Logical Filters in SQL

Project description

This simulation project puts the performer, **Maheswar Reddy Avula**, into the position of a system administrator for an organization. Responsibilities include obtaining specific information about employees, their machines, and the departments they belong to from the database. The team needs this data to investigate potential security issues and to update computers.

(For readability and simplicity, the outputs have been limited to 5 table entries out of 200)

Retrieve after hours failed login attempts

Direction: The team is investigating failed login attempts that were made after business hours. The admin must retrieve this information from the login activity by identifying all unsuccessful attempts after 18:00.

The and operator was used to specify 2 conditions in conjunction as being **login_time** after **18:00** and **success = 0**(failed attempt) to get the desired results as follows:

```
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

Direction: The team is investigating a suspicious event that occurred on **'2022-05-09'**. The admin must retrieve all login attempts that occurred on this day and the day before ('2022-05-08').

The or operator was used to define the login_date as either '2022-05-08' or **'2022-05-09'** to display the result as follows:

```
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 |       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

Direction: The team is now updating employee machines, so the admin must obtain the information about employees in the **Marketing** department who are located in all offices in the **East** building.

The and operator along with the **like** operator was used to define the department as **Marketing** and the **office** as starting with the letters **East___** as follows:

```
MariaDB [organization]> select * from employees where department = 'Marketing' and of
fice 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 |
+-------------+--------------+----------+------------+----------+
```

Retrieve employees in Finance or Sales

Direction: The team needs to perform a different update to the computers of all employees in the **Finance** or the **Sales** department, so the admin must locate information on these employees.

The **or** operator was used to retrieve employee information of the **Finance** and **Sales** departments using the following query:

```
MariaDB [organization]> select * from employees where department = 'Finance' or depar
tment = '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   |
|        1009 | NULL         | lrodriqu | Sales      | South-134   |
|        1010 | k2421212m542 | jlansky  | Finance    | South-109   |
|        1011 | l748m120n401 | drosas   | Sales      | South-292   |
```

Retrieve all employees not in IT

Direction: The team needs to make one more update. This update was already made to employee computers in the Information Technology department. The team needs information about employees who are not in that department.

To do the above task, the **not** operator was used to exclude the employees of the **Information Technology** department from the query results as follows:

```
MariaDB [organization]> select * from employees where not department = "Inforamtion T
echnology";
+-------------+-------------+----------+-----------------------+-------------+
| 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   |
|        1004 | e218f877g788 | eraab    | Human Resources       | South-127   |
|        1005 | f551g340h864 | gesparza | Human Resources       | South-366   |
```

Summary

All information required to carry out the updates was successfully obtained and displayed. All tasks were successfully completed in accordance with the directions given by the organization.