Security Related SQL Queries

Project description

Knowledge of SQL and DBMS are essential to security professionals and backend engineers alike. Though taking a class on relation databases during my undergrad, this was a nice refresher exercise in SQL queries with a security focus. In this project, I'll be using MariaDB (a MySQL fork) to investigate a security incident that happened after business hours on a company database.

Retrieve after hours failed login attempts

I know that the incident happened after business hours (18:00) and I want to investigate the failed login attempts for my investigation. The query I would use for this is:

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

As you can see, I am using **the log_in_attempts** DB and searching for afterhours logins (> 18:00) that failed (success = 0).

Retrieving login attempts on specific dates

Lets say that I wanted to refine my search and look for login attempts on specific days. I could use multiple queries, however it would be more advantageous to use the OR operator, as pictured below:

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

Continued...

Retrieving login attempts outside of Mexico

Sometimes, however, it becomes necessary to use wildcards especially when searching for string datatypes. In the example database, the 'country' column includes both 'Mexico' and 'Mex' as country names (both in reference to Mexico). Lets imagine I wanted to search for all login attempts that originated from places other than Mexico. In this instance, I would use the wildcard '%' and the 'LIKE' operator to search for logins that were attempted outside of Mexico. See below:

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

Retrieving employees in Marketing

The above example is rather simple. An example of a slightly more complicated but useful query would be, say if I wanted to find all of the employees in the Marketing department who worked in the company's eastern complex. Unfortunately for me, I have to account for the fact that the 'office' datatype includes the region as well as the building number (ex: East_170).

```
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 (0.002 sec)
```

Retrieving employees in Finance or Sales

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Finance' OR '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   |
|        1010 | k2421212m542 | jlansky  | Finance    | South-109   |
|        1015 | p611q262r945 | jsoto    | Finance    | North-271   |
|        1017 | r550s824t230 | jclark   | Finance    | North-188   |
|        1018 | s310t540u653 | abellmas | Finance    | North-403   |
|        1022 | w237x430y567 | arusso   | Finance    | West-465    |
|        1029 | d336e475f676 | ivelasco | Finance    | East-156    |
```

Retrieving all employees not in IT

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department != 'Information Technology';
```

Summary

My knowledge of relational databases spans beyond this example's scope. I would feel comfortable designing and implementing tables for my own projects or that of an organization. However, I hope the above examples provide clear evidence that I am comfortable with SQL. Beyond using MySQL/MariaDB I would feel comfortable writing code to automate any repetitive queries that were time intensive.