Apply filters to SQL queries

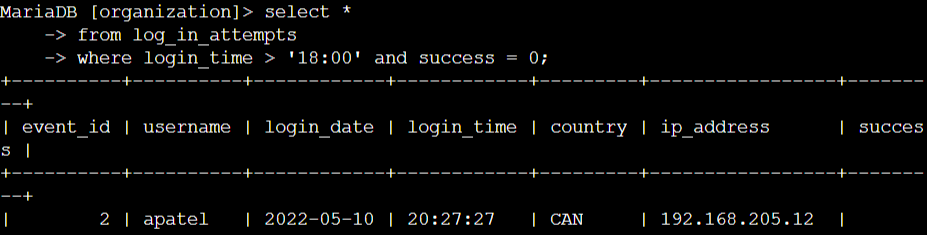
Project description

My organization is doing its best to safeguard the public info from malicious threat actors. It is my job to prevent potential security risks and regularly update the employee's systems by using tools like SQL. The following steps explain the uses of SQL:-

Retrieve after-hours failed login attempts

We discovered that there was a potential security incident that occurred after business hours (18:00) o clock now we need to check the log data of login attempts, particularly the unsuccessful login attempts.

The following code demonstrates how I created a SQL query to filter for failed login attempts that occurred after business hours.

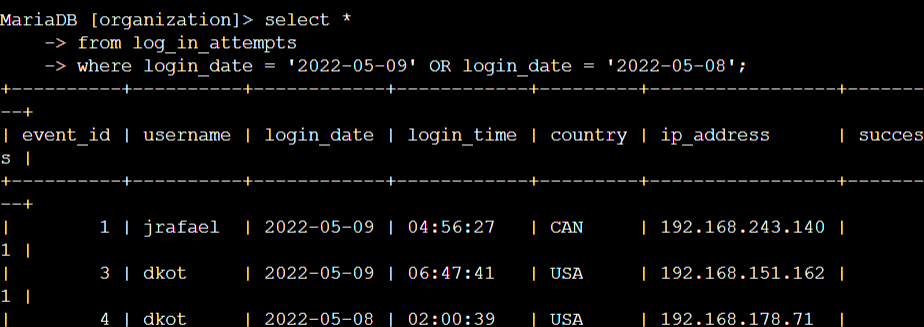


Explanation of the code:-

The first part of the screenshot is my query, and the second part is a portion of the output. This query filters out the failed login attempts after 18:00. Which is used to specify the condition required to filter out our query. login\_time > ’18:00’ represents that we want to filter out all the queries after time 18:00 and the success = 0 indicates all the failed login attempts.

Retrieve login attempts on specific dates

a suspicious attack to take place on the day 2022-05-09. So we need to investigate the login attempts that took place on and before the date 2022-05-09. So we need to filter out the login attempts that took place on dates 2022-05-09 or 2022-05-08.

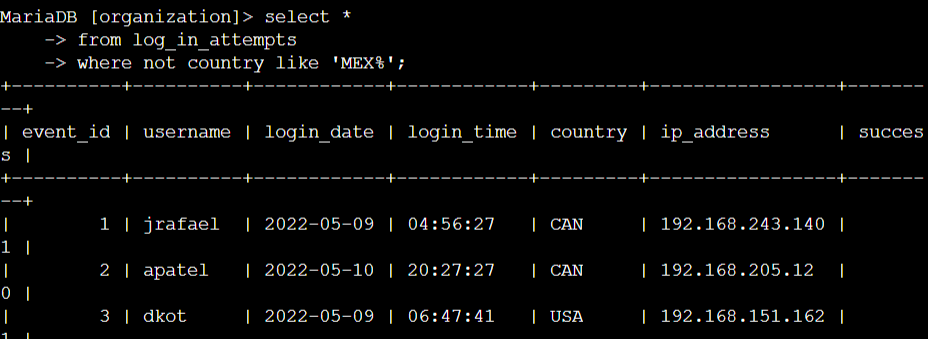


Explanation of code:-

Here we are selecting all the columns of the table log\_in\_attempts. Also, we are filtering the login attempts that took place on dates 2022-05-09 or 2022-05-08 by using ‘or’ to filter it out. As we enter the query we get the output from the system according to our query.

Retrieve login attempts outside of Mexico

There was suspicious activity with the login attempts, but the team determined that the attacks didn’t originate from Mexico. So we need to use SQL to filter out the log data by using the ‘not’ command in SQL.

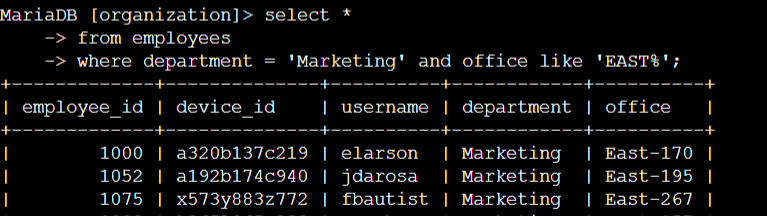


Explanation to code:-

Here we are selecting all the columns from the table from the table log\_in\_attempts. We do not want to include the log\_in attempts from Mexico so we use ‘not’ here as a negation statement and ‘like’ to exclude the entries that have MEX in their logs. If we use ‘=’ it only excludes the cases that have MEX in their country column.

Retrieve employees in Marketing

Our team wants to perform security updates on the machines of employees from the marketing department who are located on the east side of the office building. The following query explains how to filter out the log data using SQL.

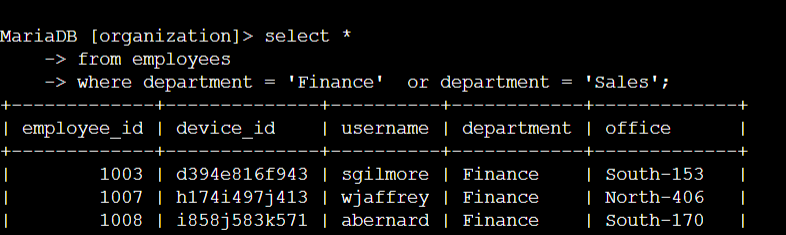


Explanation of the code:-

We are selecting all the columns of the ‘employees’ table also here we are using ‘=’ to filter out employees from the marketing department and like to filter out people who are working in the marketing department and have machines on the east side of the marketing department.

Retrieve employees in Finance or Sales

The machines for employees in the Finance and Sales departments also need to be updated. Since a different security update is needed, I have to get information on employees only from these two departments. The following code demonstrates how I created a SQL query to filter for employee machines from employees in the Finance or Sales departments.



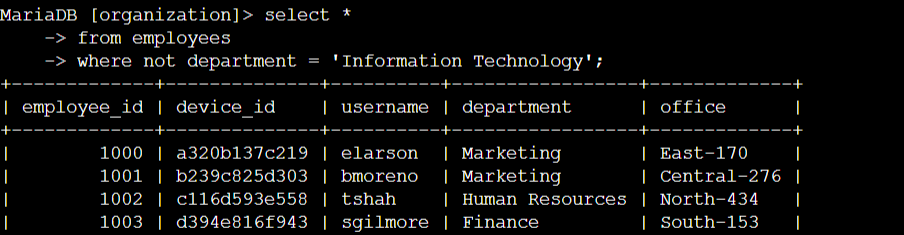
Explanation of code:-

Using SQL we are filtering out the employees from the finance and sales departments. The first condition department = ‘finance’ filters out the employees only from the finance department as we are using ‘or’ here the system filters out the employees from the sales department also.

Retrieve all employees not in the IT

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 following demonstrates how I created a SQL query to filter for employee machines from employees not in the Information Technology department.



Explanation of code:-

Here the not command excludes all cases in which the employees are from the information technology department.

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.