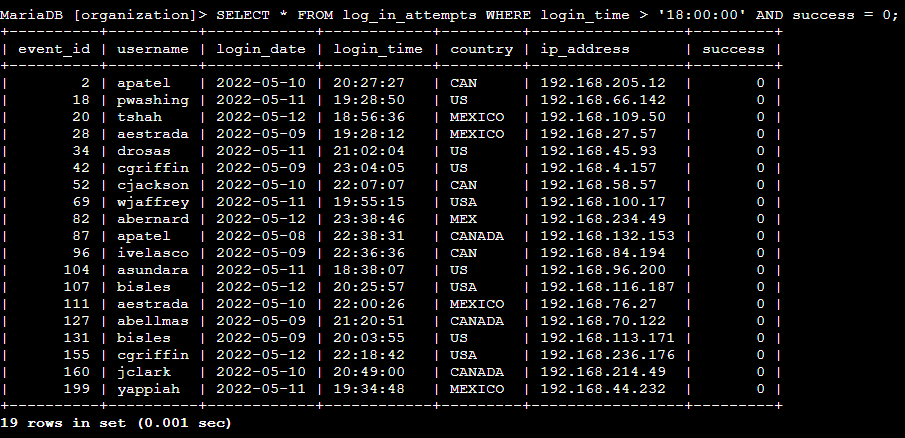
# Apply filters to SQL queries

## Project description

By using SQL I was able to find information on failed login attempts much faster than looking through logs line by line. Therefore, I was able to act faster in stopping any malicious login attempts.

## Retrieve after hours failed login attempts

SELECT \* FROM log\_in\_attempts WHERE login\_time > ‘18:00:00’ AND success = 0;



Here you can see I used the greater than (>) operator to review all login attempts after 18:00

## 

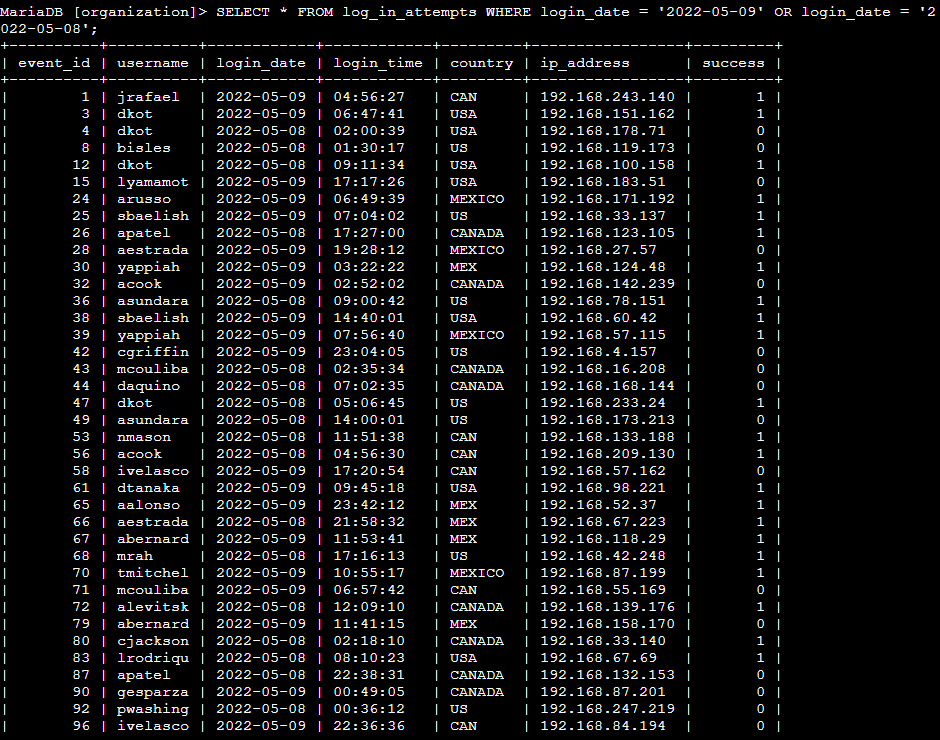
## 

## 

## 

## Retrieve login attempts on specific dates

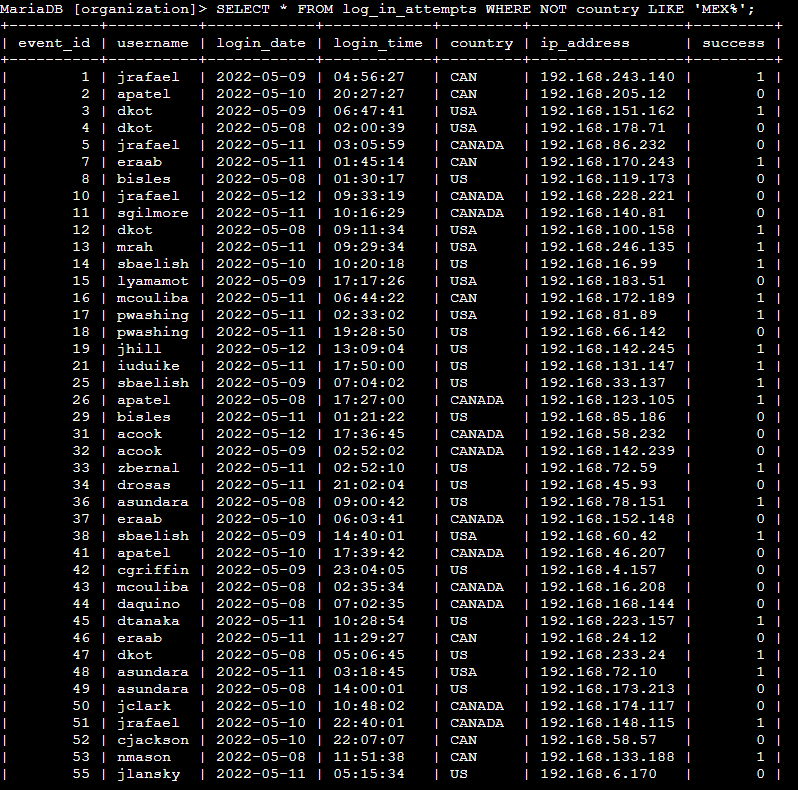
SELECT \* FROM log\_in\_attempts WHERE login\_date = ‘2022-05-09’ OR login\_date = ‘2022-05-08’;



In the screenshot above, I used the OR operator to choose 2 different dates given by the organization to review all login attempts.

## Retrieve login attempts outside of Mexico

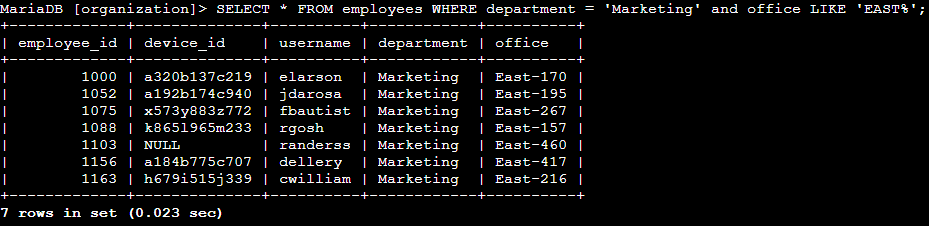
SELECT \* FROM log\_in\_attempts WHERE NOT country LIKE ‘MEX%’;



Above you can see I used the NOT operator when asked by the organization to review any logins that were not attempted in Mexico. I also use the % wildcard as some of the locations state MEXICO while others only state MEX.

## Retrieve employees in Marketing

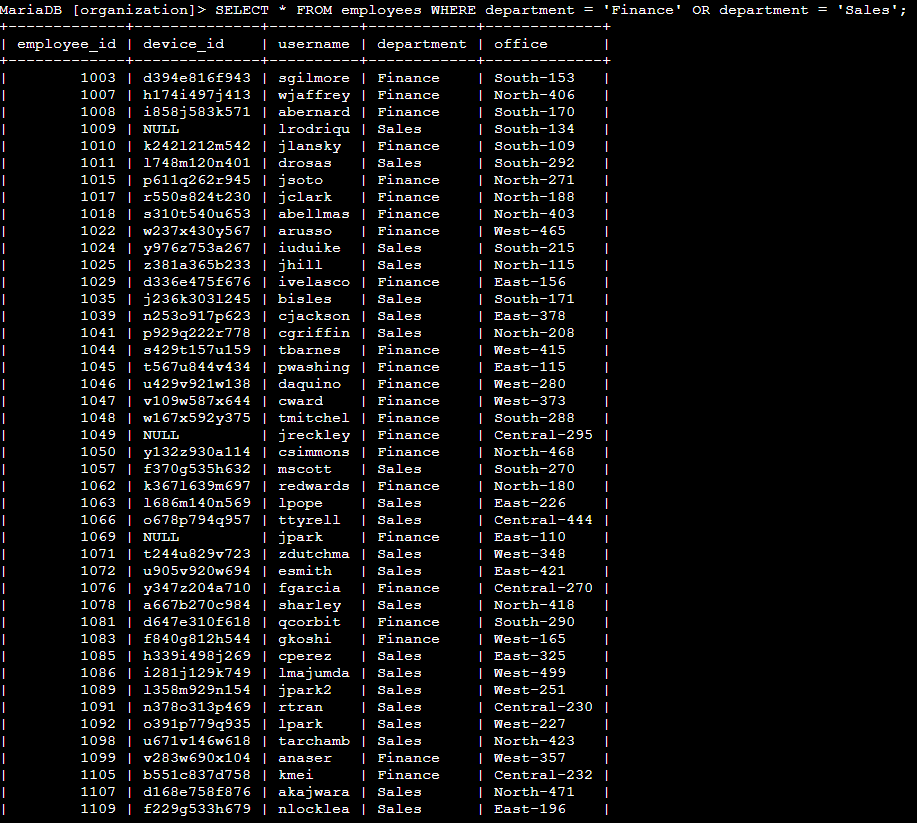
SELECT \* FROM employees WHERE department = ‘Marketing’ AND office LIKE ‘East%’;



Within this photo you can see the use of the AND operator to choose 2 different conditions requested by the organization. You can also see the use of the LIKE filter as they wanted all offices in the east building to be included.

## Retrieve employees in Finance or Sales

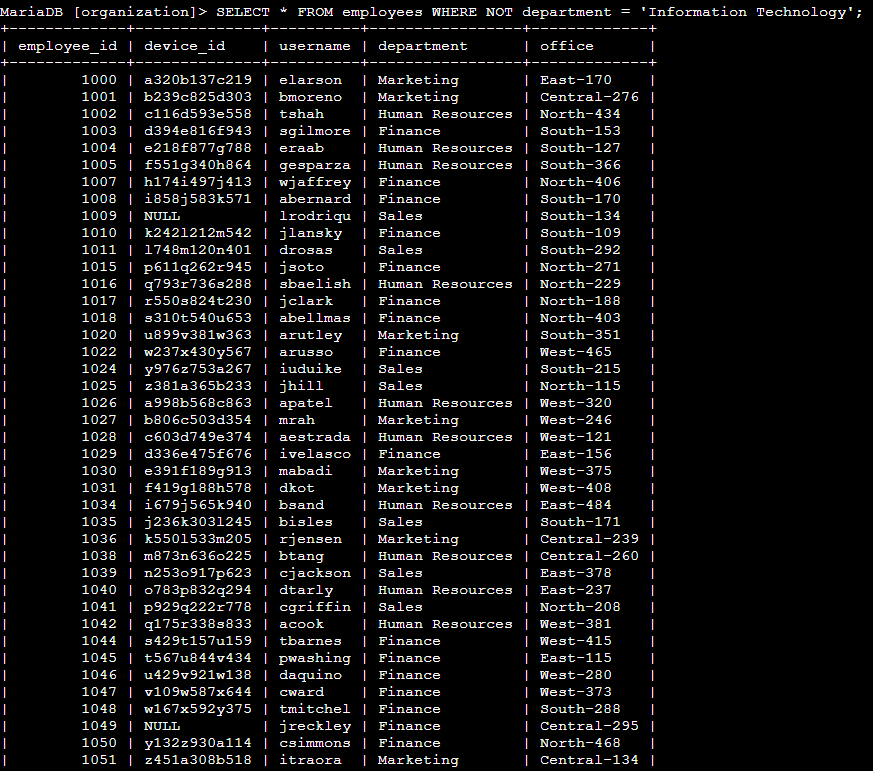
SELECT \* FROM employees WHERE department - ‘Finance’ OR department = ‘Sales’;



Here you can see the use of the OR operator as a way to find all employees in the finance or sales department.

## Retrieve all employees not in IT

SELECT \* FROM employees WHERE NOT department = ‘Information Technology’;



Lastly, it was requested to provide all employees not within the IT department. To find this information, I used the NOT operator to remove all employees from the list who were in the Information Technology department.

## Summary

Having an understanding of SQL is very important in the Cybersecurity field as it helps find information much faster than looking through lines of code one at a time. This experience has helped me further understand how and when to use each operator and filter within a database search.