Apply filters to SQL queries

Project description

This project if from SQL module.

“You are a security professional at a large organization. Part of your job is to investigate security issues to help keep the system secure. You recently discovered some potential security issues that involve login attempts and employee machines.

Your task is to examine the organization’s data in their employees and log_in_attempts tables. You’ll need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.”

Retrieve after hours failed login attempts

I acted as someone who doesn't know how data are organized. I started by describing the table.

```
MariaDB [organization]> DESCRIBE log_in_attempts;
+------------+-------------+------+-----+---------+-------+
| Field      | Type        | Null | Key | Default | Extra |
+------------+-------------+------+-----+---------+-------+
| event_id   | int(11)     | NO   | PRI | NULL    |       |
| username   | varchar(16) | NO   |     | NULL    |       |
| login_date | date        | NO   |     | NULL    |       |
| login_time | time        | NO   |     | NULL    |       |
| country    | varchar(16) | NO   |     | NULL    |       |
| ip_address | varchar(16) | NO   |     | NULL    |       |
| success    | tinyint(1)  | YES  |     | NULL    |       |
+------------+-------------+------+-----+---------+-------+
7 rows in set (0.001 sec)
```

For this project, the after hour is “18:00”.

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

```
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      | su
ccess |
+----------+----------+------------+------------+---------+-----------------+---
------+
|        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 (0.003 sec)
```

They asked me how many failed connections were after hours so I could also consider use:

SELECT COUNT(*)
FROM log_in_attempts
WHERE login_time > 18:00 AND success = false;

```
MariaDB [organization]> SELECT COUNT(*)
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = false;
+----------+
| COUNT(*) |
+----------+
|       19 |
+----------+
```

Retrieve login attempts on specific dates

The specific dates are ‘2022-05-09’ and the day before. I needed to count how many login attempts were registered between those two dates.

SELECT COUNT(*)
FROM log_in_attemtps
WHERE login_date = ‘2022-05-08’ OR login_date = ‘2022-05-09’;

```
MariaDB [organization]> SELECT COUNT(*)
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' or login_date = '2022-05-08';
+----------+
| COUNT(*) |
+----------+
|       75 |
+----------+
```

Retrieve login attempts outside of Mexico

Now, I investigate logins that did not originate in Mexico. Again, I will produce the number of login attempts.
Note that the country field includes entries with “MEX” or “MEXICO”.

SELECT COUNT(*)
FROM log_in_attempts
WHERE NOT country LIKE “MEX%”;

```
MariaDB [organization]> SELECT COUNT(*) FROM log_in_attempts WHERE NOT country L
IKE 'MEX%';
+----------+
| COUNT(*) |
+----------+
|      144 |
+----------+
1 row in set (0.001 sec)
```

Retrieve employees in Marketing

I had to retrieve all the employees in Marketing department in the new table “employees”.

DESCRIBE employees;

```
MariaDB [organization]> DESCRIBE employees;
+-------------+-------------+------+-----+---------+-------+
| Field       | Type        | Null | Key | Default | Extra |
+-------------+-------------+------+-----+---------+-------+
| employee_id | int(11)     | NO   | PRI | NULL    |       |
| device_id   | varchar(16) | YES  |     | NULL    |       |
| username    | varchar(16) | NO   |     | NULL    |       |
| department  | varchar(32) | NO   |     | NULL    |       |
| office      | varchar(32) | NO   |     | NULL    |       |
+-------------+-------------+------+-----+---------+-------+
5 rows in set (0.001 sec)
```

*SELECT **
FROM employees
WHERE department = “Marketing”;

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = "Marketing";
+-------------+-------------+----------+------------+-------------+
| employee_id | device_id   | username | department | office      |
+-------------+-------------+----------+------------+-------------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170    |
|        1001 | b239c825d303 | bmoreno  | Marketing  | Central-276 |
|        1020 | u899v381w363 | arutley  | Marketing  | South-351   |
|        1027 | b806c503d354 | mrah     | Marketing  | West-246    |
|        1030 | e391f189g913 | mabadi   | Marketing  | West-375    |
|        1031 | f419g188h578 | dkot     | Marketing  | West-408    |
|        1036 | k550l533m205 | rjensen  | Marketing  | Central-239 |
|        1051 | z451a308b518 | itraora  | Marketing  | Central-134 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195    |
|        1055 | d831e972f553 | awilliam | Marketing  | Central-256 |
|        1056 | e782f537g683 | ankala   | Marketing  | North-139   |
|        1058 | g264h852i697 | madebowa | Marketing  | South-119   |
|        1059 | h832i322j795 | jnguyen  | Marketing  | South-255   |
|        1064 | NULL         | ejones   | Marketing  | South-477   |
|        1067 | p288q432r721 | lwhite   | Marketing  | North-277   |
|        1073 | v135w241x773 | srobinso | Marketing  | Central-494 |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267    |
|        1079 | b433c245d868 | gmedina  | Marketing  | North-456   |
|        1080 | c568d742e974 | gmoon    | Marketing  | North-156   |
|        1088 | k865l965m233 | rgosh    | Marketing  | East-157    |
|        1102 | y943z930a241 | kselassi | Marketing  | South-378   |
```

Retrieve employees in Finance or Sales

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

```
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   |
|        1009 | NULL         | lrodriqu | Sales      | South-134   |
|        1010 | k242l212m542 | jlansky  | Finance    | South-109   |
|        1011 | l748m120n401 | drosas   | Sales      | South-292   |
|        1015 | p611q262r945 | jsoto    | Finance    | North-271   |
|        1017 | r550s824t230 | jclark   | Finance    | North-188   |
|        1018 | s310t540u653 | abellmas | Finance    | North-403   |
|        1022 | w237x430y567 | arusso   | Finance    | West-465    |
|        1024 | y976z753a267 | iuduike  | Sales      | South-215   |
|        1025 | z381a365b233 | jhill    | Sales      | North-115   |
|        1029 | d336e475f676 | ivelasco | Finance    | East-156    |
|        1035 | j236k3031245 | bisles   | Sales      | South-171   |
|        1039 | n253o917p623 | cjackson | Sales      | East-378    |
|        1041 | p929q222r778 | cgriffin | Sales      | North-208   |
|        1044 | s429t157u159 | tbarnes  | Finance    | West-415    |
```

Retrieve all employees not in IT

I need to provide the number of people who don't work in the Information technology department.

```
SELECT COUNT (*)
FROM employees
WHERE department != “Information Technology”;
```

```
MariaDB [organization]> SELECT COUNT(*) FROM employees WHERE department != "Info
rmation Technology";
+----------+
| COUNT(*) |
+----------+
|      161 |
+----------+
```

Summary

I used different filters to find specific data in two SQL tables about login attempts of employees information.