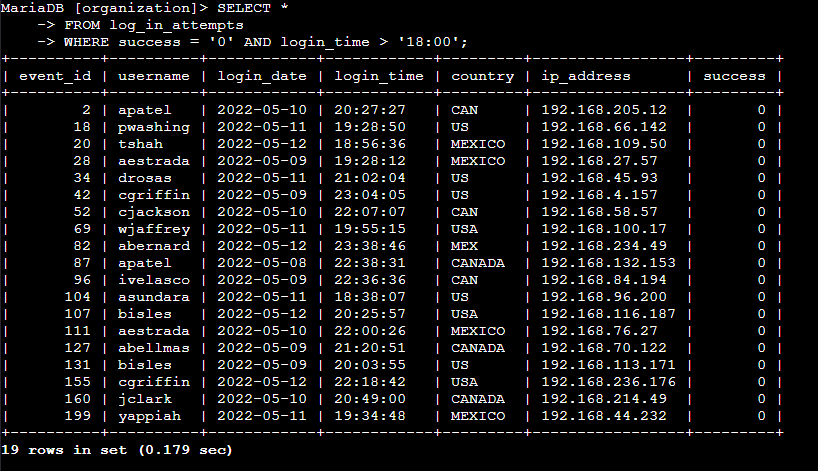
# Apply filters to SQL queries

## Project description

I discovered some potential security issues that involve login attempts and employee machines.

I’ll be examining the organization’s data in their *employees* and *log\_in\_attempts* tables. I'll need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

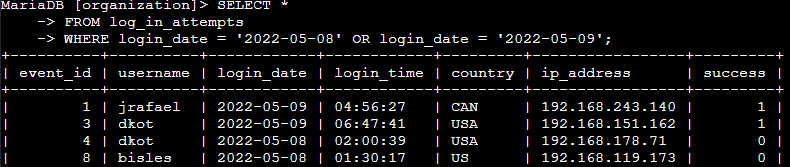
## Retrieve after hours failed login attempts

In order to retrieve the after hours failed login attempts I will be querying the database for all login attempts after work hours that failed and since I’m asking for two things the data must match I will be using *AND*:  
  


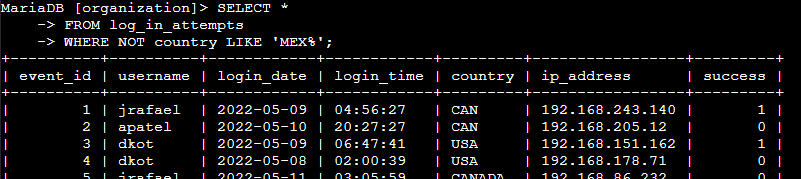
## 

## 

## Retrieve login attempts on specific dates

We had a suspicious event that occurred on 2022-05-09 and so I will be querying for logins on this date and the day before and since I am searching for information with either date I’ll be using *OR:*  
  


## Retrieve login attempts outside of Mexico

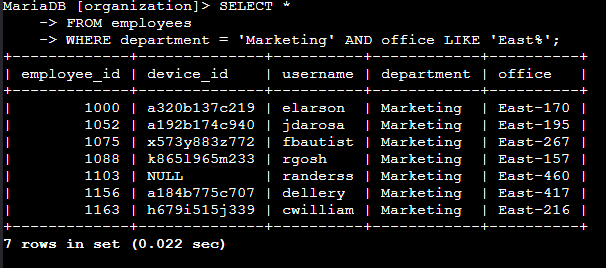
These login attempts did not happen in mexico so I can filter that out of my queries using *NOT* and *LIKE* along with a wildcard since we use both MEXICO and MEX in the entries and we need both:  
  


## 

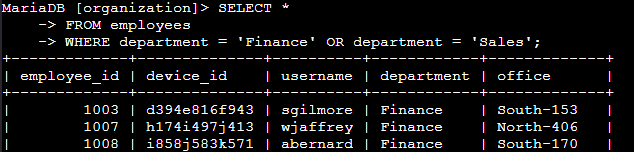
## 

## 

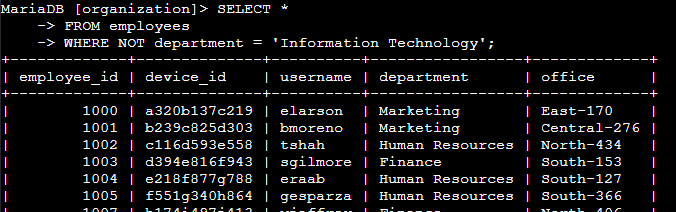
## Retrieve employees in Marketing

I need the machines for everyone in the Marketing department and which side of the building they are in so I'll be using *AND* and *LIKE* with a wildcare since there’s multiple office numbers:  
  


## Retrieve employees in Finance or Sales

We need to apply updates to both the Finance and Sale department and for that I will be querying with *OR* to filter out every department besides the two I need:  
  


## Retrieve all employees not in IT

The last updates we need to do are for all machines not in the Information Technology department, for this query I’ll be using *NOT* to return all departments besides IT:  
  


## Summary

This whole scenario was to teach the functions of *AND*, *OR*, and *NOT* and how one could use it with SQL query to search for information a cybersecurity professional might need in their day to day job duties. SQL is a great way to quickly pull up data if you do not have another solution in place to do so. This information could be used to find an intrusion attempt, out of date equipment that poses a risk to a company, or to present data to executives or shareholders in order for them to better understand and make decisions.