# Apply filters to SQL queries

## Project description

**I am a Security Professional at a large Organization. My organization is working to make their system more secure. I have been tasked with ensuring the system is safe, and to investigate all potential security issues, and update employee computers as needed. The following steps provide examples of how I used SQL with filters to perform security-related tasks.**

.

## Retrieve after hours failed login attempts

A screenshot of a computer screen

Description automatically generated

**A suspicious event occurred on 2022-05-09. Any login activity that happened on 2022-05-09 or on the day before needs to be investigated. Using the SQL Code – SELECT \* FROM log\_in\_attempts WHERE login\_time > ’18:00’ AND success = false; the code went through the tables and filtered in only the login attempts that failed. The first condition is login\_time > '18:00', which filters for the login attempts that occurred after 18:00. The second condition is success = FALSE, filters for the failed login attempts. There were 19 Attempts in this example.**

## Retrieve login attempts on specific dates

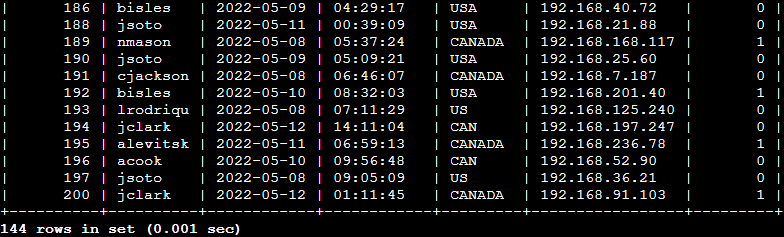
A screenshot of a computer screen

Description automatically generated  
**There was a potential security incident that occurred after business hours (after 18:00). All after hours login attempts that failed need to be investigated**. **The Following SQL code shown above – SELECT \* FROM log\_in\_attempts WHERE login\_date = ‘2022-05-09’ OR login\_date = ‘2022-05-08’; I used a WHERE clause with an OR operator to filter my results to output only login attempts that occurred on either 2022-05-09 or 2022-05-08. The first condition is login\_date = '2022-05-09'; which filters for logins on 2022-05-09. The second condition is login\_date = '2022-05-08'; which filters for logins on 2022-05-08, there were 75 attempts between the 2 dates.**

## Retrieve login attempts outside of Mexico

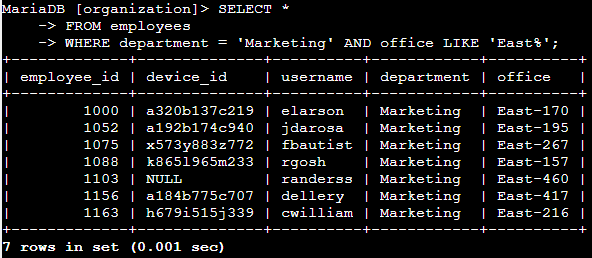
A screen shot of a computer

Description automatically generated



**After investigating the organization’s data on login attempts, it appears that there is an issue with the login attempts that came from outside the city of Mexico. These login attempts should be investigated. The following SQL Code SELECT \* FROM log\_in\_attempts WHERE NOT country LIKE ‘mex%’; First, I started by selecting all data from the log\_in\_attempts table. Then, I used a WHERE clause with NOT to filter for countries other than Mexico. I used LIKE with MEX% as the pattern to match because the dataset represents Mexico as MEX and MEXICO. The percentage sign (%) represents any number of unspecified characters when used with LIKE was used to filter all the information, all attempts that are NOT Mexico where shown. In this case there were 144 log in attempts by Canada, USA, and US.**

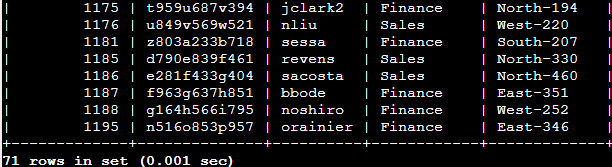
## Retrieve employees in Marketing



**My team wants to update the computers for certain employees in the Marketing department. To do this, I must get information on which employee machines to update.**

**The Following SQL Code SELECT \* FROM employees WHERE department = ‘Marketing’ AND office LIKE ‘East%’; First, I started by selecting all data from the employees table, Then, I used a WHERE clause with AND to filter for employees who work in the Marketing department and in the East building. The first condition is the department = 'Marketing', which filters for employees so that only those in the Marketing department are shown. The second condition is the office LIKE 'East%', which filters for employees in the East building there were 7 employees meeting the conditions found.**

## Retrieve employees in Finance or Sales A screenshot of a computer screen Description automatically generated



**The machines for employees in the Finance and Sales departments also need to be updated. Since a different security update is needed, I must get information on employees only from these two departments. The SQL CODE SELECT \* FROM employees WHERE department = ‘Finance’ OR department = ‘Sales’; was used to filter the employee records so that only employees from the Finance or Sales departments are shown, the first condition is department = 'Finance', which filters for employees from the Finance department. The second condition is department = 'Sales', which filters for employees from the Sales department there were 71 results in total.**

## Retrieve all employees not in ITS

## A screenshot of a computer screen Description automatically generated

## 

**My team needs to make one more security update on employees who are not in the Information Technology department. To make the update, I first have to get information on these employees. The SQL Code SELECT \* FROM employees WHERE NOT department = “Information Technology’; is used to filter out the Information Technology department so that only Finance, Marketing, Sales, and Human Resources departments were displayed making it easier to search for specific information.**

## Summary

**I applied different SQL filters to get specific information on login attempts and employee machines. I used two different tables, log\_in\_attempts and employees. I used the AND, OR, and NOT operators to filter for the specific information needed for each task. I also used LIKE and the percentage sign (%) wildcard to filter for patterns.**