# Apply filters to SQL queries

## Project description

In this project I will be using SQL filters to examine security incident where there where multiple failed login attempts from employee computers past business hours (6:00 PM)

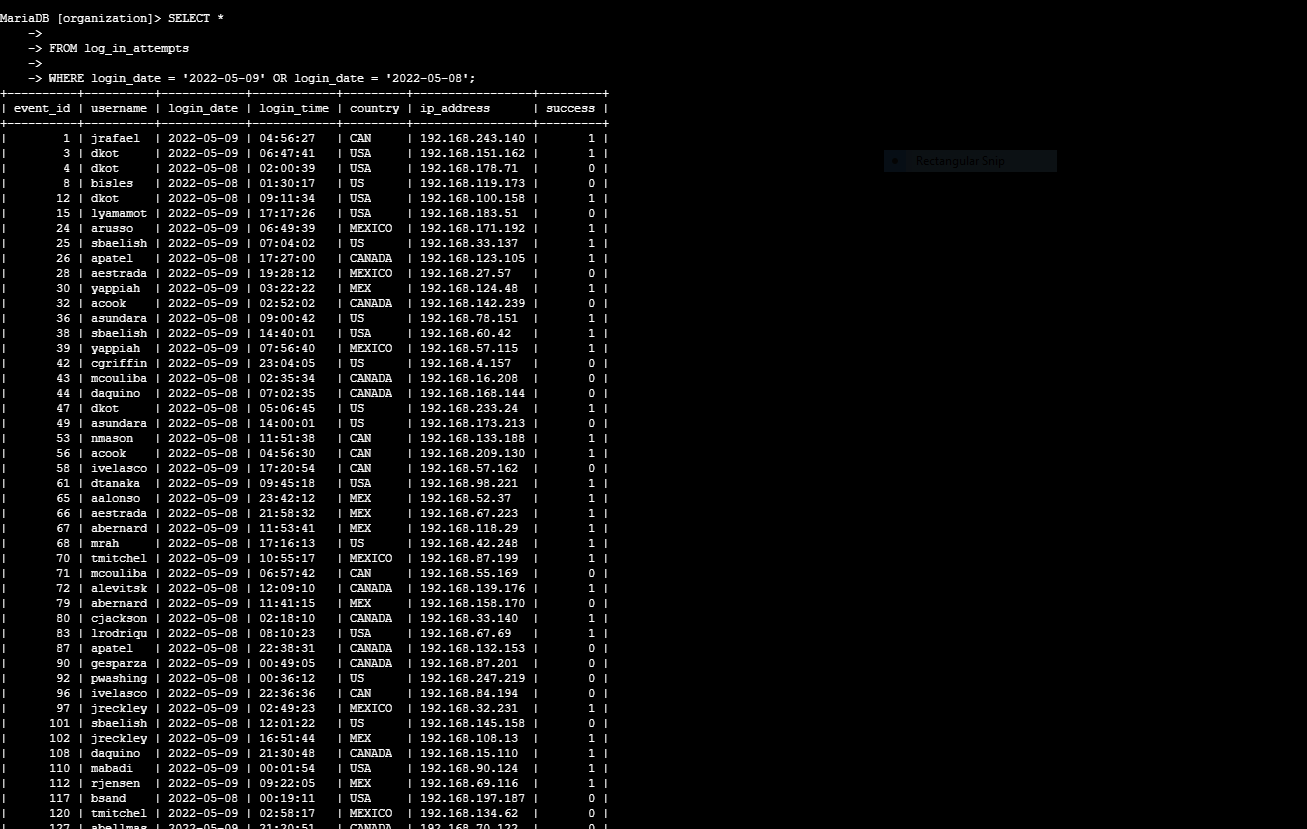
## Retrieve after hours failed login attempts

A screenshot of a computer screen

Description automatically generated

This above command retrieves all the failed login attempts after 18:00 .We find a total of 19 failed logins were made .Here I have used WHERE query to search from login times that were past(>) 18:00 with conditions of success is FALSE

## Retrieve login attempts on specific dates



The security incident occurred between 22-05-09. The above command filters all the failed login attempts between these dates . We find a total of 75 login attempts were made in these two days. I used WHERE and OR to filter from the login attempts and the dates when the event occurred .

## Retrieve login attempts outside of Mexico

A screenshot of a computer

Description automatically generated

This command narrows the search down to the specific countries the attempts were made . Here we are only seeing the attempts that are from USA and Canada . I used NOT to exclude a specific country in this case is Mexico with LIKE ‘’mex%” .The % after mex predicts any country that’s name starts with “mex” and removes it .

## Retrieve employees in Marketing

A screenshot of a computer

Description automatically generated

This command only shows the login attempts made by marketing department. Used Where , AND and Like to only display the employees and their office from marketing department in this case we are only looking at office located in the EAST .

## Retrieve employees in Finance or Sales

A screenshot of a computer

Description automatically generated

This checks the employee attempts between Finance and Sales. Here I used the OR operator to only view results from Finance or Sales department.

## Retrieve all employees not in IT

A screenshot of a computer

Description automatically generated

Lastly retrieved all the login attempts made from employees that where not from the IT department. Used NOT operator to check activity from all departments except IT

## Summary

Demonstrated how SQL query can be used to narrow down results to specifically investigate suspicions activity from any given user, date and time. The use of AND, OR, NOT , WHERE & LIKE helped to further filter the data that needs to be investigated .