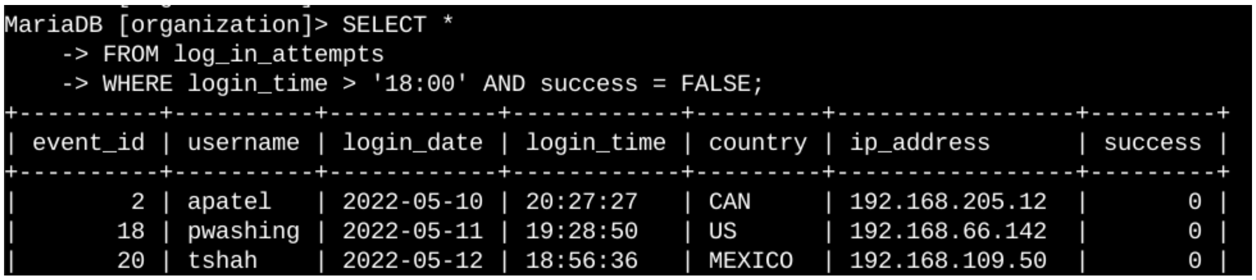
Apply Filters to SQL Queries

Project description

My organization is improving its system security. My role is to identify potential security issues, ensure system safety, and update employee computers as needed. The following examples show how I used SQL with filters to complete these security-related tasks.

Retrieve after-hours failed login attempts

A potential security incident occurred after business hours (after 18:00). All failed login attempts during that time needed to be reviewed.

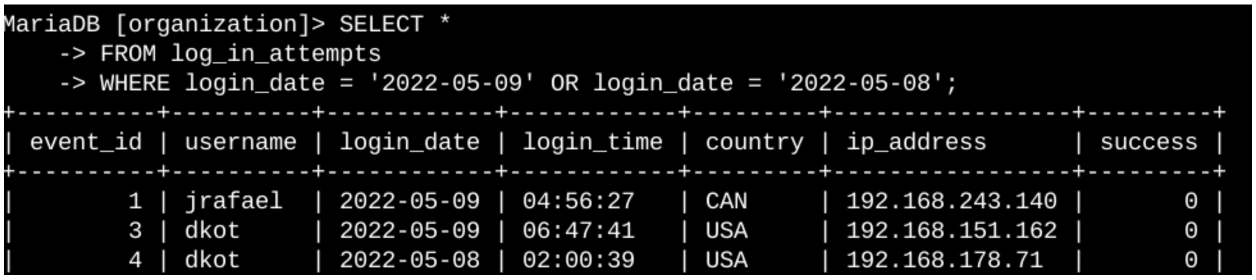


```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = FALSE;
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50  |       0 |
```

The first part of the screenshot is my query, and the second part is a portion of the output. This query filters for failed login attempts after 18:00. The first condition, `log_time > ‘18:00’` limits results to attempts made after business hours, while the second, `success = FALSE` returns only unsuccessful logins.

Retrieve login attempts on specific dates

A suspicious event took place on 2022-05-09. All login activity from that date and the previous day required investigation.

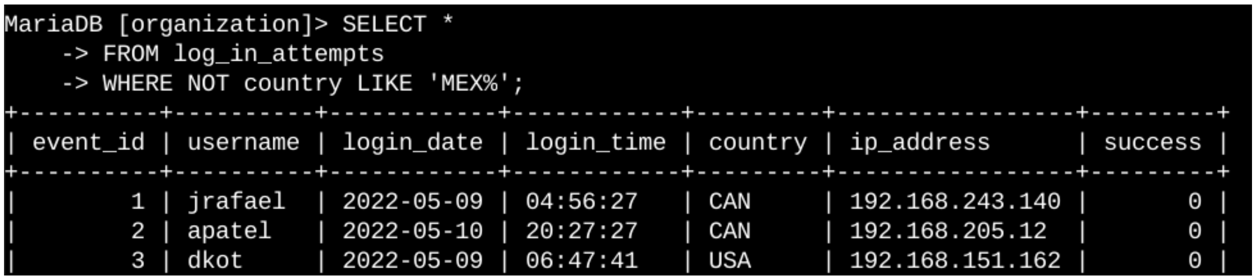


```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       0 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
```

The first part of the screenshot is my query, and the second part is a portion of the output. This query retrieves all login attempts from May 8 and 9, 2022, using an `OR` operator to return records from either date.

Retrieve login attempts outside of Mexico

Login attempts originating outside of Mexico needed to be examined.

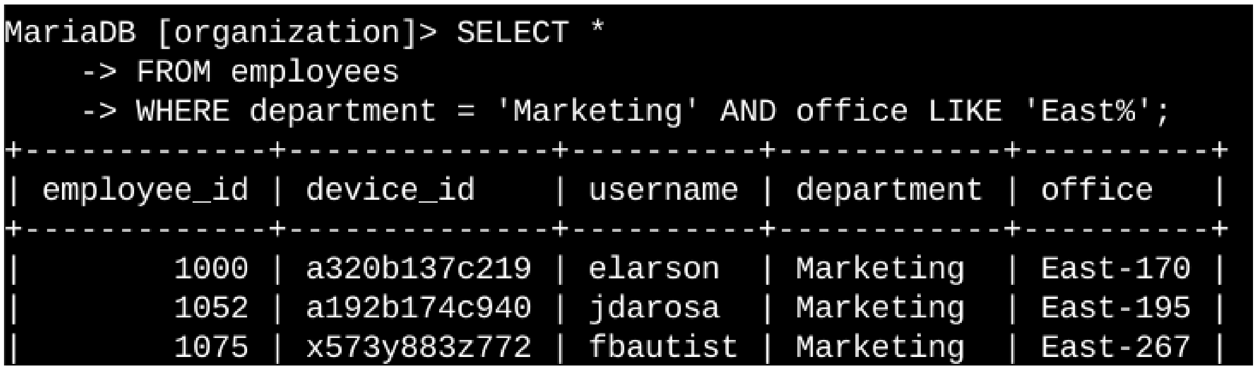


```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT country LIKE 'MEX%';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       0 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       0 |
```

The first part of the screenshot is my query, and the second part is a portion of the output. This query filters for all login attempts from countries other than Mexico. The `LIKE` operator with the pattern `MEX%` matches both "MEX" and "MEXICO." The `(%)` symbol acts as a wildcard representing any number of characters.

Retrieve employees in the Marketing department

My team needed to update computers for employees in the Marketing department located in the East building.

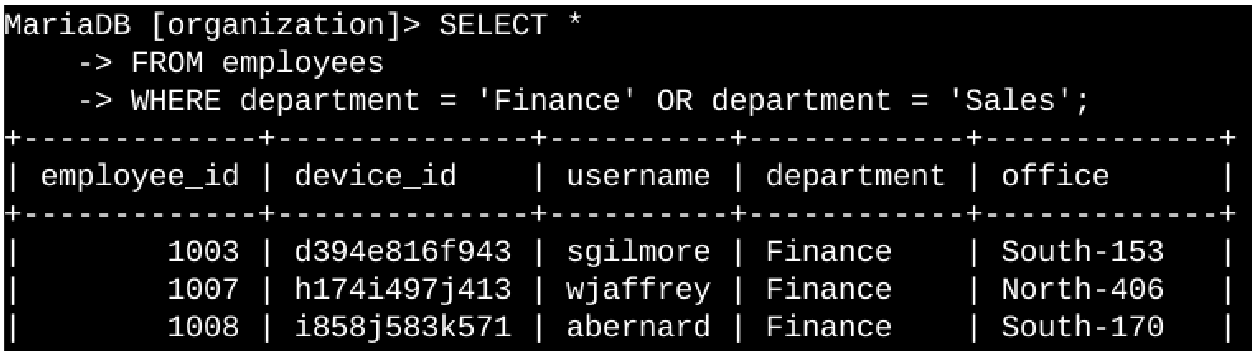


```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Marketing' AND office LIKE 'East%';
+-------------+--------------+----------+------------+-----------+
| employee_id | device_id    | username | department | office    |
+-------------+--------------+----------+------------+-----------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195 |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267 |
```

This query returns employees who work in the Marketing department and are based in the East building. The `LIKE` operator matches any record beginning with "East," accounting for specific office numbers.

Retrieve employees in Finance or Sales

Employees in the Finance and Sales departments required a separate security update.

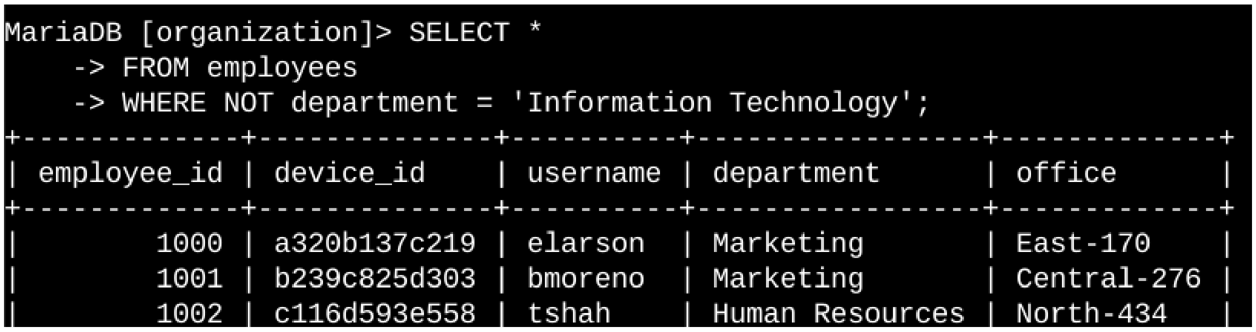


```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Finance' OR department = 'Sales';
+-------------+--------------+----------+------------+-------------+
| employee_id | device_id    | username | department | office      |
+-------------+--------------+----------+------------+-------------+
|        1003 | d394e816f943 | sgilmore | Finance    | South-153   |
|        1007 | h174i497j413 | wjaffrey | Finance    | North-406   |
|        1008 | i858j583k571 | abernard | Finance    | South-170   |
```

The first part of the screenshot is my query, and the second part is a portion of the output. This query retrieves all employees from either the Finance or Sales departments. The `OR` operator ensures results include both groups.

Retrieve all employees not in IT

The team also needed to update systems for employees outside the Information Technology department.



```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE NOT department = 'Information Technology';
+-------------+-------------+----------+-----------------+-------------+
| employee_id | device_id   | username | department      | office      |
+-------------+-------------+----------+-----------------+-------------+
|        1000 | a320b137c219 | elarson  | Marketing       | East-170    |
|        1001 | b239c825d303 | bmoreno  | Marketing       | Central-276 |
|        1002 | c116d593e558 | tshah    | Human Resources | North-434   |
```

This query returns all employees not in the IT department using the `NOT` condition.

Summary

I applied filters in SQL to extract specific information from the log_in_attempts and employees tables. By applying the `AND`, `OR`, and `NOT` operators, along with `LIKE` and the (`%`) wildcard to filter for patterns, I efficiently narrowed down the data to support system security and employee update tasks.