Table formats

This document describes how the tables used for this portfolio activity are organized. The `organization` database contains the following two tables:

- `log_in_attempts`
- `employees`

log_in_attempts

The `log_in_attempts` table has the following columns:

- `event_id`: The identification number assigned to each login event
- `username`: The username of the employee
- `login_date`: The date the login attempt was recorded
- `login_time`: The time the login attempt was recorded
- `country`: The country where the login attempt occurred
- `ip_address`: The IP address of that employee's machine
- `success`: The success of the login attempt; `FALSE` indicates a failed attempt

In the MariaDB shell, these columns are returned as:

```
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
```

employees

The `employees` table has the following columns:

- `employee_id`: The identification number assigned to each employee
- `device_id`: The identification number assigned to each device used by the employee
- `username`: The username of the employee
- `department`: The department the employee is in
- `office`: The office the employee is located in

In the MariaDB shell, these columns are returned as:

```
+-------------+--------------+----------+------------------------+-------------+
| employee_id | device_id    | username | department             | office      |
+-------------+--------------+----------+------------------------+-------------+
```

Apply filters to SQL queries

Project description

This project is concerned with investigating and addressing potential security incidents within an organization's employee database. Using SQL, we perform various queries to retrieve specific information from the `log_in_attempts` and `employees` tables. These queries help identify after-hours failed login attempts, suspicious login activities on particular dates, login attempts outside of a specified country, and employee information based on departmental and office location filters. The results aid in performing targeted security updates and investigations.

Retrieve after hours failed login attempts

```
SELECT *
FROM log_in_attempts
WHERE login_time > '18:00:00'
  AND success = FALSE;
```

This query retrieves all columns from the `log_in_attempts` table where the `login_time` is later than 18:00 (6:00 PM) and the `success` column indicates a failed login attempt. The `AND` operator is used to combine these two conditions.

Retrieve login attempts on specific dates

```
SELECT *
FROM log_in_attempts
WHERE login_date = '2022-05-09'
   OR login_date = '2022-05-08';
```

This query retrieves all columns from the `log_in_attempts` table where the `login_date` is either 2022-05-09 or 2022-05-08. The `OR` operator is used to include login attempts from both dates.

Retrieve login attempts outside of Mexico

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

This query retrieves all columns from the `log_in_attempts` table where the `country` column does not start with 'MEX' or 'MEXICO'. The `NOT LIKE` operator is used to exclude records where the country is either 'MEX' or 'MEXICO'.

Retrieve employees in Marketing

```
SELECT *
FROM employees
WHERE department = 'Marketing'
 AND office LIKE 'East-%';
```

This query retrieves all columns from the `employees` table where the `department` is 'Marketing' and the `office` column indicates a location in the East building. The `LIKE` operator with a wildcard `%` is used to match any office location that starts with 'East-'.

Retrieve employees in Finance or Sales

```
SELECT *
FROM employees
WHERE department = 'Sales'
  OR department = 'Finance';
```

This query retrieves all columns from the `employees` table where the `department` is either 'Sales' or 'Finance'. The `OR` operator is used to include employees from both departments.

Retrieve all employees not in IT

```
SELECT *
FROM employees
WHERE NOT department = 'Information Technology';
```

This query retrieves all columns from the `employees` table where the `department` is not 'Information Technology'. The `NOT` operator is used to exclude records where the department is 'Information Technology'.

Summary

We executed a series of SQL queries to filter and retrieve relevant data from the `log_in_attempts` and `employees` tables. The queries focused on identifying after-hours failed login attempts, login attempts on specific dates, and those occurring outside of Mexico. Additionally, we retrieved employee information for those in specific departments and offices, excluding those in the Information Technology department. These tasks support the overall goal of investigating security incidents and performing necessary updates to employee machines.

Example of work in terminal:

```
MariaDB [organization]> clear
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 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157   |       0 |
|       52 | cjackson | 2022-05-10 | 22:07:07   | CAN     | 192.168.58.57   |       0 |
|       69 | wjaffrey | 2022-05-11 | 19:55:15   | USA     | 192.168.100.17  |       0 |
|       82 | abernard | 2022-05-12 | 23:38:46   | MEX     | 192.168.234.49  |       0 |
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANADA  | 192.168.132.153 |       0 |
|       96 | ivelasco | 2022-05-09 | 22:36:36   | CAN     | 192.168.84.194  |       0 |
|      104 | asundara | 2022-05-11 | 18:38:07   | US      | 192.168.96.200  |       0 |
|      107 | bisles   | 2022-05-12 | 20:25:57   | USA     | 192.168.116.187 |       0 |
|      111 | aestrada | 2022-05-10 | 22:00:26   | MEXICO  | 192.168.76.27   |       0 |
|      127 | abellmas | 2022-05-09 | 21:20:51   | CANADA  | 192.168.70.122  |       0 |
|      131 | bisles   | 2022-05-09 | 20:03:55   | US      | 192.168.113.171 |       0 |
|      155 | cgriffin | 2022-05-12 | 22:18:42   | USA     | 192.168.236.176 |       0 |
|      160 | jclark   | 2022-05-10 | 20:49:00   | CANADA  | 192.168.214.49  |       0 |
|      199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO  | 192.168.44.232  |       0 |
+----------+----------+------------+------------+---------+-----------------+---------+
19 rows in set (0.001 sec)

MariaDB [organization]>
```