Portfolio Activity: Apply filters to SQL queries

Project description

This project demonstrates how to filter and retrieve specific information from SQL tables in a cybersecurity context. Using the log_in_attempts and employees tables, I performed queries to investigate security issues, identify after-hours failed logins, check login activity on specific dates, and retrieve employee information based on department and office location.

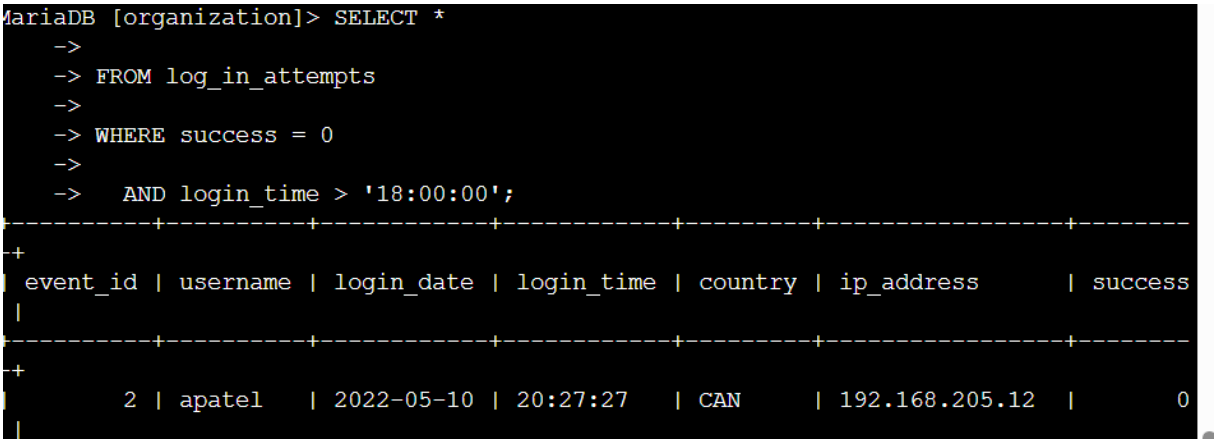
Retrieve after hours failed login attempts

Query:

```
SELECT *

FROM log_in_attempts

WHERE success = 0

  AND login_time > '18:00:00';
```

Explanation:
This query selects all records where the login attempt failed (success = 0) and occurred after 6 PM. It helps identify potential security issues outside of regular business hours.

Output:



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

Retrieve login attempts on specific dates

Query:

```
SELECT *

FROM log_in_attempts
```

```
WHERE login_date = '2022-05-09'
  OR login_date = '2022-05-08';
```

Explanation:
This query filters login attempts that occurred on May 8 and May 9, 2022, to investigate a suspicious event. The OR operator allows selecting multiple dates.

Output:

```
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 |       1
 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1
```

Retrieve login attempts outside of Mexico

Query:

```
SELECT *
FROM log_in_attempts
WHERE country NOT LIKE 'MEX%'
  AND country NOT LIKE 'MEXICO%';
```

Explanation:
This query retrieves all login attempts outside Mexico. The NOT LIKE operator excludes any country values starting with "MEX" or "MEXICO".

Output:

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE country NOT 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 |       1
 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0
 |
```

Retrieve employees in Marketing

Query:

```
SELECT *

FROM employees

WHERE department LIKE '%Marketing%'

  AND office LIKE 'East%';
```

Explanation:
This query identifies employees in the Marketing department located in any office in the East building. The LIKE operator with % matches any characters before or after the keyword.

Output:

```
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE department LIKE '%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 (0.003 sec)
```

Retrieve employees in Finance or Sales

Query:

```
SELECT *

FROM employees

WHERE department LIKE '%Finance%'

   OR department LIKE '%Sales%';
```

Explanation:
This query retrieves all employees in either the Finance or Sales departments. The OR operator allows filtering multiple conditions.

Output:

```
MariaDB [organization]>
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE department LIKE '%Finance%'
    ->
    ->    OR department LIKE '%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   |
```

Retrieve all employees not in IT

Query:

```
SELECT *

FROM employees

WHERE department NOT LIKE '%Information Technology%';
```

Explanation:
This query selects all employees who are not in the Information Technology department. The NOT LIKE operator excludes IT employees.

Output:

```
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE department NOT LIKE '%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   |
```

Summary

In this project, I applied SQL queries to filter records in log_in_attempts and employees tables. I used AND, OR, NOT, LIKE, and date/time filters to investigate potential security issues and retrieve employee information. These queries demonstrate my ability to analyze data, identify anomalies, and prepare reports for cybersecurity purposes.
