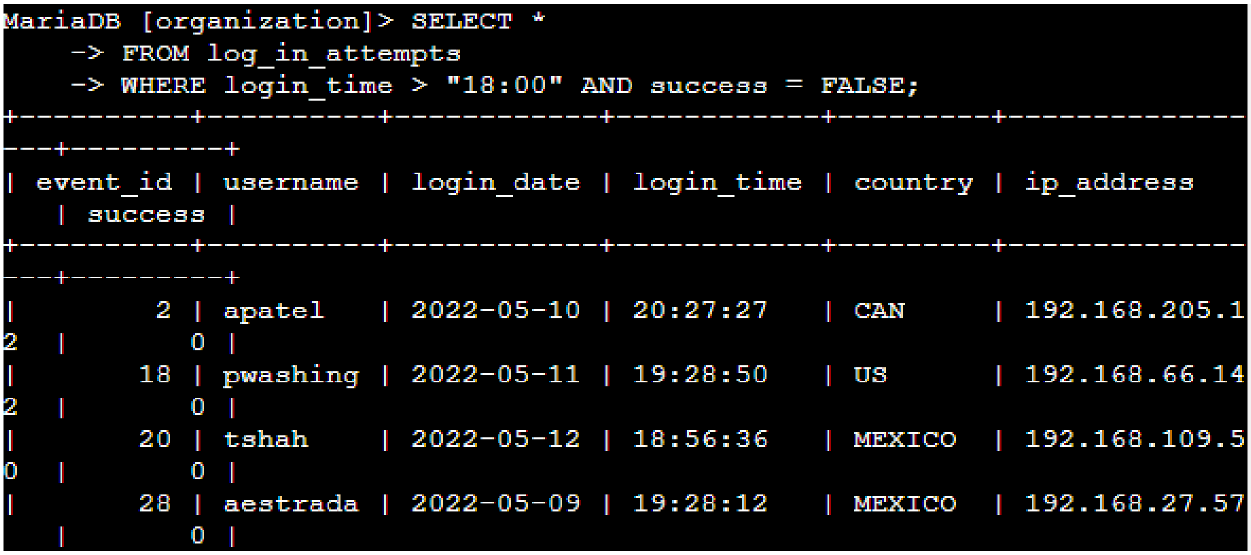
Apply filters to SQL queries

Project description

My team needed to investigate potential security threats. I used SQL to apply filters to obtain specific information about employees, their machines, and the departments they belong to from the database.

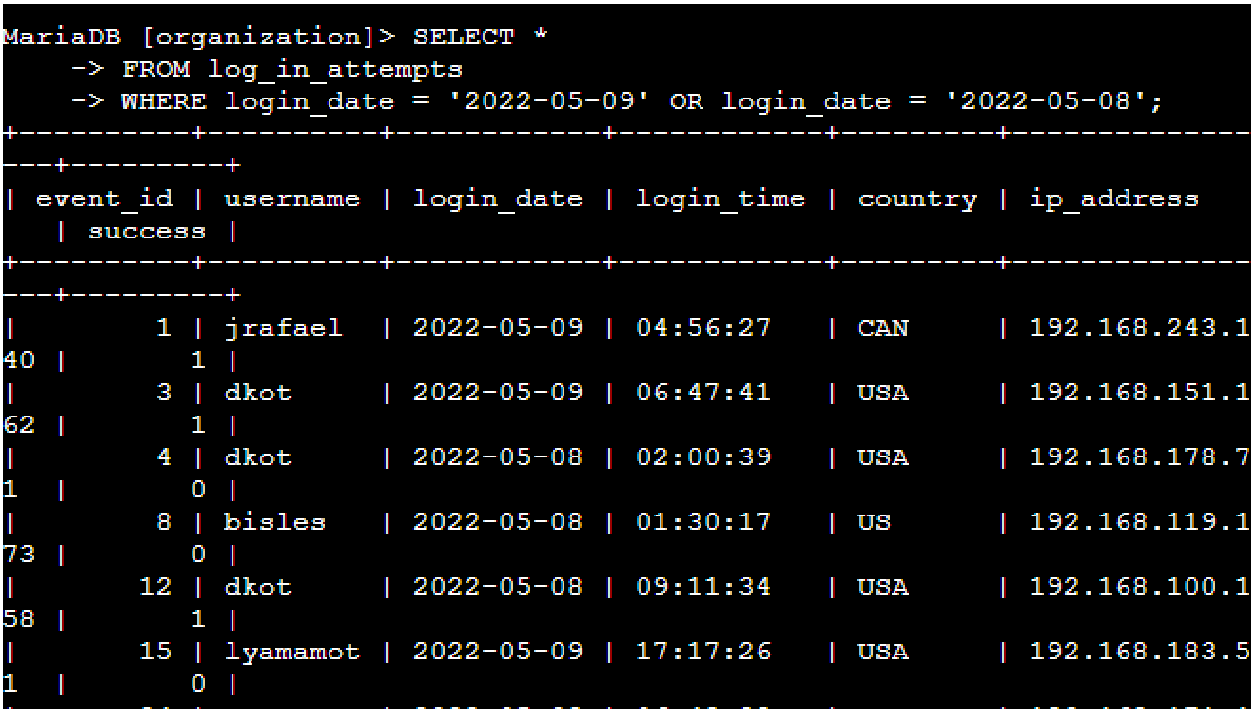
Retrieve after hours failed login attempts



```
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
   | success |
+----------+----------+------------+------------+---------+-------------
---+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.1
2  |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.14
2  |       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.5
0  |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57
   |       0 |
```

My query searches for all failed login attempts made after 18:00.

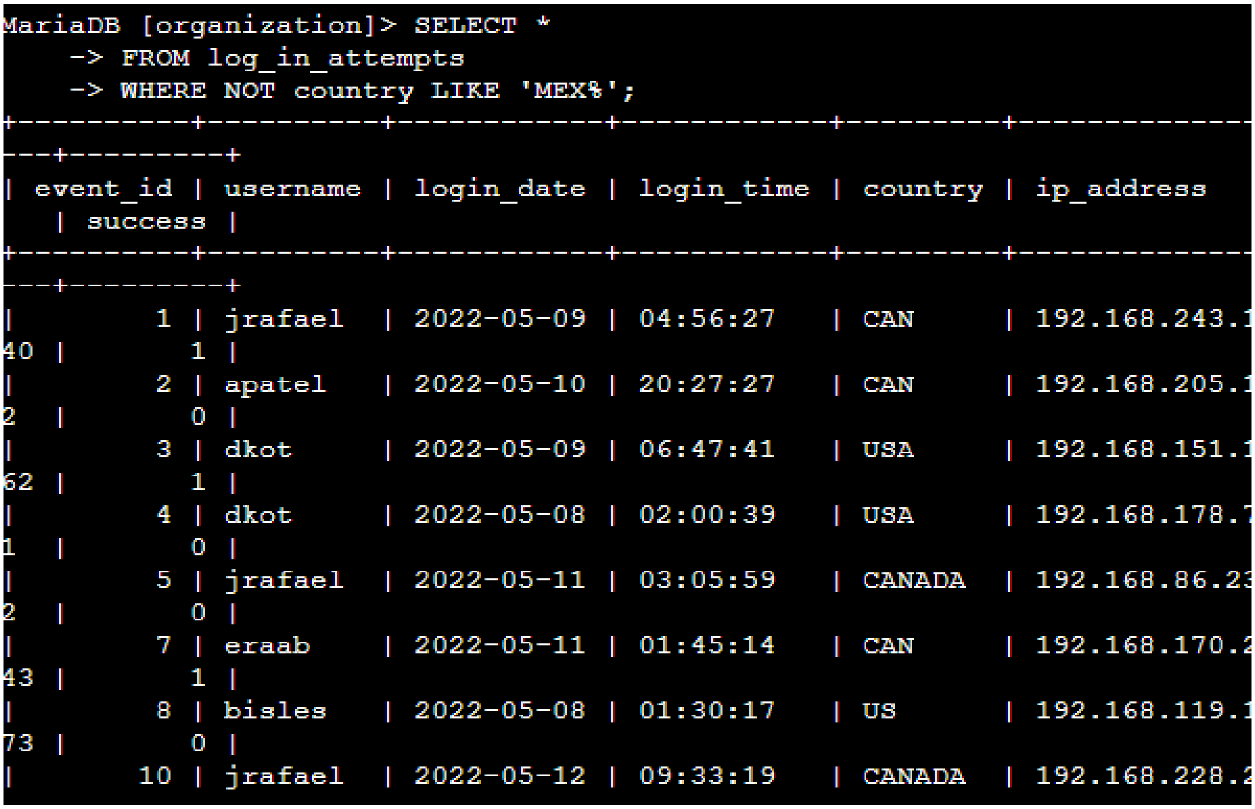
Retrieve login attempts on specific dates



```
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     | 192.168.243.1
40 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.1
62 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.7
1  |       0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.1
73 |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.1
58 |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.5
1  |       0 |
```

My team was investigating a suspicious event that occurred on 2022-05-09 and 2022-05-08, so I applied a filter to search for login attempts made on these two days.

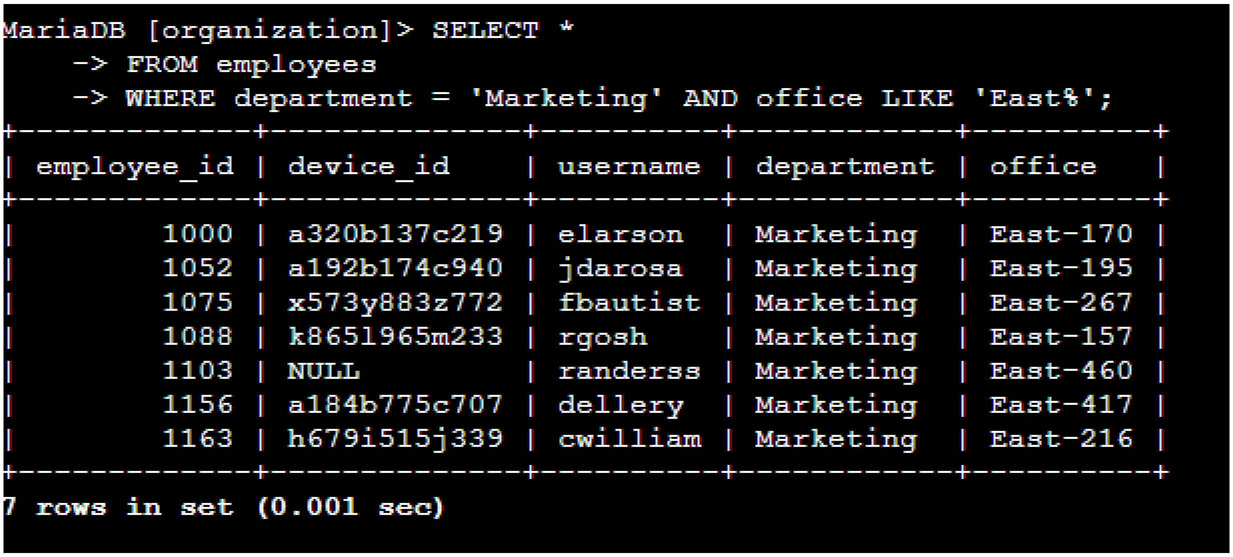
Retrieve login attempts outside of Mexico



```
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     | 192.168.243.1
40 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.1
2  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.1
62 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.7
1  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.23
2  |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.2
43 |       1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.1
73 |       0 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.228.2
```

Here I applied a filter to only retrieve login attempts not made in Mexico, and used ‘MEX%’ to exclude logins that include both “MEX” and anything longer such as “MEXICO.”

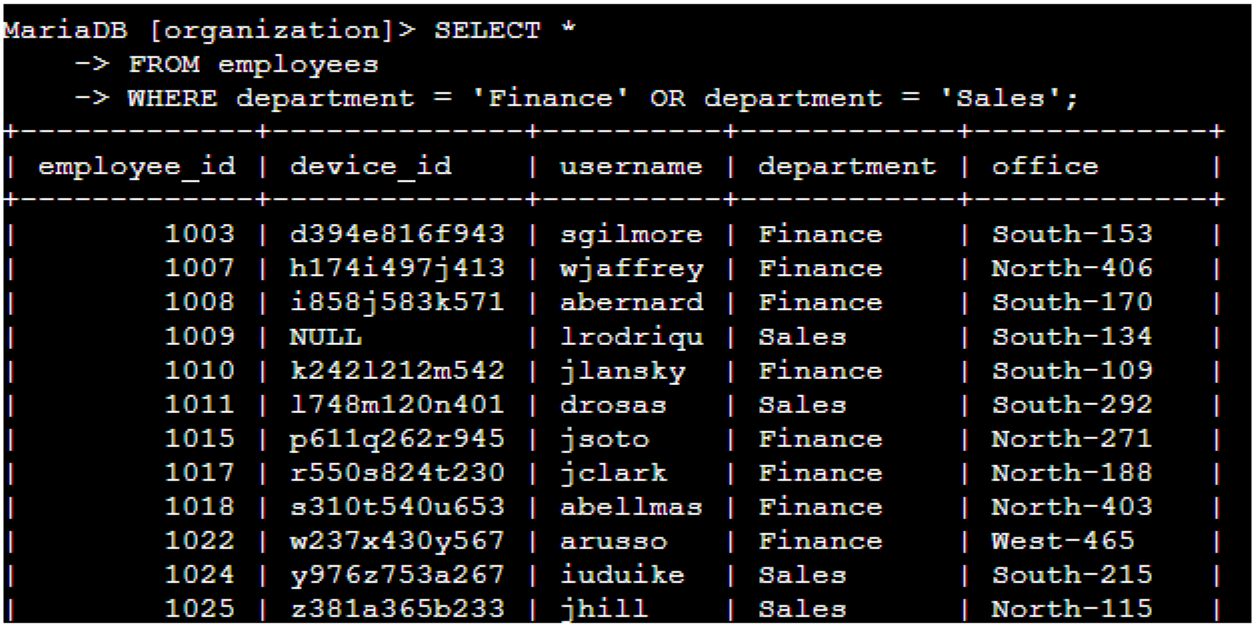
Retrieve employees in Marketing



```
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 (0.001 sec)
```

My team needed to update machines. Here I applied a filter to search for all employees in the Marketing department located in all offices in the East building.

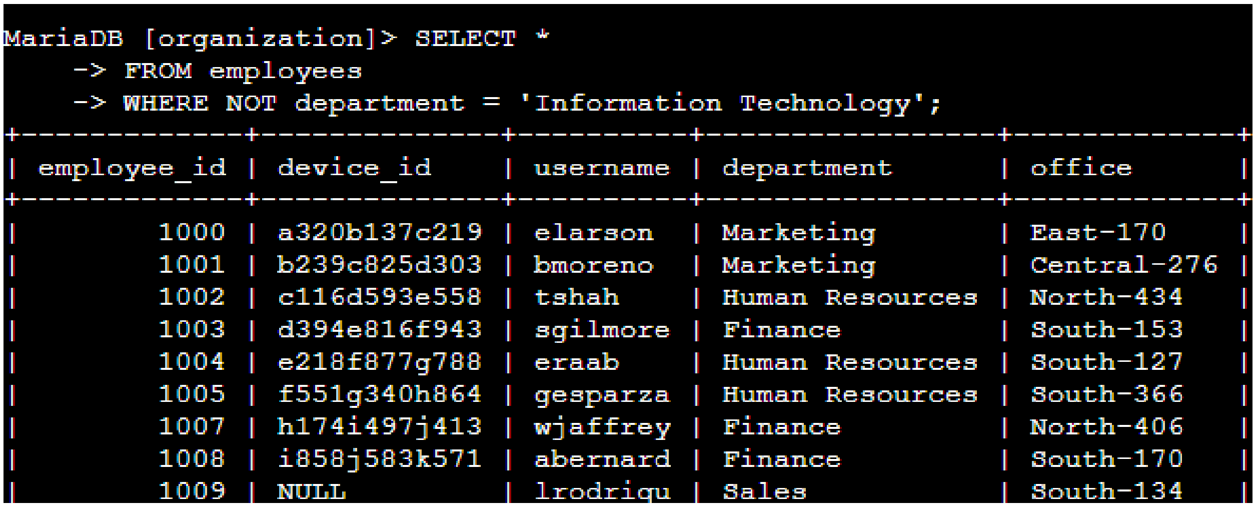
Retrieve employees in Finance or Sales



```
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 | k2421212m542 | jlansky  | Finance    | South-109   |
|        1011 | 1748m120n401 | 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   |
```

My team needed to update the computers belonging to those in the Finance and Sales departments. Here I applied a filter to retrieve all employees in these departments.

Retrieve all employees not in IT



```
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   |
```

My team needed to make one more update to computers belonging to everyone not in the IT department. Here I applied a filter to retrieve information about everyone not in the IT department.

Summary

My team investigated failed login attempts and a suspicious event that occurred on two days. My team also needed to update computers for specific employees, so I applied filters to SQL queries to retrieve the information necessary using AND, LIKE, OR, NOT, and the percentage sign wildcard (%).