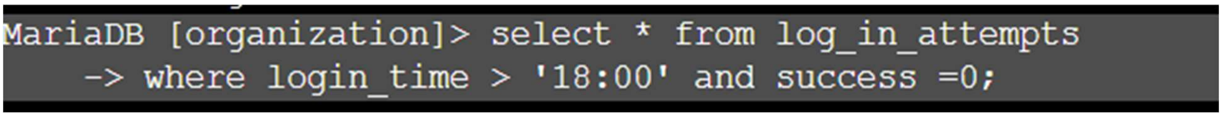
Apply filters to SQL queries

Project description

As a Security Analyst it is my job to investigate any security incidents and mitigate any potential risk. To be able to execute my role I use SQL commands to filter, retrieve and analyze data to secure my organization's systems. The following shows some of the commands I use in SQL to achieve some of my security related responsibilities.

Retrieve after hours failed login attempts

In an investigation of the security incident that happened recently, I found out that the incident happened after working hours of the organization (after 6 PM). I ran a SQL query to find out all the failed login attempts.

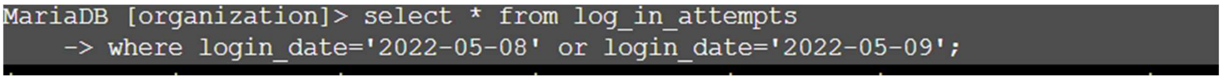


```
MariaDB [organization]> select * from log_in_attempts
    -> where login_time > '18:00' and success =0;
```

The query retrieves all failed login attempts after the hour of 18:00 (6 PM). I was able to retrieve 19 failed login attempts in the system. The command selects all records from the log_in_attempts table that meet two conditions, the login_time after ‘18:00’ and the success of login is set to 0 (which represents False or failed). I used the ‘AND’ logical operator to combine the two conditions and only return a result that meets both conditions. .

Retrieve login attempts on specific dates

There was a security incident on two specific dates. In an effort to investigate the incident, I run a SQL query on the log_in_attempts to retrieve all login attempts on those dates.

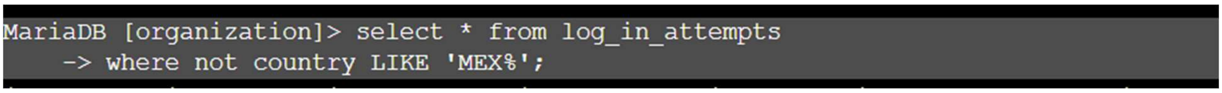


```
MariaDB [organization]> select * from log_in_attempts
    -> where login_date='2022-05-08' or login_date='2022-05-09';
```

The above screen shot shows a sample of the command I used to retrieve all records from the log_in_attempts table that matches two conditions, the login_date on 2022–05-08 and the login_in date 2022-05-09. I used the 'OR' logical operator to combine the two conditions and return records of a login attempt that meets either of the conditions and both conditions. As a result I was able to get 75 records of login attempts on those two dates. The 'OR' operator returns records that meet either of the conditions to be true.

Retrieve login attempts outside of Mexico

After noticing some suspicious login attempts from countries outside of Mexico, I started investigating.To be able to retrieve records of login attempts that are outside of Mexico, I run SQL command by using a combination of two operators.

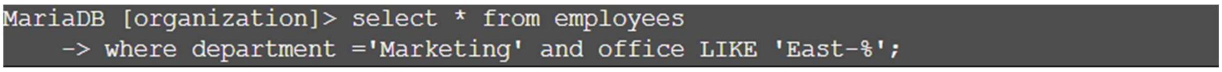


```
MariaDB [organization]> select * from log_in_attempts
    -> where not country LIKE 'MEX%';
```

As shown in the sample command screenshot, the command retrieves all data from the log_in_attemps table meets two conditions. The 'NOT' operator will retrieve records from the table except the conditions that will be set next, in this case Country is the condition used.
I also used the 'LIKE' operator to be able to use the '%' wild card. This wild card represents a different number of characters and different combinations of characters.

Retrieve employees in Marketing

In order to make some security software installations in the marketing department, I needed to get information on which offices belong to the marketing department. I ran the following sample sql command to achieve this task.

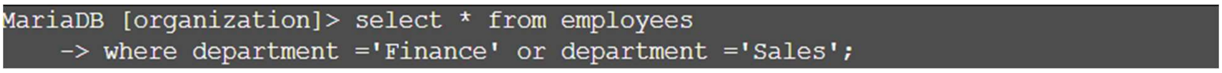


```
MariaDB [organization]> select * from employees
    -> where department ='Marketing' and office LIKE 'East-%';
```

The command selects all information from the employees table which matches two conditions. The conditions are the department name which is marketing and the office designation. As the offices are designated by an alpha numeric combination , I used the LIKE operator with the '%' wildcard.

Retrieve employees in Finance or Sales

In order to perform some security software updates on the finance and sales department computers, I needed to retrieve information only from these two departments. The following screenshot shows a sample Sql command I used to get all the employees and thier devices form the finance and sales department.

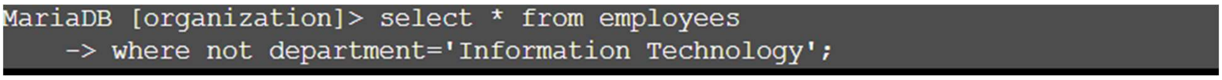


```
MariaDB [organization]> select * from employees
    -> where department ='Finance' or department ='Sales';
```

The first section of the command selects all records from employees table and the second section of the command filters out the record based on the departments finance and sales.
I used the ‘OR’ operator to be able to get the employees information witch are in either one of the departments.

Retrieve all employees not in IT

I needed 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.



```
MariaDB [organization]> select * from employees
    -> where not department='Information Technology';
```

The first part of the screenshot is my query, and the second part is a portion of the output. The query returns all employees not in the Information Technology department. First, I started by selecting all data from the employees table. Then, I used a WHERE clause with NOT to filter for employees not in this department.

Summary

As shown in the document above I used several commands and queries of SQL to perform some security operations. I used two tables to filter out the necessary records and I used operators to further enhance the filter. The operators I used are ‘AND’, ‘OR’,’NOT’ and I used wildcards such as ‘LIKE’ in combination with the ‘%’.