# Apply filters to SQL queries

## Project description

The organization asked me to investigate security issues to help keep the system secure. I recently discovered some potential security issues that involve login attempts and employee machines. examine the organization’s data in their employees and log\_in\_attempts

tables. I used SQL filters to retrieve records from different datasets and investigated potential security issues.

## Retrieve after hours failed login attempts

I recently discovered a potential security incident that occurred after business hours. To investigate this, I need to query the log\_in\_attempts table and review after hours login activity. I used filters in SQL to create a query that identifies all failed login attempts that occurred after 18:00.

I used the code

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

A screen shot of a computer

Description automatically generated

Here the code is telling the SQL to search all columns from the file log\_in\_attempts to look for login time greater than 18:00 and check if the login attempt is success or failed.

A total of 19 failed login attempts were made after 18:00.

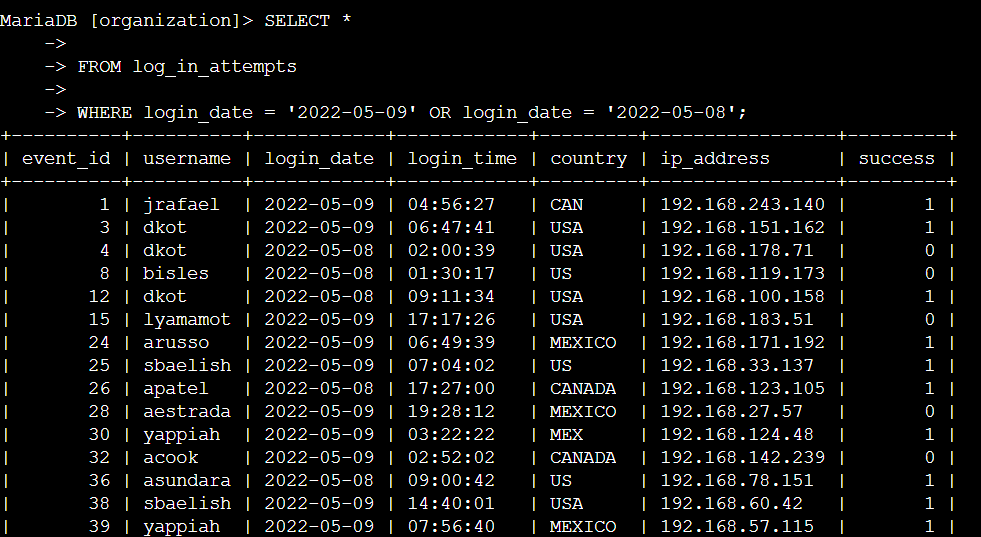
Note\* 0 indicates a failed attempt and 1 indicates a successful attempt.

## Retrieve login attempts on specific dates

I noticed a suspicious event occurred on 2022-05-09. To investigate this event, I reviewed all login attempts which occurred on this day and the day before. I Used filters in SQL to create a query that identifies all login attempts that occurred on 2022-05-09 or 2022-05-08.

I used the code

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

Here the code is telling the SQL to search all columns from the file log\_in\_attempts to look for login\_date from 2022-05-08 to 2022-05-09. The OR command is used to combine two or more conditions in a single query. It returns a result if at least one of the conditions is met. A screen shot of a computer screen

Description automatically generated There were 75 login attempts made on the specified dates. The last output gives us how many entries were registered. So based on the query there were 75 login attempts made between 2022-05-09 to 2022-05-08.

## Retrieve login attempts outside of Mexico

There’s been suspicious activity with login attempts, but the team has determined that this activity didn't originate in Mexico. The team asked me to investigate login attempts that occurred outside of Mexico. I Used filters in SQL to create a query that identifies all login attempts that occurred outside of Mexico.

I used the code

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

This filters out the file by excluding Mexico. Mex and all MEX related entries. The NOT command is used to negate a condition in a query. And LIKE command is used in a WHERE clause to search for a specified pattern in a column.

A screen shot of a computer

Description automatically generated

A screen shot of a computer screen

Description automatically generated

After excluding MEXICO country from the search there were 144 login attempts made outside of mexico.

## Retrieve employees in Marketing

The team wants to perform security updates on specific employee machines in the Marketing department. The team assigned me to get information on these employee machines and asked me to query the **employees** table. I Used filters in SQL to create a query that identifies all employees in the Marketing department for all offices in the East building.

I Used the code

SELECT \* FROM employees WHERE department = ‘Marketing’ and office like “east%”;

This SQL code looks for the file employees and filters out the marketing department and the LIKE command looks for the specific sting which was east office buildings that has numerical numbers after east.

A screen shot of a computer

Description automatically generated

The last line gives us the total of 7 employees in the marketing department in all of the east office buildings.

## Retrieve employees in Finance or Sales

The Team now needs to perform a different security update on machines for employees in the Sales and Finance departments. I Used filters in SQL to create a query that identifies all employees in the Sales or Finance departments.

The code that I used is

SELECT \* FROM employees WHERE department = ‘Finance’ or department =’sales”;

A screenshot of a computer screen

Description automatically generated This command lists out all the employees in the sales and finance department as I used the OR command to combine both the departments.

## Retrieve all employees not in IT

The team needs to make one more update to employee machines. The team asked me to exclude all the employees who are in the Information Technology department since they already had this update, but employees in all other departments need it. I Used filters in SQL to create a query which identifies all employees not in the IT department.

The code that I used is

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

The NOT command negates the Information Technology department and lists all other departments who need an update. There are 161 employees from different departments who need an update.

A screen shot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

## Summary

I applied filters to SQL queries 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.