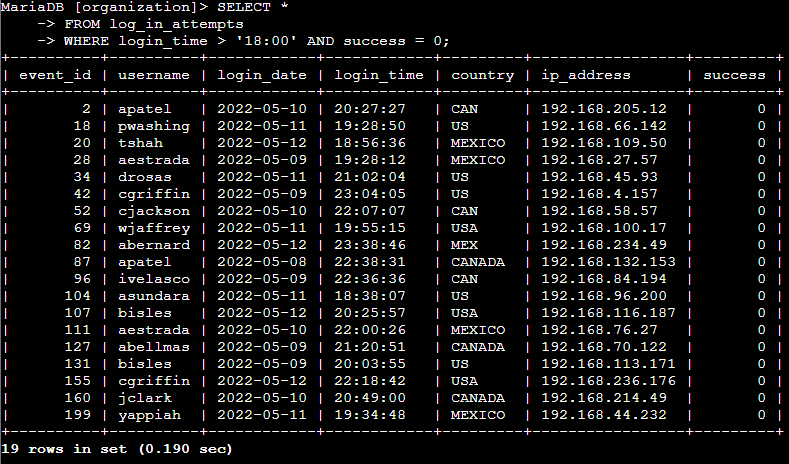
# Apply filters to SQL queries

## Project description

SQL, or structured query language, is a powerful tool that can be utilized by security specialists in order to quickly gather information from logs. Below, I will demonstrate some ways I am able to use it and what I am doing with each query.

## Retrieve after hours failed login attempts

Below is an example of pulling information regarding failed login attempts after 18:00, or 6PM, on a log file. First, I started by selecting the log\_in\_attempts table, using SELECT \* FROM log\_in\_attempts. Then, using the WHERE filter, I selected only times AFTER 18:00 and with a success value of 0 (F in boolean, since this is how SQL stores boolean values.

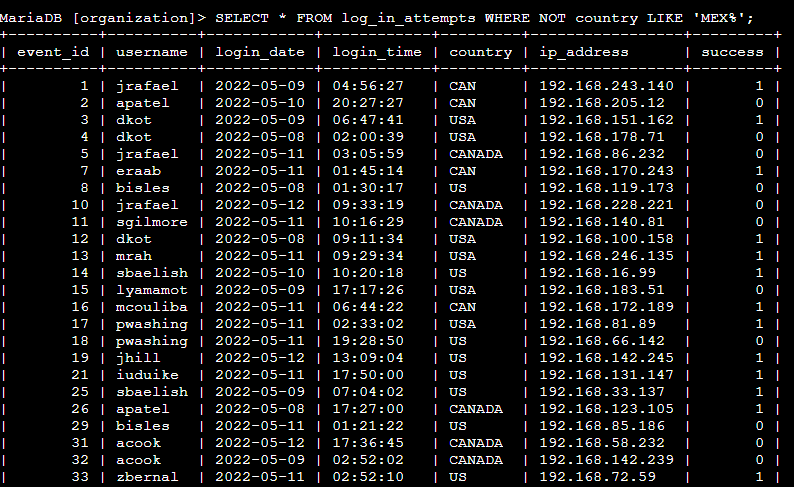
## Retrieve login attempts on specific dates

Below is an example of using “OR” to search for logins on specific dates; I have used the WHERE to filter the login date by either 2022-05-08 or 2022-05-09. This kind of query would be useful if you were to use SQL to check specific dates for suspicious activity.

## 

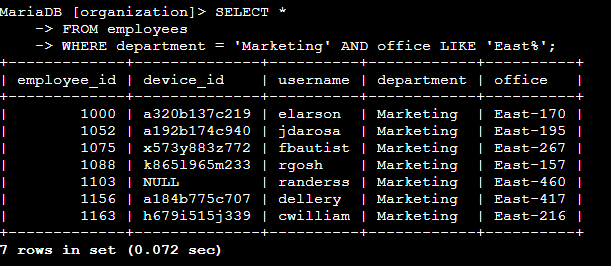
## Retrieve login attempts outside of Mexico

In this example, we are searching login attempts outside of Mexico; in SQL, we are required to use “WHERE NOT” and the “LIKE” function, along with the % wild card. This is because the database is inconsistent on how Mexico is labeled, and may be either MEX or MEXICO in the database.



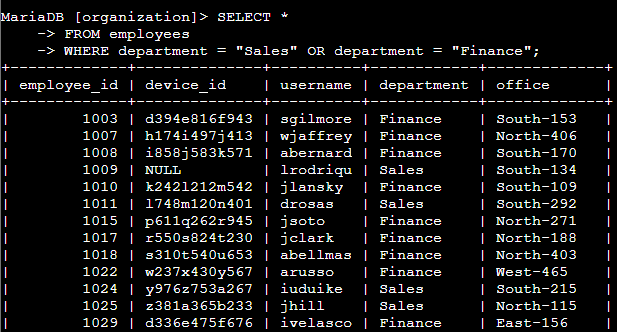
## Retrieve employees in Marketing

In this example, let’s say for a system update, we are retrieving all members of the Marketing department that are in the East buildings. Since there is more than one East building, a wild card makes it easy to pull all of the employees since they all start with ‘East’



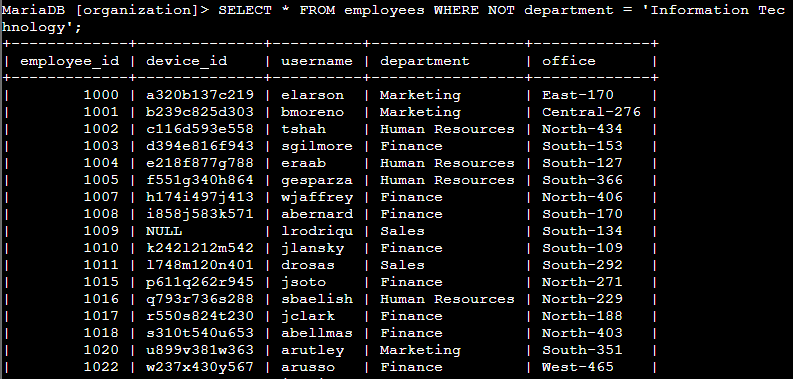
## Retrieve employees in Finance or Sales

The below query is for if we wanted to select ALL employees in finance or sales departments. This shows the usefulness of the OR function.



## Retrieve all employees not in IT

Finally, we can use the WHERE NOT function to select all employees not in a certain group – in this example we are choosing “Information Technology”

****

## Summary

SQL is a powerful language that can be used to retrieve important data from logs and other sources fairly quickly. I’m glad I know how to use it!