Apply filters to SQL queries

Project description

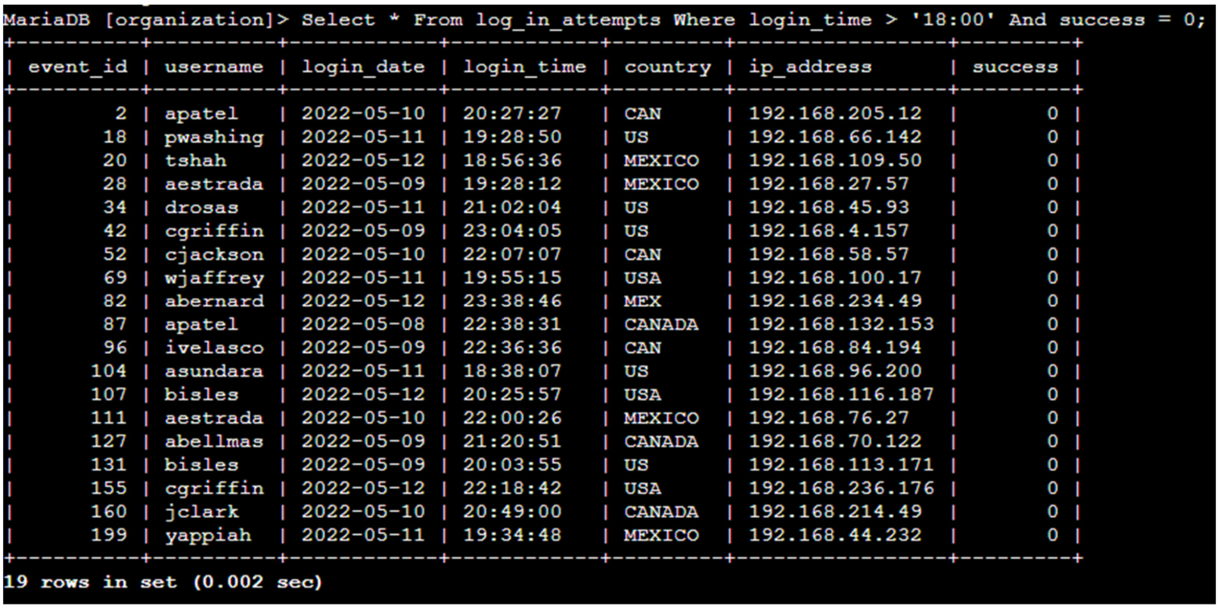
As a security professional at a large organization, part of my job is to investigate security issues to help keep the system secure. I recently discovered some potential security issues that involve login attempts and employee machines.

My task will be to examine the organization’s data in their *employees* and *log_in_attempts* tables. I will need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

Retrieve after hours failed login attempts:

In order to analyze a potential incident occurring after business hours I need to query the log_in_attempts table and investigate failed attempts after business hours. For that, and considering a double condition I need to use the **where** condition with the **AND** operator.

SQL Query -> Select * From log_in_attempts Where login_time >’18:00’ And success = 0;



```
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 (0.002 sec)
```

Retrieve login attempts on specific dates:

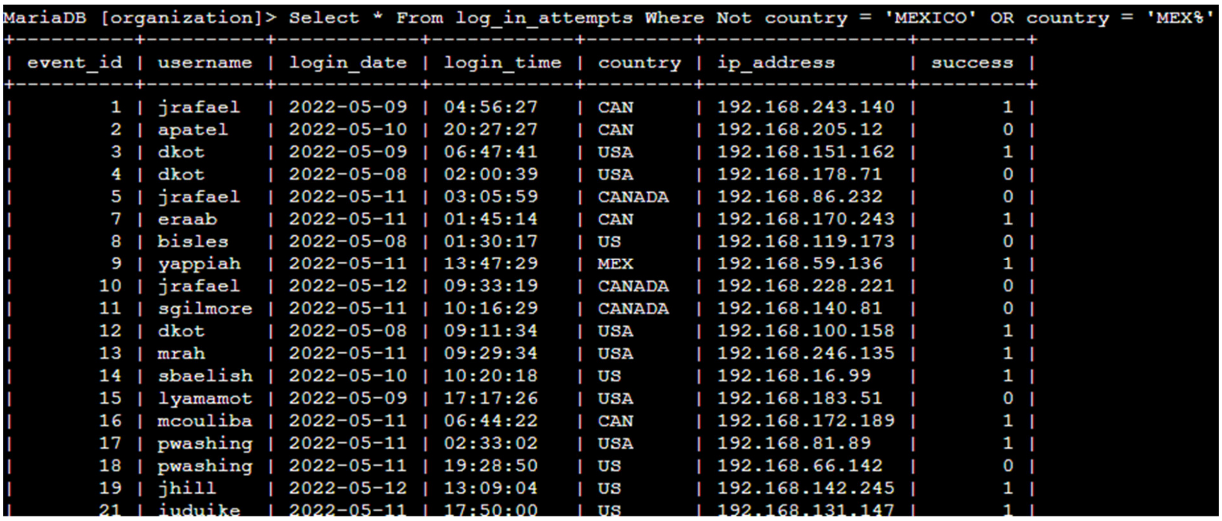
After analyzing the result, I detected a suspicious event on ‘2022-05-09’. To investigate more deeply I need to analyze the events of this day and the day before. For that i will use the **Between** condition to include both days in the search,

SQL Query -> Select * From log_in_attempts Where login_date Between ‘2022-05-08’ And ‘2022-05-09’;

Retrieve login attempts outside of Mexico:

After analysis my team found that the suspicious activity didn't start from Mexico. For that reason we need to filter all the records with sources outside of MEXICO or MEX. I will a use a **OR** operator to guarantee that.

SQL Query -> Select * From log_in_attempts Where NOT country=’MEXICO’ OR country =’MEX%’;

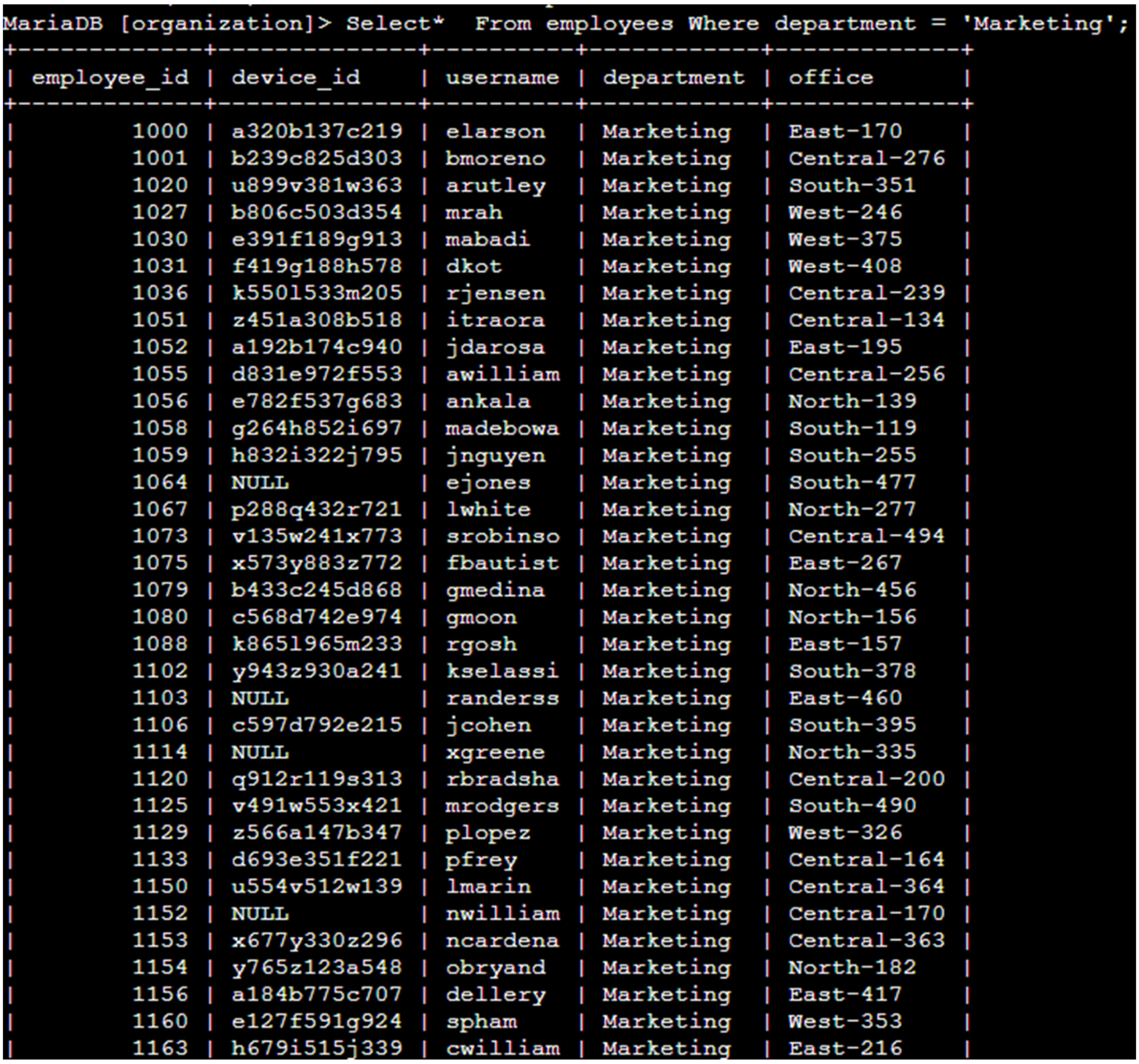


```
MariaDB [organization]> Select * From log_in_attempts Where Not country = 'MEXICO' OR country = 'MEX%'
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        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 |
|        9 | yappiah  | 2022-05-11 | 13:47:29   | MEX     | 192.168.59.136  |       1 |
|       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 |
```

Retrieve employees in Marketing:

Identify all employees in the Marketing department. For that we only need to use the **Where** condition.

SQL Query -> Select * From employees Where department = ‘Marketing’;

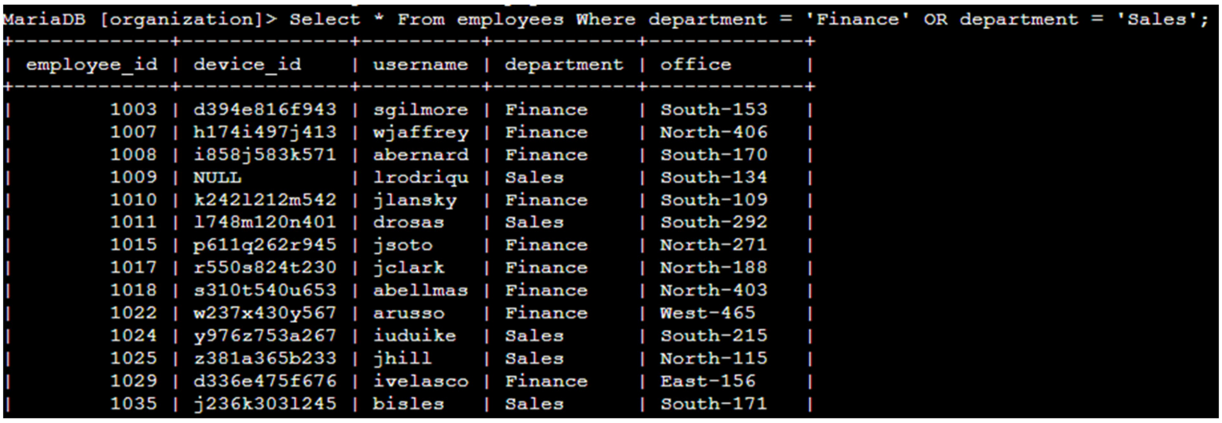


```
MariaDB [organization]> Select*  From employees Where department = 'Marketing';
+-------------+---------------+----------+------------+-------------+
| employee_id | device_id     | username | department | office      |
+-------------+---------------+----------+------------+-------------+
|        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 | k5501533m205  | 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 | k8651965m233  | rgosh    | Marketing  | East-157    |
|        1102 | y943z930a241  | kselassi | Marketing  | South-378   |
|        1103 | NULL          | randerss | Marketing  | East-460    |
|        1106 | c597d792e215  | jcohen   | Marketing  | South-395   |
|        1114 | NULL          | xgreene  | Marketing  | North-335   |
|        1120 | q912r119s313  | rbradsha | Marketing  | Central-200 |
|        1125 | v491w553x421  | mrodgers | Marketing  | South-490   |
|        1129 | z566a147b347  | plopez   | Marketing  | West-326    |
|        1133 | d693e351f221  | pfrey    | Marketing  | Central-164 |
|        1150 | u554v512w139  | lmarin   | Marketing  | Central-364 |
|        1152 | NULL          | nwilliam | Marketing  | Central-170 |
|        1153 | x677y330z296  | ncardena | Marketing  | Central-363 |
|        1154 | y765z123a548  | obryand  | Marketing  | North-182   |
|        1156 | a184b775c707  | dellery  | Marketing  | East-417    |
|        1160 | e127f591g924  | spham    | Marketing  | West-353    |
|        1163 | h679i515j339  | cwilliam | Marketing  | East-216    |
```

Retrieve employees in Finance or Sales:

Identify all employees in the Marketing department. For that we need to use the **Where** condition and the **OR** operator to respect both conditions.

SQL Query -> Select * From employees Where department = ‘Finance’ OR department = ‘Sales’;

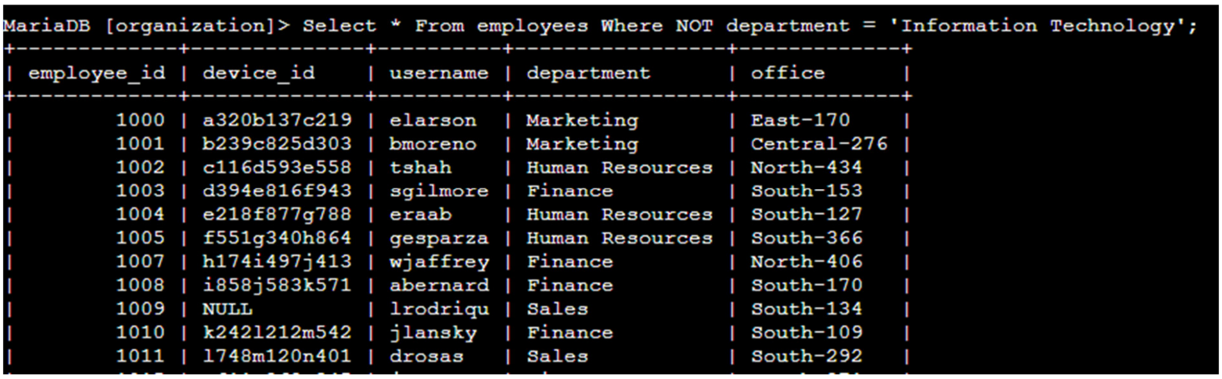


```
MariaDB [organization]> Select * From employees Where department = 'Finance' OR department = 'Sales';
+-------------+--------------+----------+------------+-------------+
| employee_id | device_id    | username | department | office      |
+-------------+--------------+----------+------------+-------------+
|        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 | k2421212m542 | 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   |
```

Retrieve all employees not in IT:

Identify all employees not in the IT department. For that we need to use the **Where** condition and the **NOT** operator to respect both conditions.

SQL Query -> Select * From employees Where NOT department = ‘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   |
```

Summary:

With all these queries we were able to analyze a security incident including when and where it occurs. In addition, we analyze some specific departments and their employees.