Apply filters to SQL queries

Project description

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

ran a SQL query to view all failed login attempts made after 18:00.

```
Server version: 10.3.39-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [organization]> clear
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date > '18:00' AND success = FALSE;
+----------+----------+------------+------------+---------+------------------+---------+
| 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 |
|        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 |
|        6 | arutley  | 2022-05-12 | 17:00:59   | MEXICO  | 192.168.3.24     |       0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173  |       0 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.228.221  |       0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.81   |       0 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51   |       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 |
|       22 | rjensen  | 2022-05-11 | 00:59:26   | MEX     | 192.168.213.128  |       0 |
|       27 | aalonso  | 2022-05-10 | 01:55:35   | MEX     | 192.168.103.210  |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57    |       0 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.186   |       0 |
|       31 | acook    | 2022-05-12 | 17:36:45   | CANADA  | 192.168.58.232   |       0 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.239  |       0 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93    |       0 |
|       35 | tshah    | 2022-05-10 | 15:26:08   | MEX     | 192.168.92.147   |       0 |
|       37 | eraab    | 2022-05-10 | 06:03:41   | CANADA  | 192.168.152.148  |       0 |
|       40 | aalonso  | 2022-05-12 | 15:15:46   | MEX     | 192.168.174.186  |       0 |
|       41 | apatel   | 2022-05-10 | 17:39:42   | CANADA  | 192.168.46.207   |       0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157    |       0 |
|       43 | mcouliba | 2022-05-08 | 02:35:34   | CANADA  | 192.168.16.208   |       0 |
|       44 | daquino  | 2022-05-08 | 07:02:35   | CANADA  | 192.168.168.144  |       0 |
|       46 | eraab    | 2022-05-11 | 11:29:27   | CAN     | 192.168.24.12    |       0 |
|       49 | asundara | 2022-05-08 | 14:00:01   | US      | 192.168.173.213  |       0 |
|       50 | jclark   | 2022-05-10 | 10:48:02   | CANADA  | 192.168.174.117  |       0 |
|       52 | cjackson | 2022-05-10 | 22:07:07   | CAN     | 192.168.58.57    |       0 |
|       55 | jlansky  | 2022-05-11 | 05:15:34   | US      | 192.168.6.170    |       0 |
|       58 | ivelasco | 2022-05-09 | 17:20:54   | CAN     | 192.168.57.162   |       0 |
|       59 | rjensen  | 2022-05-12 | 04:52:08   | MEX     | 192.168.54.140   |       0 |
|       63 | tmitchel | 2022-05-11 | 14:13:41   | MEXICO  | 192.168.110.131  |       0 |
|       69 | wjaffrey | 2022-05-11 | 19:55:15   | USA     | 192.168.100.17   |       0 |
|       71 | mcouliba | 2022-05-09 | 06:57:42   | CAN     | 192.168.55.169   |       0 |
|       73 | zbernal  | 2022-05-10 | 17:46:45   | USA     | 192.168.80.46    |       0 |
|       76 | bmoreno  | 2022-05-10 | 10:53:55   | CAN     | 192.168.61.200   |       0 |
|       78 | smartell | 2022-05-10 | 05:55:53   | MEX     | 192.168.41.88    |       0 |
|       79 | abernard | 2022-05-09 | 11:41:15   | MEX     | 192.168.158.170  |       0 |
```

As you can see these are all the failed login attempts because the success = 0 and the data with those failed attempts i.e., login attempt, what country it originated from, and the IP address .

Retrieve login attempts on specific dates

```
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 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71    |       0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173   |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158   |       1 |
|       15 | lyamamot | 2022-05-08 | 17:17:26   | USA     | 192.168.183.51    |       0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.192   |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.137    |       1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.105   |       1 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57     |       0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.48    |       1 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.239   |       0 |
|       36 | asundara | 2022-05-08 | 09:00:42   | US      | 192.168.78.151    |       1 |
|       38 | sbaelish | 2022-05-09 | 14:40:01   | USA     | 192.168.60.42     |       1 |
|       39 | yappiah  | 2022-05-09 | 07:56:40   | MEXICO  | 192.168.57.115    |       1 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157     |       0 |
|       43 | mcouliba | 2022-05-08 | 02:35:34   | CANADA  | 192.168.16.208    |       0 |
|       44 | daquino  | 2022-05-08 | 07:02:35   | CANADA  | 192.168.168.144   |       0 |
|       47 | dkot     | 2022-05-08 | 05:06:45   | US      | 192.168.233.24    |       1 |
```

To investigate a suspicious event on 2022-05-09, the SQL query selects all columns from the login_attempts table where the login date is either 2022-05-09 or 2022-05-08 using the WHERE clause with OR operators.

Retrieve login attempts outside of Mexico

The SQL query selects all columns from the login_attempts table where the country column does not contain 'MEX' or 'MEXICO', utilizing the LIKE keyword with % as a wildcard to capture variations in country representations and thereby retrieving login attempts outside of Mexico.

```
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 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243  |       1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173  |       0 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.228.221  |       0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.81   |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158  |       1 |
|       13 | mrah     | 2022-05-11 | 09:29:34   | USA     | 192.168.246.135  |       1 |
|       14 | sbaelish | 2022-05-10 | 10:20:18   | US      | 192.168.16.99    |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51   |       0 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.189  |       1 |
|       17 | pwashing | 2022-05-11 | 02:33:02   | USA     | 192.168.81.89    |       1 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142   |       0 |
|       19 | jhill    | 2022-05-12 | 13:09:04   | US      | 192.168.142.245  |       1 |
|       21 | iuduike  | 2022-05-11 | 17:50:00   | US      | 192.168.131.147  |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.137   |       1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.105  |       1 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.186   |       0 |
|       31 | acook    | 2022-05-12 | 17:36:45   | CANADA  | 192.168.58.232   |       0 |
```

Retrieve employees in Marketing

The query retrieves information on employees in the Marketing department within the East building by selecting rows where the department contains 'Marketing' and the office starts with 'East'.

```
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 (0.032 sec)
```

Retrieve employees in Finance or Sales

The SQL query selects all columns from the employees table where the department column includes either 'Sales' or 'Finance,' effectively identifying employees in these two departments.

```
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 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243 |       1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |       0 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.228.221 |       0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.81  |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158 |       1 |
|       13 | mrah     | 2022-05-11 | 09:29:34   | USA     | 192.168.246.135 |       1 |
|       14 | sbaelish | 2022-05-10 | 10:20:18   | US      | 192.168.16.99   |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51  |       0 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.189 |       1 |
|       17 | pwashing | 2022-05-11 | 02:33:02   | USA     | 192.168.81.89   |       1 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |       0 |
|       19 | jhill    | 2022-05-12 | 13:09:04   | US      | 192.168.142.245 |       1 |
|       21 | iuduike  | 2022-05-11 | 17:50:00   | US      | 192.168.131.147 |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.137  |       1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.105 |       1 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.186  |       0 |
|       31 | acook    | 2022-05-12 | 17:36:45   | CANADA  | 192.168.58.232  |       0 |
```

Retrieve all employees not in IT

This query achieves the same result as the previous query, utilizing the NOT keyword along with the equality condition to exclude rows where the department is 'Information Technology.'

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE NOT department = '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   |
|        1004 | e218f877g788 | eraab    | Human Resources     | South-127   |
|        1005 | f551g340h864 | gesparza | Human Resources     | South-366   |
|        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   |
|        1015 | p611q262r945 | jsoto    | Finance             | North-271   |
|        1016 | q793r736s288 | sbaelish | Human Resources     | North-229   |
|        1017 | r550s824t230 | jclark   | Finance             | North-188   |
|        1018 | s310t540u653 | abellmas | Finance             | North-403   |
|        1020 | u899v381w363 | arutley  | Marketing           | South-351   |
|        1022 | w237x430y567 | arusso   | Finance             | West-465    |
|        1024 | y976z753a267 | iuduike  | Sales               | South-215   |
|        1025 | z381a365b233 | jhill    | Sales               | North-115   |
```

Summary

I used SQL queries with operators like AND, NOT, LIKE, and % to efficiently filter through thousands of records, extracting relevant information on suspicious login attempts, system security updates, and employee details, saving significant time compared to manual searches.