Tab 1

# Portfolio activity:

# Apply filters to SQL queries

## Project description

In this portfolio project I will be dealing with potential security issues that involve login attempts and employee machines.My task is to examine the organization’s data in their (employees) and (log\_in\_attempts) tables. I’ll need to use SQL filters(( and, not, or) to retrieve records from different datasets and investigate the potential security issues.

# Table formats

This document describes how the tables used for this portfolio activity are organized. The organization database contains the following two tables:

* log\_in\_attempts
* employees

## log\_in\_attempts

The log\_in\_attempts table has the following columns:

* event\_id: The identification number assigned to each login event
* username: The username of the employee
* login\_date: The date the login attempt was recorded
* login\_time: The time the login attempt was recorded
* country: The country where the login attempt occurred
* ip\_address: The IP address of that employee’s machine
* success: The success of the login attempt; FALSE indicates a failed attempt

In the MariaDB shell, these columns are returned as:



## employees

The employees table has the following columns:

* employee\_id: The identification number assigned to each employee
* device\_id: The identification number assigned to each device used by the employee
* username: The username of the employee
* department: The department the employee is in
* office: The office the employee is located in

In the MariaDB shell, these columns are returned as:

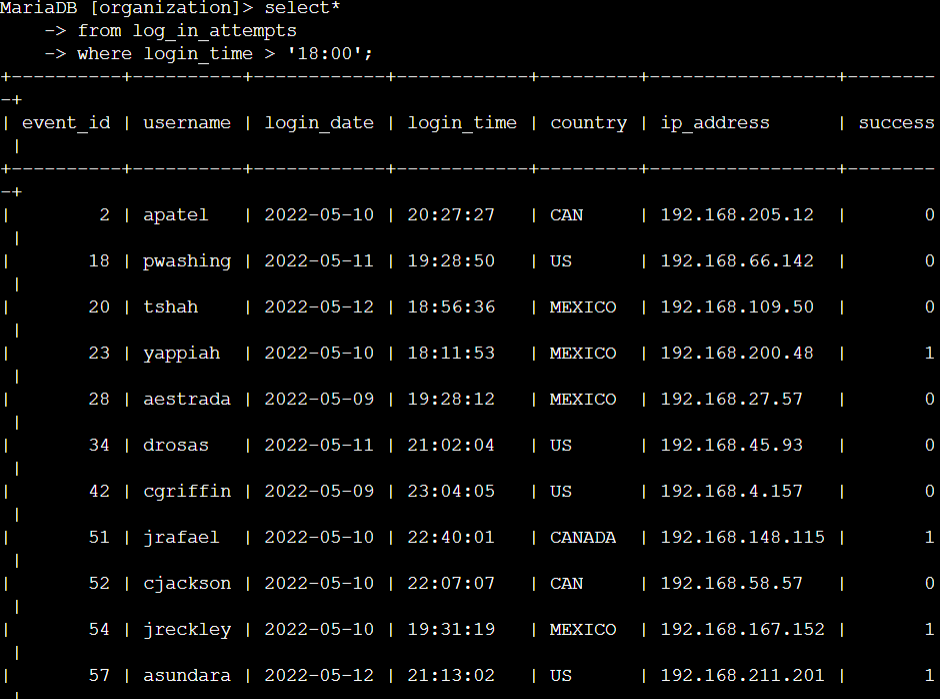


## Retrieve after hours failed login attempts

My team and I recently discovered a potential security incident that occurred after business hours.

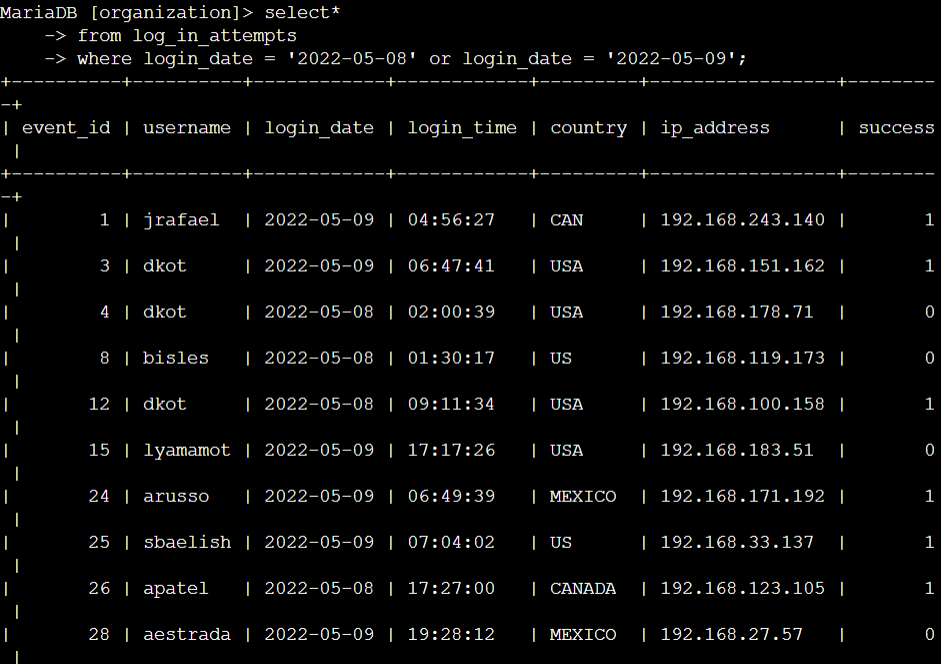
The first part of the screenshot is my query, and the second part is a portion of the output.

In order to retrieve the after hours failed login attempts ,I used the (select\*) command-line so that SQL could return all the columns (from) the (log\_in\_attemps) table I am searching from. I then entered the (where login\_time > ‘18:00’;) command-line so that I could filter out all the login attempts that happened after 18:00.



## Retrieve login attempts on specific dates

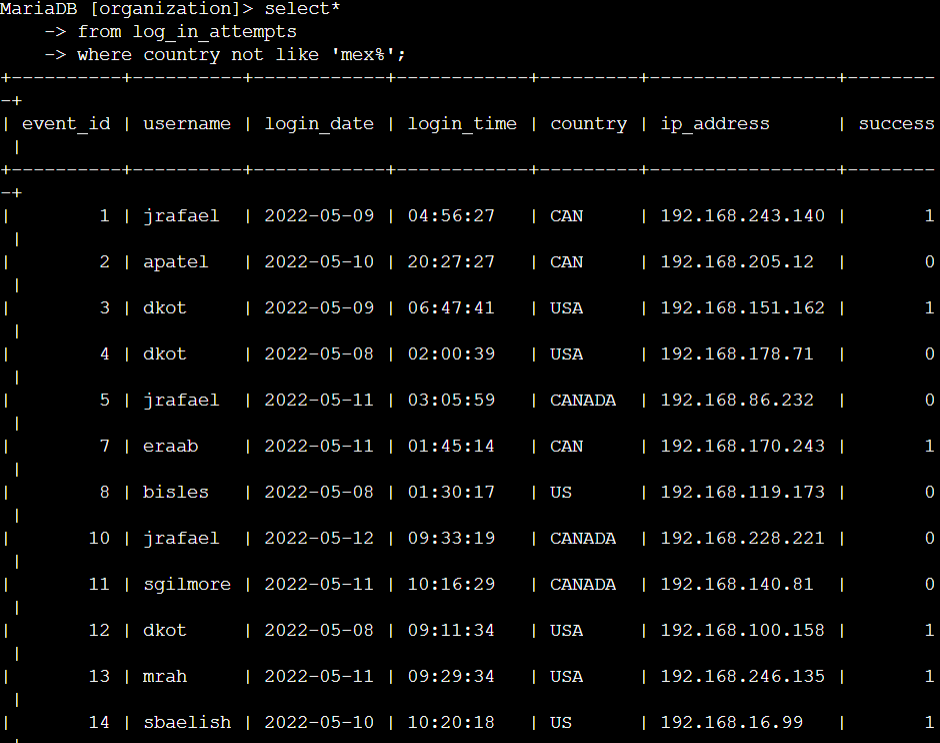
A suspicious event occurred on 2022-05-09. Therefore I will review all login attempts which occurred on this day and the day before. I did this by using the (select\*) command-line so that SQL could return all the columns (from) the (log\_in\_attemps) table i then used (where login\_date = ‘2022-05-08’ or login\_date = ‘2022-05-09’;) to filter out all the dates after the suspicious event day and only had the dates of the 2022-05-08 and 2022-05-09 events and login attempts in our table.

In this command we used the (or) filter.

(continue to next page)

## 

## Retrieve login attempts outside of Mexico

There’s been suspicious activity with login attempts, but the team has determined that this activity didn't originate in Mexico.Now, I need to investigate login attempts that occurred outside of Mexico. I used the (select\*) command-line so that SQL could return all the columns (from) the (log\_in\_attemps) table. I then went on to type (where country) to indicate that I now want to access information from the country column the (not)command to indicate that do not want a specific country but rather all the other countries in the column (like) is used for wildcards (%) instead of (=) I theN commanded (‘mex%’;) because the country column contains values of both MEX and MEXICO to represent mexico so typing mex% implies to the system all strings in the countrie column that start with “mex” should be excluded. In this task I used the (not) filter.

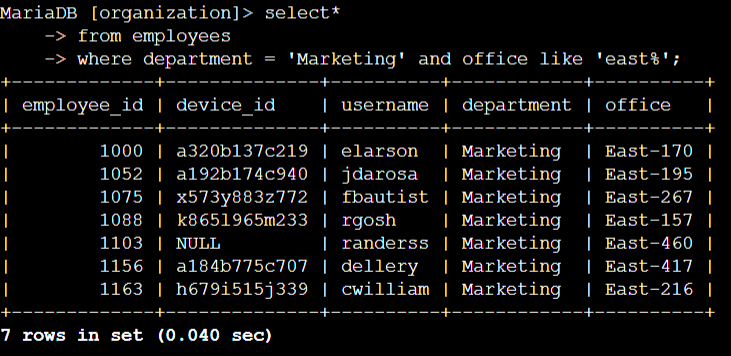
(continue to next page)

## 

## 

## Retrieve employees in Marketing

My team wants to perform security updates on specific employee machines in the Marketing department. I am responsible for getting information on these employee machines. I used (select\*) to receive all the columns of the table, for this task i used an employee table(from employees) to get back information about employees i then went on to command (where department=’Marketing’ and office like ‘east%’;) because we want all the employees who are in the marketing department (and) the east office. I used (‘east%’) because I do not want any specific office from the east, I want all of them so (%) is a placeholder for all the other characters after “east”.In this task I used the (and) filter.



(continue to next page)

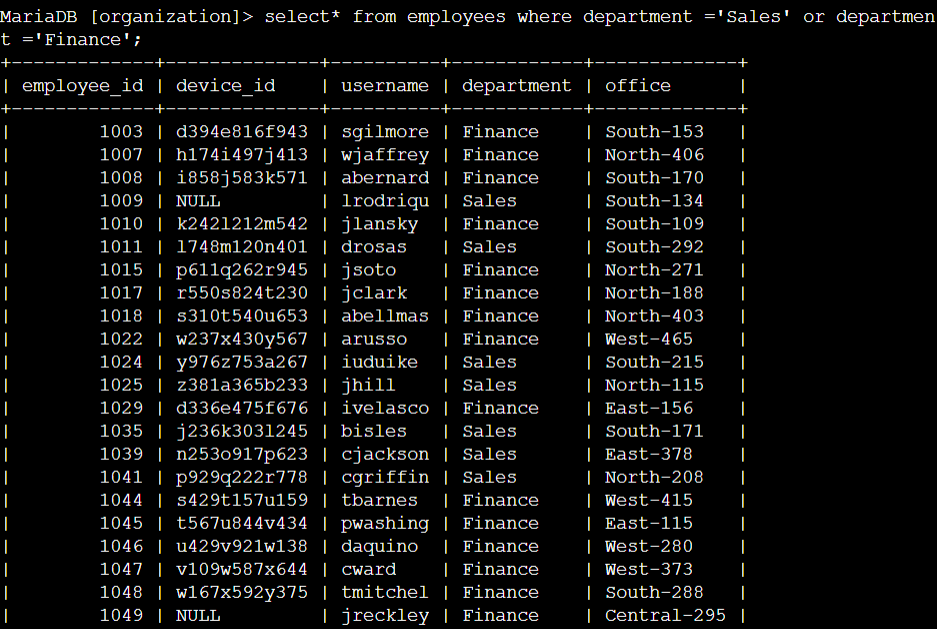
## 

## 

## 

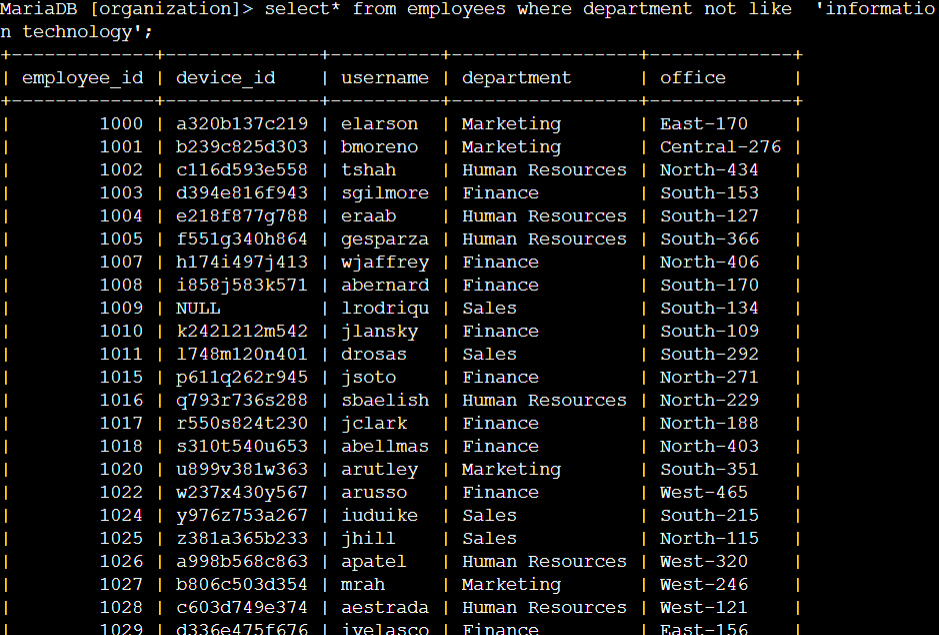
## Retrieve employees in Finance or Sales

My team now needs to perform a different security update on machines for employees in the Sales and Finance departments.



## Retrieve all employees not in IT

My team needed to make one more update to employee machines. The employees who are in the Information Technology department already had this update, but employees in all other departments need it.



## Summary

I've used the filters ( and, not, or) in this portfolio project