Apply filters to SQL queries

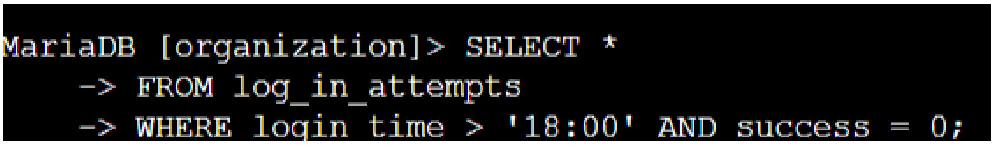
Project description

I am using SQL to complete a hypothetical activity where I am a security professional at a large organization. Using SQL is useful for obtaining information from the database quickly.

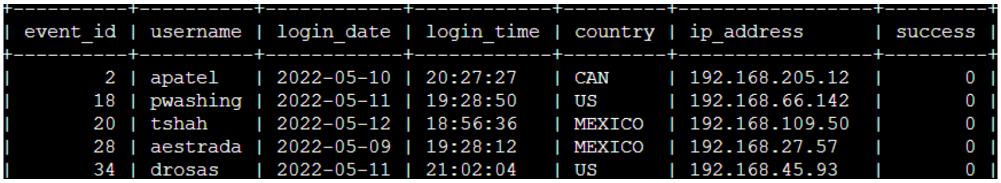
There have been some potential security issues regarding login attempts and employee machines. I am tasked to examine the organization's data in the employees and login attempts tables in order to investigate these issues. I will use logical operators such as AND, OR, and NOT as filters in order to add results specific to the security threat given. I will be providing screenshots of queries used when obtaining data from SQL for each scenario.

Retrieve after-hours failed login attempts

A potential security incident occurred after business hours; to investigate this I used a filter in SQL when putting a query in the log_in_attempts tables. With the WHERE operator, I selected the “login_time” along with the “>” symbol to retrieve all attempts after 18:00 hours. Additionally, I added another condition to show all failed successes after that time using the AND filter, which ensured both conditions would be met in the query. Because the table is reflected in binary numbers, True can be represented as 1, and false can be represented by 0. There were 19 failed login attempts.



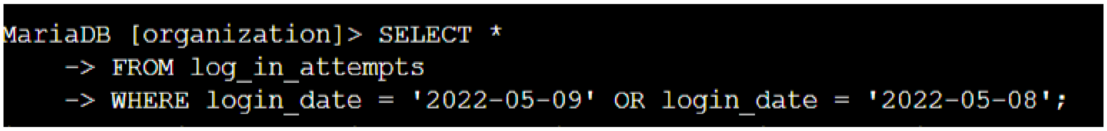
```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = 0;
```



```
+----------+----------+------------+------------+---------+-----------------+---------+
| 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 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |       0 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93   |       0 |
```

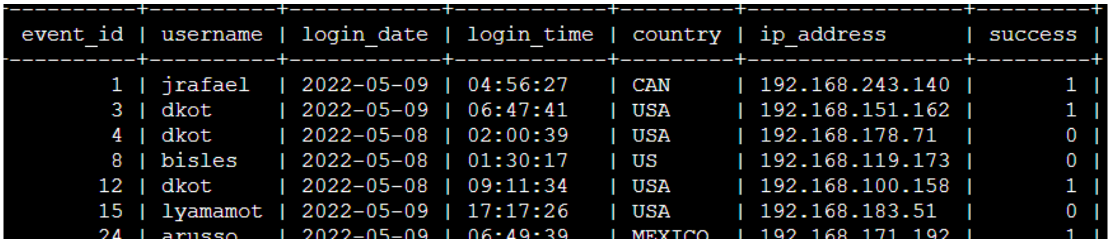
Retrieve login attempts on specific dates

There was a suspicious event that occurred on 2022-05-09; to investigate this, I will be reviewing all login attempts made on this day and the day before. I submitted a query using the OR filter so that either condition can be met. The query results will show all login attempts made within 2022-05-09 or 2022-05-08.



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

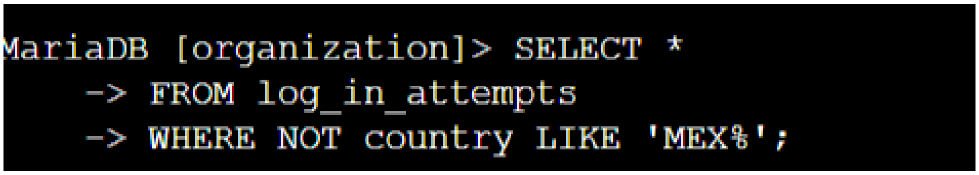
Results...



```
----------+----------+------------+------------+---------+-----------------+---------+
 event_id | username | login_date | login_time | country | ip_address      | success |
----------+----------+------------+------------+---------+-----------------+---------+
        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       1 |
        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |       0 |
       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158 |       1 |
       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51  |       0 |
       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.192 |       1 |
```

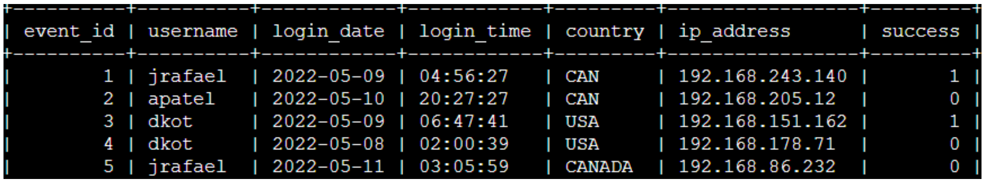
Retrieve login attempts outside of Mexico

There were potentially suspicious activities found; however, they did not originate in Mexico. I used SQL to retrieve the login data for all users who did not reside in Mexico. The "LIKE" operator, also used in place of an equal sign, was used with the "%" as a wild card due to some of the country names being abbreviated as MEX versus Mexico. The results will reflect all login attempts for all users not in Mexico.



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT country LIKE 'MEX%';
```

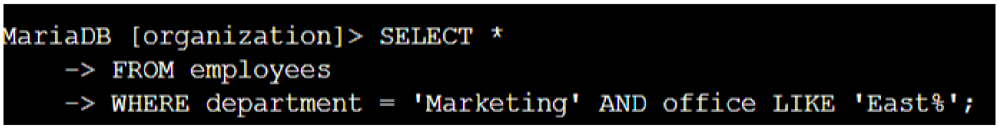
Results...



```
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |       0 |
```

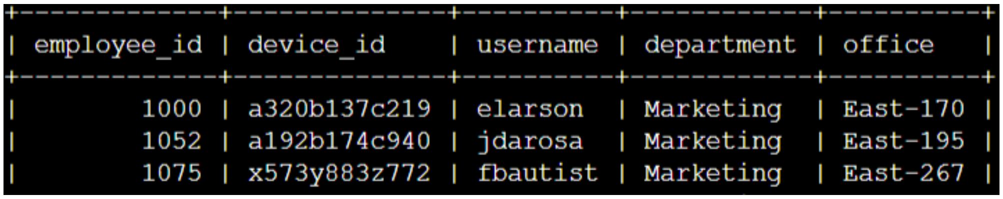
Retrieve employees in Marketing

I am tasked to provide security updates for employees in the Marketing team in the East building. I have used SQL to retrieve data from the specified employees. I have used the AND filter in order to have both the department and office conditions met. Because there are multiple office numbers, I have also included the “LIKE” operator to include all office numbers in the East building. This query will return only those in the Marketing department with an office that contains “East”.



```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Marketing' AND office LIKE 'East%';
```

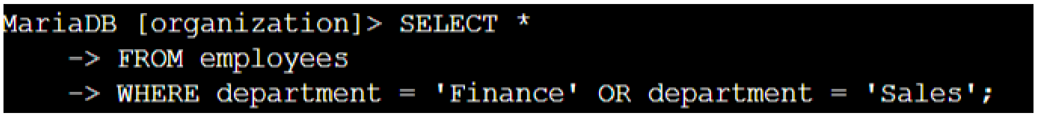
Results...



```
+-------------+---------------+----------+------------+----------+
| 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 |
```

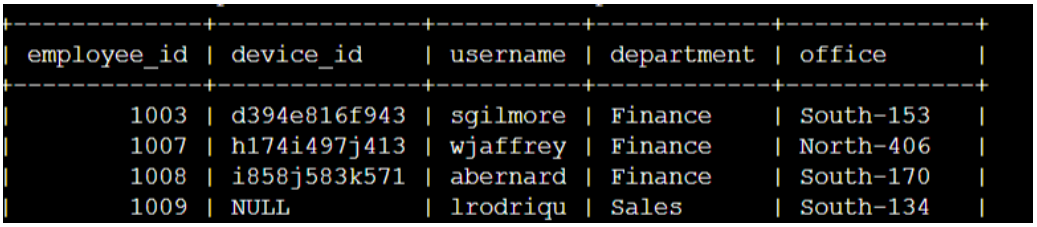
Retrieve employees in Finance or Sales

The team has been provided with a task to update information for employees in the Finance and Sales Departments. When retrieving data in SQL, I have used the “OR” filter in my query so the table results will show me only those in either department. Although I am filtering from the same column, I still specified each filter. The query results will show all employees from the Finance or the Sales department.



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

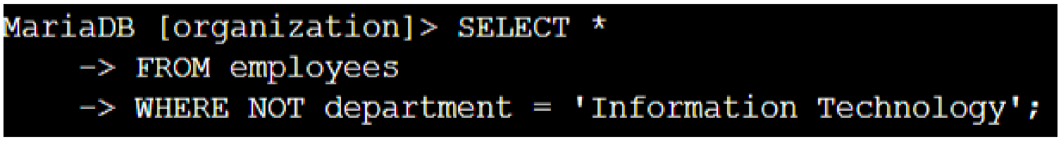
Results...



```
+-------------+---------------+----------+------------+-------------+
| 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   |
|        1009 | NULL          | lrodriqu | Sales      | South-134   |
```

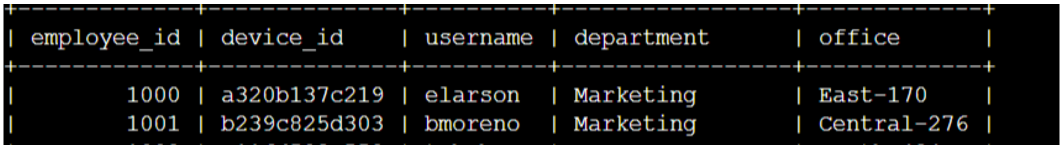
Retrieve all employees not in IT

There is a final update required for the employee in the organization; however, all persons in the IT department have already received this update. The query I used will include the “NOT” filter, which will negate this condition. This filter is used directly after an operator such as “WHERE”. This will show me all the results of employees who are not in the IT department.



```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE NOT department = 'Information Technology';
```

Results…



```
+-------------+---------------+----------+-----------------+-------------+
| employee_id | device_id     | username | department      | office      |
+-------------+---------------+----------+-----------------+-------------+
|        1000 | a320b137c219  | elarson  | Marketing       | East-170    |
|        1001 | b239c825d303  | bmoreno  | Marketing       | Central-276 |
```

SELECT * (The word SELECT is used along with the “*” as a way to select all columns in the specified table.)
FROM employees (FROM is used to specify the table we are pulling the information from)
WHERE NOT *department* = 'Information Technology'; (WHERE is used as a condition, like “where’ are we getting the information from in the table, and what are we filtering. “NOT” is an example of a filter used along with operators such as WHERE to add a specific condition negating a condition; “*department”* is the condition.) In this example, the query tells me that I am attempting to get data FROM all the “employees” table data, but only show me those that are NOT in the Information Tecnology department.

Summary

There are many ways to protect an organization from cyber threats, and SQL is an important tool that makes it easy to obtain a huge amount of information from, as well as to create and interact with the database effectively. SQL was used to obtain specific data in order to investigate issues regarding login attempts and employee machines. In this project, operators such as AND, OR, and NOT were used to combine or negate conditions when investigating scenarios. These are logical operators that help apply specific filters when looking for threat-related information.