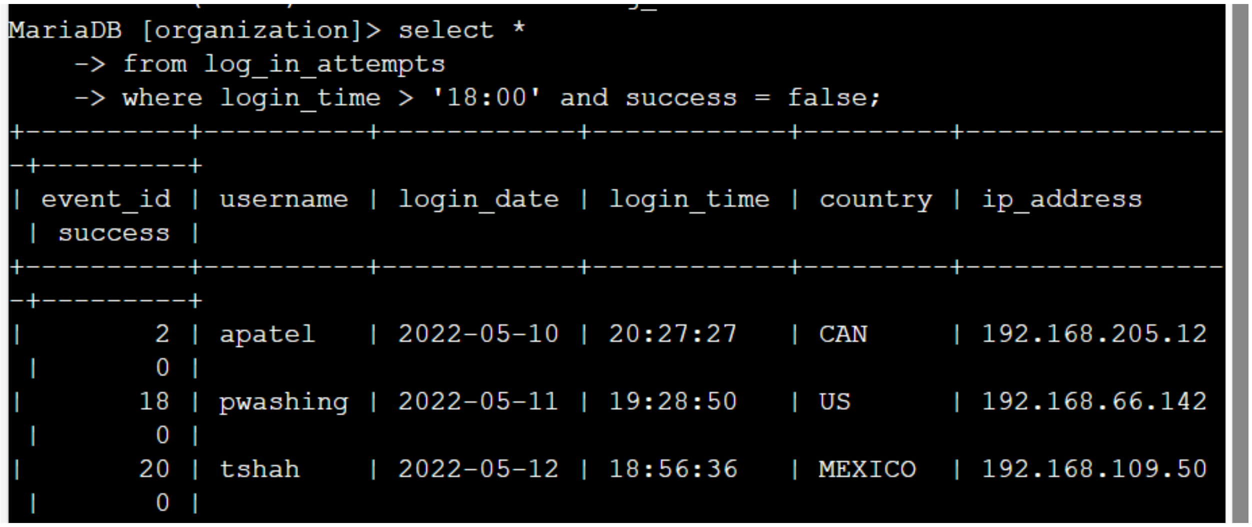
Apply filters to SQL queries

Project description

The Organization I work for has security as its utmost priority. So I was tasked with making sure that the system is safe and all updates on all employee computers are carried out when due.
I used SQL with filters to perform the different tasks I was given.

Retrieve after hours failed login attempts

We had a potential security incident and we found out that it happened after business hours (18.00). This necessitated us to query all the login attempts after close of work. So I used SQL query to filter for the login attempts from after work.



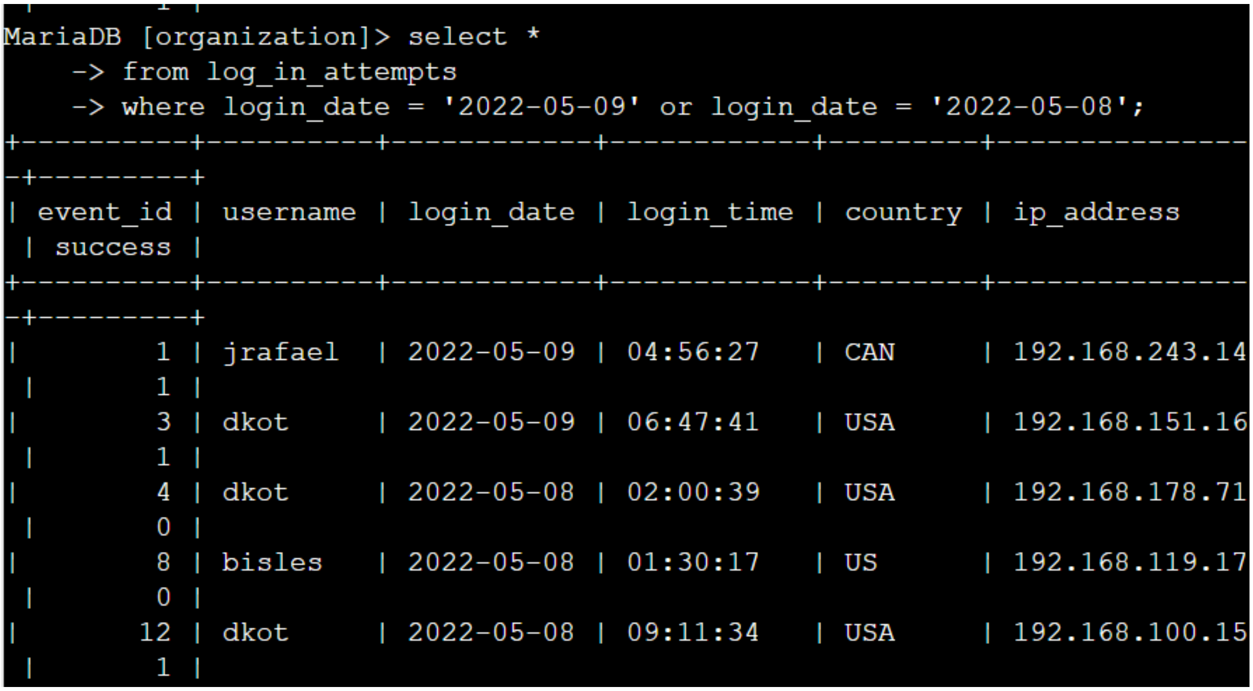
```
MariaDB [organization]> select *
    -> from log_in_attempts
    -> where login_time > '18:00' and success = false;
+----------+----------+------------+------------+---------+----------------
-+---------+
| event_id | username | login_date | login_time | country | ip_address
 | success |
+----------+----------+------------+------------+---------+----------------
-+---------+
|        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 this screenshot is my query, the second part shows a part of the output. This started by selecting all the data from the log_in_attempts table. I then used the WHERE clause with an AND operator to filter the results to show an output of all login attempts after 18.00 and returned unsuccessful.
First condition login_time > ‘18.00’, filters for login after 18.00.
Second condition success = False, filters for failed login attempts.

Retrieve login attempts on specific dates

We had an event that happened on the 22-05-09,and this was very suspicious. I was then tasked with investigating every login activity that happened on that day or the day before.

I used the following code to show how I created a SQL query to filter for the login attempts for those days.



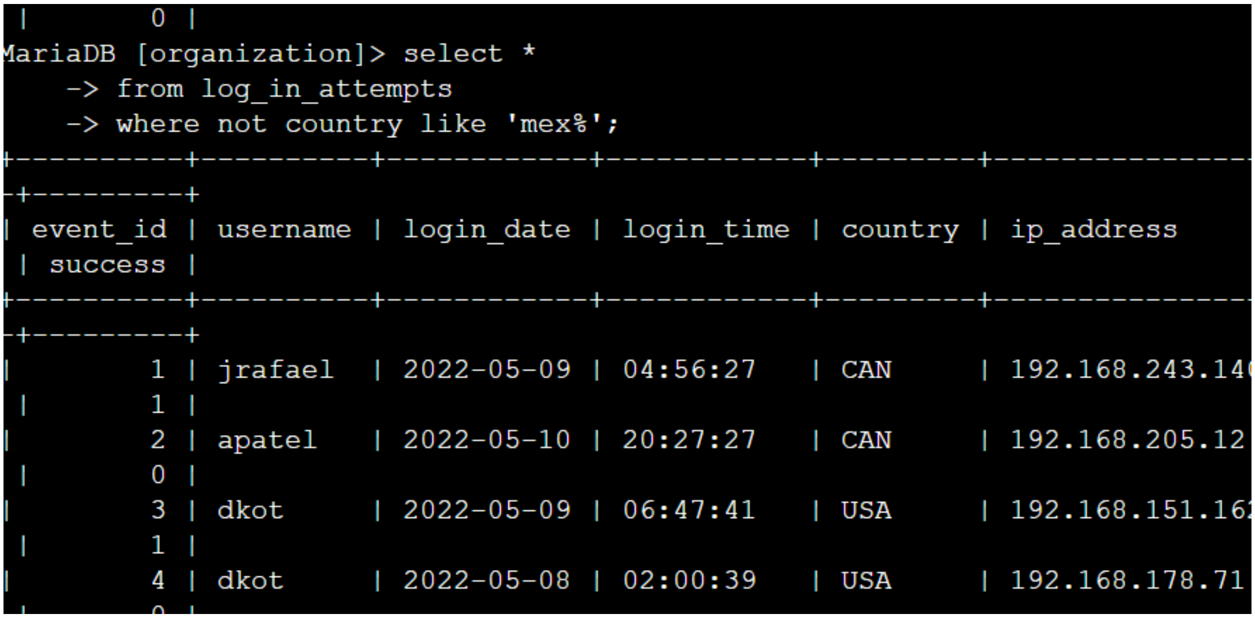
```
 |        1 |
MariaDB [organization]> select *
    -> from log_in_attempts
    -> where login_date = '2022-05-09' or login_date = '2022-05-08';
+----------+----------+------------+------------+---------+---------------
-+---------+
| event_id | username | login_date | login_time | country | ip_address
 | success |
+----------+----------+------------+------------+---------+---------------
-+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.14
 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.16
 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71
 |       0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.17
 |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.15
 |       1 |
```

The query returns all login attempts that occurred on 2-05-09 or a day before it. I started by selecting all data from the log_in_attempts,then I used the WHERE clause with the OR operator to filter the attempts on the said days.

FIRST CONDITION login_date = ‘2022-05-09’,filters for login on this date,
SECOND CONDITION login_date = ‘2022-05-08’, filters for login on the day before.

Retrieve login attempts outside of Mexico

I noticed some security concerns from the logins that came in from outside of Mexico and this made me decide to investigate further.
I used the following code to create a SQL filter to query login attempts outside of mexico.



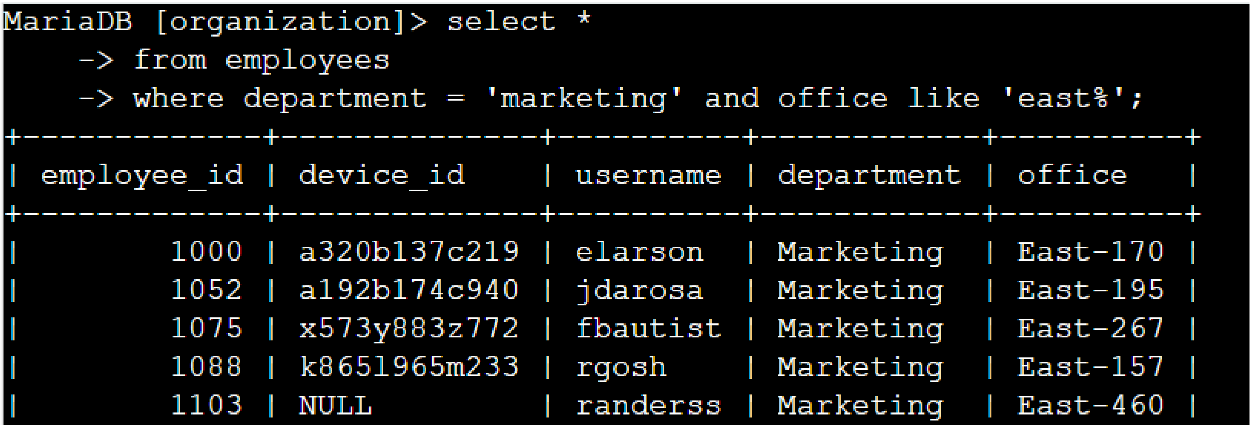
```
 |       0 |
MariaDB [organization]> select *
    -> from log_in_attempts
    -> where not country like 'mex%';
+----------+----------+------------+------------+---------+----------------
-+---------+
| event_id | username | login_date | login_time | country | ip_address
 | success |
+----------+----------+------------+------------+---------+----------------
-+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.14
 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12
 |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.16
 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71
 |       0 |
```

This query returned all login attempts that occurred in countries other than mexico. I started by selecting all the data from the log_in_attempts table,then i used a WHERE clause with NOT to

Filter for the countries other than Mexico.
Like was used with Mex% because the percentage sign represents any number of unspecified characters when used with LIKE.

Retrieve employees in Marketing

MY team wants to perform an update to the computers of some employees in the marketing department.
I used the following code to show how i used SQL query to filter employee machines from employees in the marketing department in the East building



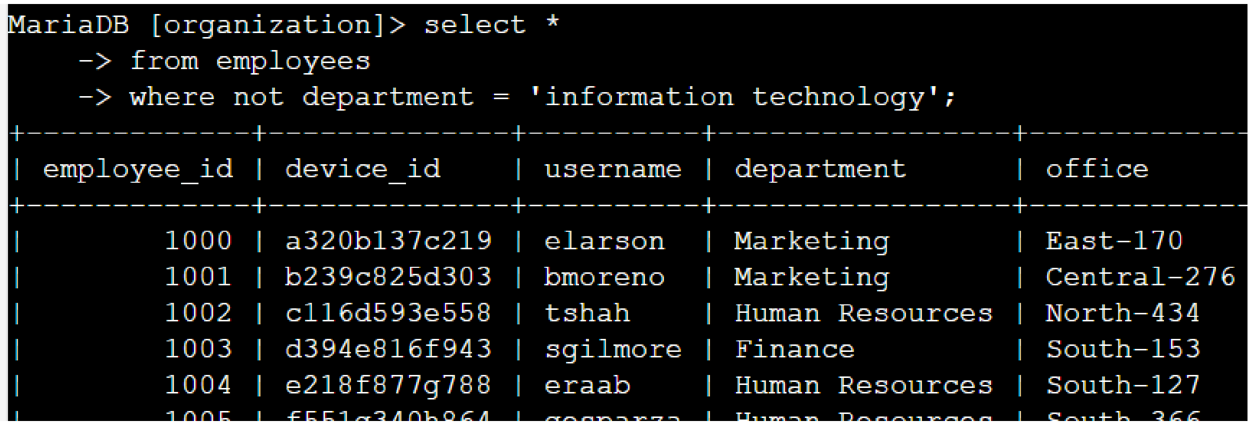
```
MariaDB [organization]> select *
    -> from employees
    -> where department = 'marketing' and office like 'east%';
+-------------+-------------+----------+------------+----------+
| employee_id | device_id   | username | department | office   |
+-------------+-------------+----------+------------+----------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195 |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267 |
|        1088 | k8651965m233 | rgosh    | Marketing  | East-157 |
|        1103 | NULL         | randerss | Marketing  | East-460 |
```

The query returned all employees in the marketing department in the East Building. I started by selecting data from the employees table. Then I used the WHERE clause with AND to filter for employees who work for the marketing department and are in the East Building.

First condition, department = ‘Marketing’ this filters for employees in the marketing department. Second condition, office LIKE ‘East%.

Retrieve all employees not in IT

My team made one more security update on employee machines from employees not bin 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
|        1003 | d394e816f943 | sgilmore | Finance         | South-153
|        1004 | e218f877g788 | eraab    | Human Resources | South-127
|        1005 | f551g340h864 | gesparza | Human Resources | South-366
```

The query returned all employees that are not in the Information Technology department.

I started by selecting all the data from the employees table. I then used the WHERE clause with NOT to filter for employees not in this department.

Summary

I introduced filters to SQL queries to get information on login attempts and employees using different machines. The two tables that I used are the log_in_attempts table and the employees table.T he operators I used for this project are the AND, OR, and NOT to filter the needed information and the LIKE and the percentage sign(%) wildcard to get information on patterns.