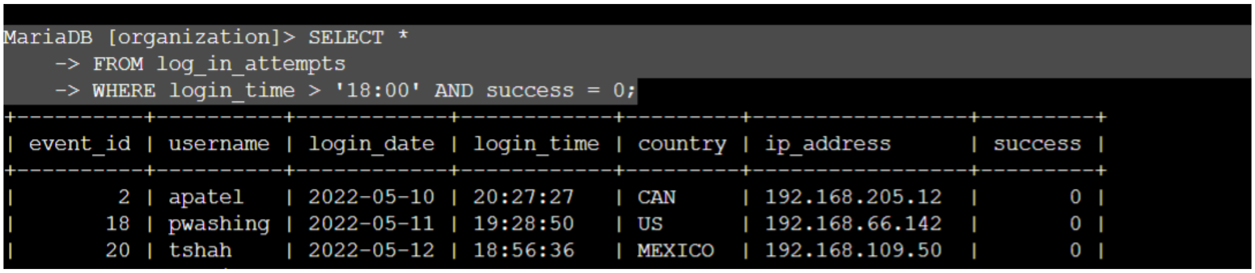
Apply filters to SQL queries

Project description

The scenario is to investigate security issues to help keep the system secure. Some potential security issues that involve login attempts and employee machines must be investigated. The following steps provide examples of how I used SQL with filters to perform security-related tasks.

Retrieve after hours failed login attempts

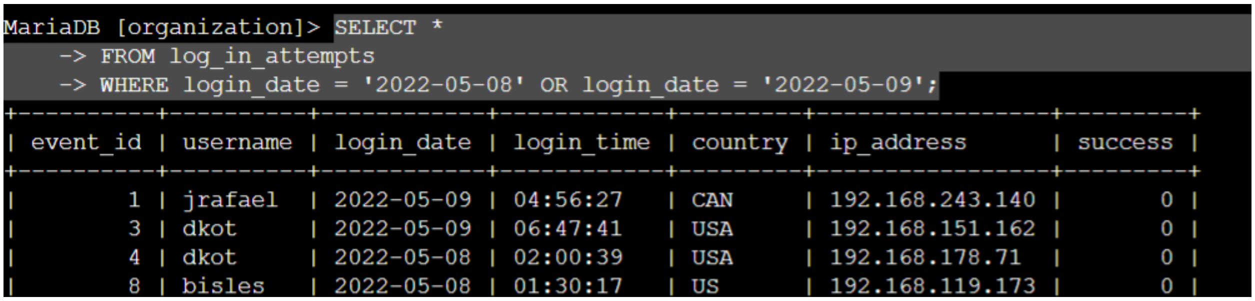
SELECT * to show all columns from the log_in_attempts table, where the filter condition is for login times after 18:00, which is outside of business hours, and for failed access attempts. AND is used to filter on two conditions. AND specifies that both conditions, after business hours and failed login attempts, must be met simultaneously. A value of 0 indicates failed login attempts. The first part of the screenshot is a query, and the second part is a portion of the output.



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = 0;
+----------+----------+------------+------------+---------+-----------------+---------+
| 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 |
```

Retrieve login attempts on specific dates

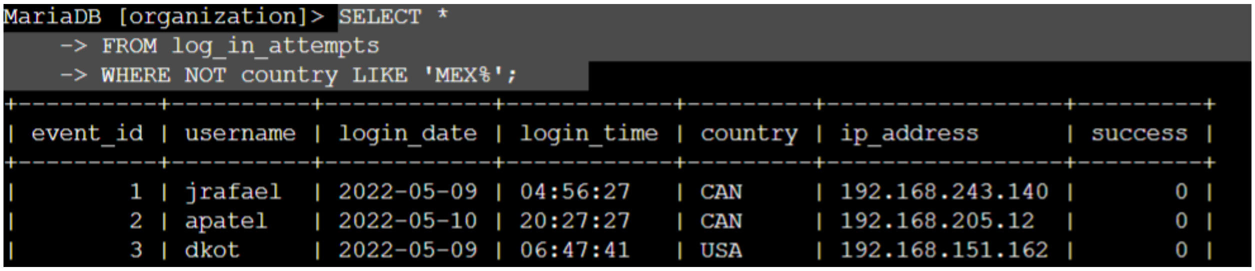
Query retrieves all columns from log_in_attempts table where login date either 2022-05-08 or the day after. The OR operator connects two conditions, but OR specifies that either condition can be met. It returns results where either the first condition (login date is 2022-05-08), the second condition (login date is 2022-05-09), or both are met.



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-08' OR login_date = '2022-05-09';
+----------+----------+------------+------------+---------+-----------------+---------+
| 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 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |       0 |
```

Retrieve login attempts outside of Mexico

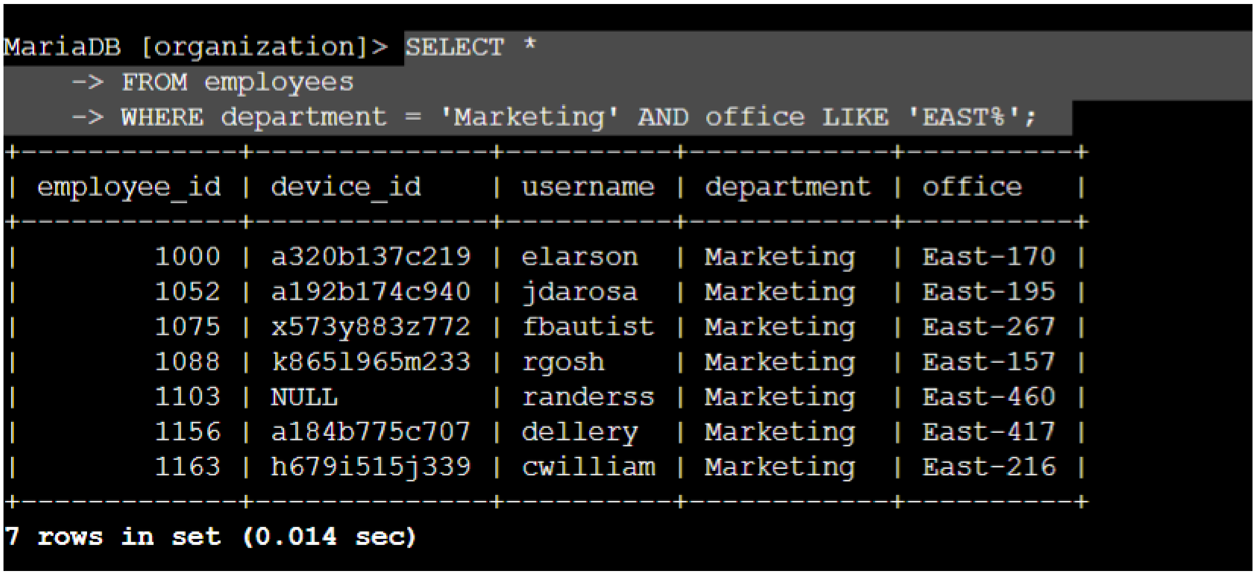
The query retrieves all columns from the log_in_attempts table where the country is not Mexico. The NOT operator filters output based on countries. The NOT operator negates a condition. This means that SQL returns all records that don't match the condition specified in the query. LIKE is used with WHERE to search for a pattern which is 'MEX' in a column.



```
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 |
```

Retrieve employees in Marketing

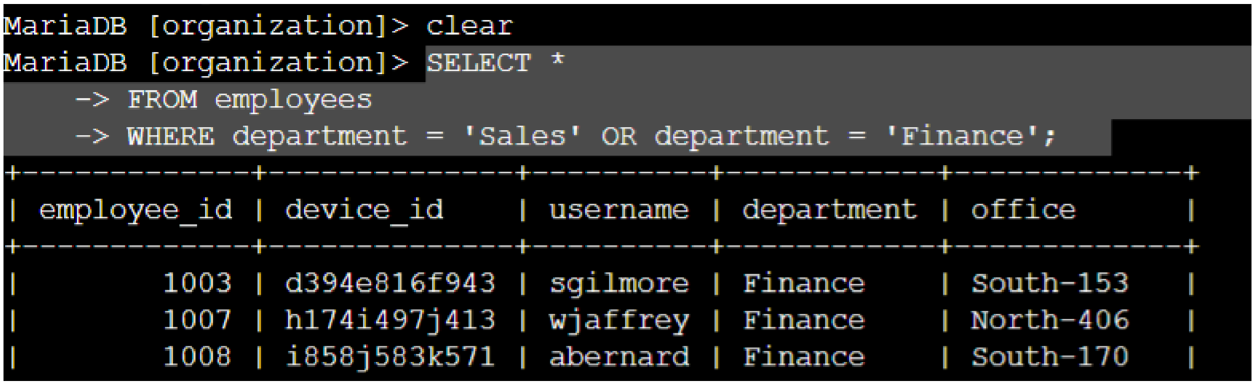
The query retrieves all columns from the log_in_attempts table where all employees in the Marketing department for all offices in the East building. AND is used to filter on two conditions. This query returns all records with values in the office column that start with the pattern of 'east'. This means all employees in the East office are returned.



```
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 |
|        1156 | a184b775c707 | dellery  | Marketing  | East-417 |
|        1163 | h679i515j339 | cwilliam | Marketing  | East-216 |
+-------------+--------------+----------+------------+----------+
7 rows in set (0.014 sec)
```

Retrieve employees in Finance or Sales

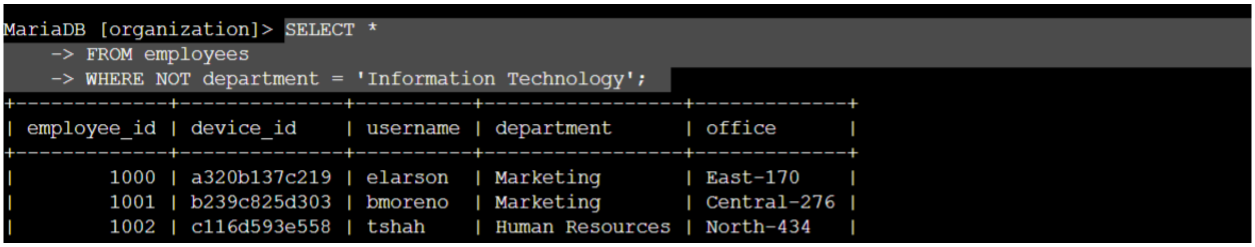
Now needed to perform a different security update on machines for employees in the Sales and Finance departments. First, selecting all data from the employees table. Then, used a WHERE clause with OR to filter for employees who are in the Finance and Sales departments. The OR operator displays employees from either the Sales or the Finance departments.



```
MariaDB [organization]> clear
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Sales' OR department = 'Finance';
+-------------+--------------+----------+------------+-------------+
| 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   |
```

Retrieve all employees not in IT

One more update needed to employee machines.The employees who are in the Information Technology department already had this update, but employees in all other departments need it. The NOT operator is used in SQL to create a query that identifies all employees who are not in the IT 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   |
```

Summary

In this project, I applied filters to SQL queries to extract specific information about login attempts and employee machines. I examined the organization's data in their employees and log_in_attempts tables. 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.