Apply filters to SQL queries

Project description

The research team at my organization needs to update the file permissions for specific files and directories within the "projects" directory, as the current permissions do not align with the required authorization levels. Updating these permissions will enhance system security. To accomplish this, I carried out the following tasks:

Retrieve after hours failed login attempts

A potential security incident occurred after business hours (after 18:00). Any failed login attempts during this time need to be investigated.

The following code shows how I created an SQL query to filter for failed login attempts that took place after business hours..

```
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 shows my query, and the second part shows a portion of the output. This query filters for failed login attempts that happened after 18:00. First, I selected all data from the "log_in_attempts" table. Then, I used a WHERE clause with an AND operator to filter the results for login attempts that occurred after 18:00 and were unsuccessful. The first condition, `login_time > '18:00'`, filters for attempts after 18:00. The second condition, `success = FALSE`, filters for failed login attempts.

Retrieve login attempts on specific dates

A suspicious event took place on 2022-05-09. Any login activity on that day or the day before needs to be investigated.

The following code shows how I created an SQL query to filter for login attempts that occurred on those specific dates.

```
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 shows my query, and the second part shows a portion of the output. This query returns all login attempts that occurred on 2022-05-09 or 2022-05-08. First, I selected all data from the "log_in_attempts" table. Then, I used a WHERE clause with an OR operator to filter the results to show only login attempts on either 2022-05-09 or 2022-05-08. The first condition, `login_date = '2022-05-09'`, filters for logins on 2022-05-09. The second condition, `login_date = '2022-05-08'`, filters for logins on 2022-05-08.

Retrieve login attempts outside of Mexico

After reviewing the organization's data on login attempts, I believe there is an issue with the attempts made outside of Mexico. These login attempts should be investigated.

The following code shows how I created an SQL query to filter for login attempts that occurred outside of Mexico.

```
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 shows my query, and the second part shows a portion of the output. This query returns all login attempts that occurred in countries other than Mexico. First, I selected all data from the "log_in_attempts" table. Then, I used a WHERE clause with NOT to filter out Mexico. I used the LIKE operator with "MEX%" as the pattern, since the dataset represents Mexico as "MEX" or "MEXICO." The

percentage sign (%) is a wildcard in LIKE, meaning it matches any number of characters.

Retrieve employees in Marketing

My team plans to update the computers for certain employees in the Marketing department. To do this, I need to gather information about which employee machines need updating.

The following code shows how I created an SQL query to filter for employee machines from 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 |
```

The first part of the screenshot shows my query, and the second part displays a portion of the output. This query returns all employees in the Marketing department located in the East building. First, I selected all data from the "employees" table. Then, I used a WHERE clause with AND to filter for employees who are in the Marketing department and work in the East building. I used LIKE with "East%" to match the office column, as it represents the East building along with the specific office number. The first condition, `department = 'Marketing'`, filters for employees in the Marketing department. The second condition, `office LIKE 'East%'`, filters for employees in the East building.

Retrieve employees in Finance or Sales

The machines for employees in the Finance and Sales departments also need to be updated. Since a different security update is required, I need to gather information on employees from only these two departments.

The following code shows how I created an SQL query to filter for employee machines from employees in the Finance or Sales departments.

```
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 shows my query, and the second part displays a portion of the output. This query returns all employees in the Finance and Sales departments. First, I selected all data from the "employees" table. Then, I used a WHERE clause with OR to filter for employees in either the Finance or Sales departments. I used the OR operator instead of AND because I want to include employees from both departments. The first condition, `department = 'Finance'`, filters for employees in the Finance department. The second condition, `department = 'Sales'`, filters for employees in the Sales department.

Retrieve all employees not in IT

My team needs to make one more security update for employees who are not in the Information Technology department. To do this, I first need to gather information on these employees.

The following shows how I created an 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';
+-------------+-------------+----------+-----------------+-------------+
| 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   |
```

The first part of the screenshot shows my query, and the second part displays a portion of the output. This query returns all employees who are not in the Information Technology department. First, I selected all data from the "employees" table. Then, I used a WHERE clause with NOT to filter for employees who are not in this department.

Summary

I applied filters to SQL queries to gather specific information on login attempts and employee machines, using two different tables: log_in_attempts and employees. I utilized the AND, OR, and NOT operators to narrow down the data for each task. Additionally, I used the LIKE operator along with the percentage sign (%) wildcard to filter for specific patterns.