Apply filters to SQL queries

Project description

An organization, MariaDB, wants to investigate potential security issues and find which computers need updates. Using SQL I can search and filter for the information we need.

Retrieve after hours failed login attempts

Using the following query we are able to see that there are 19 failed attempts to login after business hours.

```
clear
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 41
Server version: 10.3.39-MariaDB-0+deb10u2 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_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 (0.219 sec)

MariaDB [organization]>
```

Retrieve login attempts on specific dates

There was a security event on May 9th, 2022. The organization requested all logins from the date and the day before.

```
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      | 2022-05-09 | 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    | 2022-05-09 | 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  | 2022-05-08 | 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  | 2022-05-09 | 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      | 2022-05-09 | 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  | 2022-05-08 | 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 | jreckley  | 2022-05-09 | 02:49:23   | MEXICO  | 192.168.32.231  |       1 |
|      101 | sbaelish  | 2022-05-08 | 12:01:22   | US      | 192.168.145.158 |       0 |
|      102 | jreckley  | 2022-05-09 | 16:51:44   | MEX     | 192.168.108.13  |       1 |
|      108 | daquino   | 2022-05-09 | 21:30:48   | CANADA  | 192.168.15.110  |       1 |
|      110 | mabadi    | 2022-05-09 | 00:01:54   | USA     | 192.168.90.124  |       1 |
|      112 | rjensen   | 2022-05-09 | 09:22:05   | MEX     | 192.168.69.116  |       1 |
```

```
|      110 | mabadi    | 2022-05-09 | 00:01:54   | USA     | 192.168.90.124  |       1 |
|      112 | rjensen   | 2022-05-09 | 09:22:05   | MEX     | 192.168.69.116  |       1 |
|      117 | bsand     | 2022-05-08 | 00:19:11   | USA     | 192.168.197.187 |       0 |
|      120 | tmitchel  | 2022-05-09 | 02:58:17   | MEXICO  | 192.168.134.62  |       0 |
|      127 | abellmas  | 2022-05-09 | 21:20:51   | CANADA  | 192.168.70.122  |       0 |
|      128 | jclark    | 2022-05-09 | 10:45:59   | CANADA  | 192.168.122.169 |       0 |
|      131 | bisles    | 2022-05-09 | 20:03:55   | US      | 192.168.113.171 |       0 |
|      134 | iuduike   | 2022-05-09 | 06:46:40   | USA     | 192.168.22.115  |       1 |
|      135 | bsand     | 2022-05-09 | 14:06:33   | US      | 192.168.91.238  |       0 |
|      144 | daquino   | 2022-05-09 | 11:09:32   | CANADA  | 192.168.139.9   |       0 |
|      145 | ivelasco  | 2022-05-08 | 09:06:02   | CANADA  | 192.168.39.196  |       1 |
|      147 | yappiah   | 2022-05-08 | 06:04:34   | MEX     | 192.168.65.245  |       0 |
|      148 | daquino   | 2022-05-08 | 06:15:55   | CANADA  | 192.168.135.6   |       1 |
|      150 | nmason    | 2022-05-08 | 14:40:02   | CAN     | 192.168.204.124 |       0 |
|      151 | mabadi    | 2022-05-08 | 16:29:46   | USA     | 192.168.30.225  |       1 |
|      158 | smartell  | 2022-05-09 | 19:30:32   | MEXICO  | 192.168.190.178 |       1 |
|      161 | abellmas  | 2022-05-09 | 13:25:50   | CAN     | 192.168.180.205 |       0 |
|      162 | yappiah   | 2022-05-09 | 04:51:22   | MEXICO  | 192.168.162.100 |       0 |
|      163 | tmitchel  | 2022-05-08 | 09:21:16   | MEX     | 192.168.119.29  |       0 |
|      165 | jreckley  | 2022-05-08 | 15:28:43   | MEXICO  | 192.168.34.193  |       0 |
|      168 | jlansky   | 2022-05-08 | 13:25:42   | USA     | 192.168.210.94  |       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    | 2022-05-09 | 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)

MariaDB [organization]>
```

Using WHERE and OR commands, we can see there were 75 logins total on these days.

Retrieve login attempts outside of Mexico

The organization requested information about login attempts from outside of their base of operations, Mexico. Using WHERE NOT and the wildcard sign % we can see there were 144 attempts made from 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 |
|      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 (0.000 sec)
```

Retrieve Computer Update Information for Marketing

The organization requested to know which computers in the Marketing department in the East wing need updates. Using the following query we are able to find this information.

```
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 (0.019 sec)

MariaDB [organization]>
```

Retrieve Computer Update Information for Finance or Sales

The computers in the Finance and Sales department need updates as well, using the following query we are able to see which computers from both departments need to be updated.

```
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  |
```

Retrieve all employees not in IT

The organization also requested a list of the employees not in the IT department. Using the following query we are able to filter out those employees and have a list of everyone else.

```
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   |
```

Summary

I applied filters to SQL queries to obtain specific login attempts and employee computer information using LIKE AND OR and NOT while also using % for wildcards to find patterns.