Apply filters to SQL queries

Project description

The management at my organization has asked me to investigate potential security issues and update employee's computers as required. As a Linux administrator, I used SQL with filters to perform security-related tasks.

Retrieve after hours of failed login attempts

There were suspicious activities that occurred after business hours (after 18:00). All after hours login attempts that failed need to be investigated.

I created a SQL query on MariaDB to filter for failed login attempts that occurred a er business hours.

```
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     | 192.168.205.12  |       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, 1 warning (0.116 sec)
```

The result is based on the `log_in_attempts` table where the login_time column is after 18:00 and the login attempts are failed (0). The filter "Select * " means to select everything (all columns) and FROM `log_in_attempts` means it is from the `log_in_attempts` table. Success indicates the status of the login. If it is 0, it is a failure whereas if it is 1, it is a success. Therefore, there were 19 failed login attempts after 18:00.

Retrieve login attempts on specific dates

A suspicious event occurred on 2022-05-09. Any login activity that happened on or before 2022-05-09 needs to be investigated. Therefore, I created a SQL query to filter for login attempts that occurred 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 | 2022-05-09 | 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 |
|       49 | asundara | 2022-05-08 | 14:00:01   | US      | 192.168.173.213 |       0 |
|       53 | nmason   | 2022-05-08 | 11:51:38   | CAN     | 192.168.133.188 |       1 |
|       56 | acook    | 2022-05-08 | 04:56:30   | CAN     | 192.168.209.130 |       1 |
|       58 | ivelasco | 2022-05-09 | 17:20:54   | CAN     | 192.168.57.162  |       0 |
|       61 | dtanaka  | 2022-05-09 | 09:45:18   | USA     | 192.168.98.221  |       1 |
|       65 | aalonso  | 2022-05-09 | 23:42:12   | MEX     | 192.168.52.37   |       1 |
|       66 | aestrada | 2022-05-08 | 21:58:32   | MEX     | 192.168.67.223  |       1 |
|       67 | abernard | 2022-05-09 | 11:53:41   | MEX     | 192.168.118.29  |       1 |
|       68 | mrah     | 2022-05-08 | 17:16:13   | US      | 192.168.42.248  |       1 |
|       70 | tmitchel | 2022-05-09 | 10:55:17   | MEXICO  | 192.168.87.199  |       1 |
|       71 | mcouliba | 2022-05-09 | 06:57:42   | CAN     | 192.168.55.169  |       0 |
|       72 | alevitsk | 2022-05-08 | 12:09:10   | CANADA  | 192.168.139.176 |       1 |
|       79 | abernard | 2022-05-09 | 11:41:15   | MEX     | 192.168.158.170 |       0 |
|       80 | cjackson | 2022-05-08 | 02:18:10   | CANADA  | 192.168.33.140  |       1 |
|       83 | lrodriqu | 2022-05-08 | 08:10:23   | USA     | 192.168.67.69   |       1 |
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANADA  | 192.168.132.153 |       0 |
|       90 | gesparza | 2022-05-09 | 00:49:05   | CANADA  | 192.168.87.201  |       0 |
|       92 | pwashing | 2022-05-08 | 00:36:12   | US      | 192.168.247.219 |       0 |
|       96 | ivelasco | 2022-05-09 | 22:36:36   | CAN     | 192.168.84.194  |       0 |
|       97 | jracklev | 2022-05-09 | 02:40:33   | MEXICO  | 192.168.32.231  |       1 |
```

```
|   169 | alevitsk | 2022-05-08 | 08:10:43   | CANADA  | 192.168.210.228 |          0 |
|   170 | sbaelish | 2022-05-09 | 16:43:18   | USA     | 192.168.65.113  |          0 |
|   172 | mabadi   | 2022-05-08 | 08:06:50   | US      | 192.168.180.41  |          1 |
|   178 | sgilmore | 2022-05-08 | 12:27:22   | CAN     | 192.168.52.216  |          0 |
|   184 | alevitsk | 2022-05-08 | 03:09:48   | CAN     | 192.168.33.70   |          0 |
|   186 | bisles   | 2022-05-09 | 04:29:17   | USA     | 192.168.40.72   |          0 |
|   187 | arusso   | 2022-05-09 | 00:36:26   | MEX     | 192.168.77.137  |          0 |
|   189 | nmason   | 2022-05-08 | 05:37:24   | CANADA  | 192.168.168.117 |          1 |
|   190 | jsoto    | 2022-05-09 | 05:09:21   | USA     | 192.168.25.60   |          0 |
|   191 | cjackson | 2022-05-08 | 06:46:07   | CANADA  | 192.168.7.187   |          0 |
|   193 | lrodriqu | 2022-05-08 | 07:11:29   | US      | 192.168.125.240 |          0 |
|   197 | jsoto    | 2022-05-08 | 09:05:09   | US      | 192.168.36.21   |          0 |
+-------+----------+------------+------------+---------+-----------------+------------+
75 rows in set (0.001 sec)
```

I selected the `log_in_attempts` table and used the `WHERE` clause and `OR` operator to filter my results to output only login attempts that occurred on 2022-05-05 or 2022-05-08. As a result, there were 75 login attempts in these two days.

Retrieve login attempts outside of Mexico

After investigating the data and following the pattern, there is a strong indication that login attempts outside of Mexico should be investigated.

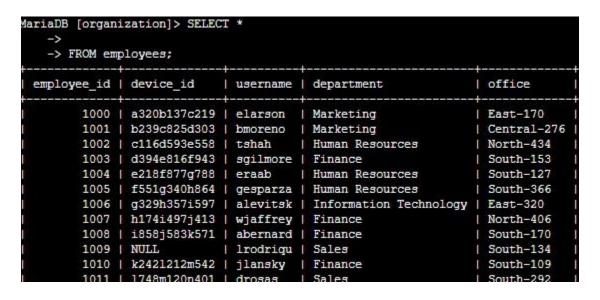I created a SQL query to filter for login attempts that occurred outside of Mexico.

```
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 |
```

```
|    183 | nmason   | 2022-05-11 | 05:29:36 | CANADA | 192.168.137.147 |      0 |
|    184 | alevitsk | 2022-05-08 | 03:09:48 | CAN    | 192.168.33.70   |      0 |
|    185 | jsoto    | 2022-05-10 | 13:34:58 | USA    | 192.168.151.91  |      0 |
|    186 | bisles   | 2022-05-09 | 04:29:17 | USA    | 192.168.40.72   |      0 |
|    188 | jsoto    | 2022-05-11 | 00:39:09 | USA    | 192.168.21.88   |      0 |
|    189 | nmason   | 2022-05-08 | 05:37:24 | CANADA | 192.168.168.117 |      1 |
|    190 | jsoto    | 2022-05-09 | 05:09:21 | USA    | 192.168.25.60   |      0 |
|    191 | cjackson | 2022-05-08 | 06:46:07 | CANADA | 192.168.7.187   |      0 |
|    192 | bisles   | 2022-05-10 | 08:32:03 | USA    | 192.168.201.40  |      1 |
|    193 | lrodriqu | 2022-05-08 | 07:11:29 | US     | 192.168.125.240 |      0 |
|    194 | jclark   | 2022-05-12 | 14:11:04 | CAN    | 192.168.197.247 |      0 |
|    195 | alevitsk | 2022-05-11 | 06:59:13 | CANADA | 192.168.236.78  |      1 |
|    196 | acook    | 2022-05-10 | 09:56:48 | CAN    | 192.168.52.90   |      0 |
|    197 | jsoto    | 2022-05-08 | 09:05:09 | US     | 192.168.36.21   |      0 |
|    200 | jclark   | 2022-05-12 | 01:11:45 | CANADA | 192.168.91.103  |      1 |
+--------+----------+------------+----------+--------+-----------------+--------+
144 rows in set (0.001 sec)
```

I used the `WHERE` clause and `NOT` operator to filter the outputs and receive the login attempts outside Mexico. However, the word "Mexico" could be "Mex", "MEX", and etc. To simplify this, I chose LIKE clause with MEX% as the pattern to match as MEX and MEXICO. The % sign indicates any unspecified characters when used with `LIKE` clause. As a result, there were 144 login attempts outside Mexico.

Retrieve employees in Marketing

My team wants to update certain computers across departments. I created a SQL query to filter for employee machines from employees in the Marketing department in the East building.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM employees;
+-------------+-------------+----------+------------------------+--------------+
| 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    |
|        1006 | g329h357i597 | alevitsk | Information Technology  | East-320     |
|        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    |
```

I first selected all the data in the `employee` table and used the `WHERE` clause to filter employees who are part of the marketing team and reside in the East building using `AND office LIKE 'East%';` As a result, there are 7 employees who match the criteria.

Retrieve employees in Finance or Sales

Across departments, plenty of employee data needs to be updated. I created a SQL query to filter for employee machines from employees in the Finance or Sales departments.

Sanil Gajbhiye - Cybersecurity Portfolio

```
|      1147 | r454s225t299 | tvega    | Finance | West-177    |
|      1148 | s328t505u907 | dharvey  | Finance | South-181   |
|      1159 | d881e710f732 | jshen    | Finance | East-193    |
|      1164 | i682j513k442 | fsmeltz  | Finance | North-163   |
|      1169 | NULL         | mmitchel | Sales   | Central-250 |
|      1174 | s371t911u987 | eortiz   | Finance | North-428   |
|      1175 | t959u687v394 | jclark2  | Finance | North-194   |
|      1176 | u849v569w521 | nliu     | Sales   | West-220    |
|      1181 | z803a233b718 | sessa    | Finance | South-207   |
|      1185 | d790e839f461 | revens   | Sales   | North-330   |
|      1186 | e281f433g404 | sacosta  | Sales   | North-460   |
|      1187 | f963g637h851 | bbode    | Finance | East-351    |
|      1188 | g164h566i795 | noshiro  | Finance | West-252    |
|      1195 | n516o853p957 | orainier | Finance | East-346    |
+-----------+--------------+----------+---------+-------------+
71 rows in set (0.001 sec)
```

I selected the Finance department and Sales department. By using the `WHERE` clause and `OR` operator
I filtered the outputs to make sure all employees who are members of both departments are listed. As a
result, there are 71 people who happen to be members of both departments.

Retrieve all employees not in IT

I created a SQL query to filter for employee machines from employees not in the Information Technology
department.

```
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   |
```

Sanil Gajbhiye - Cybersecurity Portfolio

```
 1180 | y131221la578 | medwards | Human Resources | Central-340 |
 1181 | z803a233b718 | sessa    | Finance         | South-207   |
 1183 | b566c710d544 | lquraish | Human Resources | East-400    |
 1184 | c986d200e170 | ptsosie  | Human Resources | Central-247 |
 1185 | d790e839f461 | revens   | Sales           | North-330   |
 1186 | e281f433g404 | sacosta  | Sales           | North-460   |
 1187 | f963g637h851 | bbode    | Finance         | East-351    |
 1188 | g164h566i795 | noshiro  | Finance         | West-252    |
 1189 | h784i120j837 | slefkowi | Human Resources | West-342    |
 1190 | NULL         | kcarter  | Marketing       | Central-270 |
 1191 | NULL         | shakimi  | Marketing       | Central-366 |
 1194 | m340n287o441 | zwarren  | Human Resources | West-212    |
 1195 | n516o853p957 | orainier | Finance         | East-346    |
 1198 | q308r573s459 | jmartine | Marketing       | South-117   |
 1199 | r520s571t459 | areyes   | Human Resources | East-100    |
+------+--------------+----------+-----------------+-------------+
161 rows in set (0.001 sec)
```

First, I started by selecting all data from the `employee` table. Then, I used a `WHERE` clause with `NOT` to filter for employees not in the IT department.

Summary

I applied filters to SQL queries to get specific information on `employee` and `log_in_attempts` tables. I used the `AND, OR, NOT` operators to filter for the specific information and I used `LIKE` clause and the (`%`) sign filter for patterns.