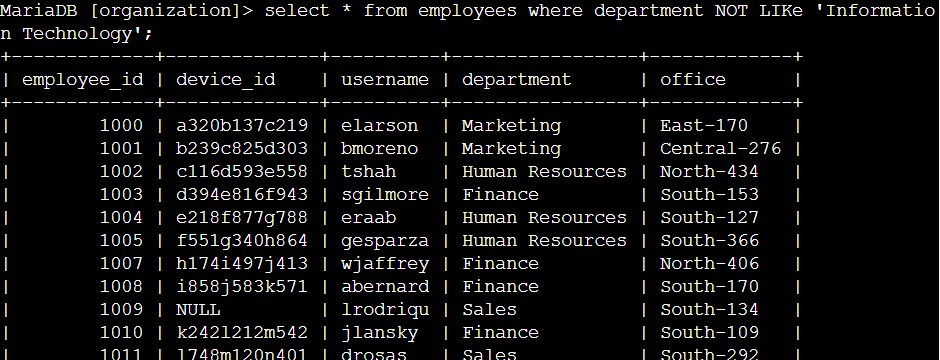
Write a SQL query to retrieve records for employees in the 'Finance' or the 'Sales' department.



The query returns the employee names from the employee table where the department of the employee is either Finance or Sales.The OR operator gives output as true if any of the conditions is true.

## Retrieve all employees not in IT

* Write a SQL query to retrieve records for employees who are not in the 'Information Technology' department.



The command gives the details of the employees which are not from the Information Technology department.The NOT operator is used to negate the result.That is first it finds the records with department Information Technology and then it gives the employee details who are not from the Information Technology department.

## Summary

In this project, we successfully used filter commands of SQL to get better result which will be easy to analyze as compared to the result without the use filter commands.These various commands helped us to get to the actual issue in very less time.