Apply More Filters in SQL

Skills Acquired:

- The WHERE keyword
- The BETWEEN and AND operators
- Operators for working with numeric or date and time data types (for example, =, >, >=)

Scenario:

In this scenario, you're investigating a recent security incident.

You need to gather information about login attempts for certain dates and times. This will help in resolving a security incident.

Task 1. Retrieve login attempts after a certain date

In this task, you need to investigate a recent security incident. To do this, you need to gather information about login attempts made after a certain date.

1. Complete the SQL query to retrieve data for login attempts made after '2022-05-09'. Replace X with the correct operator:

```
SELECT *

FROM log_in_attempts

WHERE login_date X '2022-05-09';
```

- **How many login attempts were made after 2022-05-09?**

  125

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date > '2022-05-09';
```

```
+----------+------------+-----------+--------------+---------+---------------------+
| event_id | username   | login_day | login_month  | success | login_date          |
+----------+------------+-----------+--------------+---------+---------------------+
|        2 | apatel     | Wednesday | May          |       0 | 2022-05-10 20:27:27 |
|        3 | dkot       | Thursday  | May          |       0 | 2022-05-12 22:08:05 |
|        4 | dkot       | Friday    | May          |       0 | 2022-05-13 02:40:01 |
|        5 | jrafael    | Friday    | May          |       0 | 2022-05-13 03:16:00 |
|        6 | eraab      | Friday    | May          |       1 | 2022-05-13 04:22:22 |
|        7 | bisles     | Friday    | May          |       0 | 2022-05-13 12:08:07 |
|        8 | apatel     | Friday    | May          |       0 | 2022-05-13 20:11:24 |
|        9 | apatel     | Saturday  | May          |       0 | 2022-05-14 20:44:46 |
|       10 | dkot       | Sunday    | May          |       0 | 2022-05-15 00:04:41 |
|       11 | jrafael    | Sunday    | May          |       0 | 2022-05-15 00:07:02 |
|       12 | eraab      | Sunday    | May          |       1 | 2022-05-15 00:17:02 |
|       13 | bisles     | Sunday    | May          |       0 | 2022-05-15 00:22:22 |
|       14 | apatel     | Sunday    | May          |       0 | 2022-05-15 00:24:05 |
|       15 | dkot       | Monday    | May          |       0 | 2022-05-16 00:04:41 |
|       16 | jrafael    | Monday    | May          |       0 | 2022-05-16 00:07:02 |
|       17 | eraab      | Monday    | May          |       1 | 2022-05-16 00:17:02 |
|       18 | bisles     | Monday    | May          |       0 | 2022-05-16 00:22:22 |
|       19 | apatel     | Monday    | May          |       0 | 2022-05-16 00:24:05 |
|       20 | dkot       | Tuesday   | May          |       0 | 2022-05-17 00:04:41 |
|       21 | jrafael    | Tuesday   | May          |       0 | 2022-05-17 00:07:02 |
|       22 | eraab      | Tuesday   | May          |       1 | 2022-05-17 00:17:02 |
|       23 | bisles     | Tuesday   | May          |       0 | 2022-05-17 00:22:22 |
|       24 | apatel     | Tuesday   | May          |       0 | 2022-05-17 00:24:05 |
|       25 | dkot       | Wednesday | May          |       0 | 2022-05-18 00:04:41 |
|       26 | jrafael    | Wednesday | May          |       0 | 2022-05-18 00:07:02 |
|       27 | eraab      | Wednesday | May          |       1 | 2022-05-18 00:17:02 |
|       28 | bisles     | Wednesday | May          |       0 | 2022-05-18 00:22:22 |
|       29 | apatel     | Wednesday | May          |       0 | 2022-05-18 00:24:05 |
|       30 | dkot       | Thursday  | May          |       0 | 2022-05-19 00:04:41 |
|       31 | jrafael    | Thursday  | May          |       0 | 2022-05-19 00:07:02 |
|       32 | eraab      | Thursday  | May          |       1 | 2022-05-19 00:17:02 |
|       33 | bisles     | Thursday  | May          |       0 | 2022-05-19 00:22:22 |
|       34 | apatel     | Thursday  | May          |       0 | 2022-05-19 00:24:05 |
|       35 | dkot       | Friday    | May          |       0 | 2022-05-20 00:04:41 |
|       36 | jrafael    | Friday    | May          |       0 | 2022-05-20 00:07:02 |
|       37 | eraab      | Friday    | May          |       1 | 2022-05-20 00:17:02 |
|       38 | bisles     | Friday    | May          |       0 | 2022-05-20 00:22:22 |
|       39 | apatel     | Friday    | May          |       0 | 2022-05-20 00:24:05 |
|       40 | dkot       | Saturday  | May          |       0 | 2022-05-21 00:04:41 |
|       41 | jrafael    | Saturday  | May          |       0 | 2022-05-21 00:07:02 |
|       42 | eraab      | Saturday  | May          |       1 | 2022-05-21 00:17:02 |
|       43 | bisles     | Saturday  | May          |       0 | 2022-05-21 00:22:22 |
|       44 | apatel     | Saturday  | May          |       0 | 2022-05-21 00:24:05 |
|       45 | dkot       | Sunday    | May          |       0 | 2022-05-22 00:04:41 |
|       46 | jrafael    | Sunday    | May          |       0 | 2022-05-22 00:07:02 |
|       47 | eraab      | Sunday    | May          |       1 | 2022-05-22 00:17:02 |
|       48 | bisles     | Sunday    | May          |       0 | 2022-05-22 00:22:22 |
|       49 | apatel     | Sunday    | May          |       0 | 2022-05-22 00:24:05 |
|       50 | dkot       | Monday    | May          |       0 | 2022-05-23 00:04:41 |
|       51 | jrafael    | Monday    | May          |       0 | 2022-05-23 00:07:02 |
|       52 | eraab      | Monday    | May          |       1 | 2022-05-23 00:17:02 |
|       53 | bisles     | Monday    | May          |       0 | 2022-05-23 00:22:22 |
|       54 | apatel     | Monday    | May          |       0 | 2022-05-23 00:24:05 |
|       55 | dkot       | Tuesday   | May          |       0 | 2022-05-24 00:04:41 |
|       56 | jrafael    | Tuesday   | May          |       0 | 2022-05-24 00:07:02 |
|       57 | eraab      | Tuesday   | May          |       1 | 2022-05-24 00:17:02 |
|       58 | bisles     | Tuesday   | May          |       0 | 2022-05-24 00:22:22 |
|       59 | apatel     | Tuesday   | May          |       0 | 2022-05-24 00:24:05 |
|       60 | dkot       | Wednesday | May          |       0 | 2022-05-25 00:04:41 |
|       61 | jrafael    | Wednesday | May          |       0 | 2022-05-25 00:07:02 |
|       62 | eraab      | Wednesday | May          |       1 | 2022-05-25 00:17:02 |
|       63 | bisles     | Wednesday | May          |       0 | 2022-05-25 00:22:22 |
|       64 | apatel     | Wednesday | May          |       0 | 2022-05-25 00:24:05 |
|       65 | dkot       | Thursday  | May          |       0 | 2022-05-26 00:04:41 |
|       66 | jrafael    | Thursday  | May          |       0 | 2022-05-26 00:07:02 |
|       67 | eraab      | Thursday  | May          |       1 | 2022-05-26 00:17:02 |
|       68 | bisles     | Thursday  | May          |       0 | 2022-05-26 00:22:22 |
|       69 | apatel     | Thursday  | May          |       0 | 2022-05-26 00:24:05 |
|       70 | dkot       | Friday    | May          |       0 | 2022-05-27 00:04:41 |
|       71 | jrafael    | Friday    | May          |       0 | 2022-05-27 00:07:02 |
|       72 | eraab      | Friday    | May          |       1 | 2022-05-27 00:17:02 |
|       73 | bisles     | Friday    | May          |       0 | 2022-05-27 00:22:22 |
|       74 | apatel     | Friday    | May          |       0 | 2022-05-27 00:24:05 |
|       75 | dkot       | Saturday  | May          |       0 | 2022-05-28 00:04:41 |
|       76 | jrafael    | Saturday  | May          |       0 | 2022-05-28 00:07:02 |
|       77 | eraab      | Saturday  | May          |       1 | 2022-05-28 00:17:02 |
|       78 | bisles     | Saturday  | May          |       0 | 2022-05-28 00:22:22 |
|       79 | apatel     | Saturday  | May          |       0 | 2022-05-28 00:24:05 |
|       80 | dkot       | Sunday    | May          |       0 | 2022-05-29 00:04:41 |
|       81 | jrafael    | Sunday    | May          |       0 | 2022-05-29 00:07:02 |
|       82 | eraab      | Sunday    | May          |       1 | 2022-05-29 00:17:02 |
|       83 | bisles     | Sunday    | May          |       0 | 2022-05-29 00:22:22 |
|       84 | apatel     | Sunday    | May          |       0 | 2022-05-29 00:24:05 |
|       85 | dkot       | Monday    | May          |       0 | 2022-05-30 00:04:41 |
|       86 | jrafael    | Monday    | May          |       0 | 2022-05-30 00:07:02 |
|       87 | eraab      | Monday    | May          |       1 | 2022-05-30 00:17:02 |
|       88 | bisles     | Monday    | May          |       0 | 2022-05-30 00:22:22 |
|       89 | apatel     | Monday    | May          |       0 | 2022-05-30 00:24:05 |
|       90 | dkot       | Tuesday   | May          |       0 | 2022-05-31 00:04:41 |
|       91 | jrafael    | Tuesday   | May          |       0 | 2022-05-31 00:07:02 |
|       92 | eraab      | Tuesday   | May          |       1 | 2022-05-31 00:17:02 |
|       93 | bisles     | Tuesday   | May          |       0 | 2022-05-31 00:22:22 |
|       94 | apatel     | Tuesday   | May          |       0 | 2022-05-31 00:24:05 |
|       95 | dkot       | Wednesday | May          |       0 | 2022-06-01 00:04:41 |
|       96 | jrafael    | Wednesday | May          |       0 | 2022-06-01 00:07:02 |
|       97 | eraab      | Wednesday | May          |       1 | 2022-06-01 00:17:02 |
|       98 | bisles     | Wednesday | May          |       0 | 2022-06-01 00:22:22 |
|       99 | apatel     | Wednesday | May          |       0 | 2022-06-01 00:24:05 |
|      100 | dkot       | Thursday  | May          |       0 | 2022-06-02 00:04:41 |
|      101 | jrafael    | Thursday  | May          |       0 | 2022-06-02 00:07:02 |
|      102 | eraab      | Thursday  | May          |       1 | 2022-06-02 00:17:02 |
|      103 | bisles     | Thursday  | May          |       0 | 2022-06-02 00:22:22 |
|      104 | apatel     | Thursday  | May          |       0 | 2022-06-02 00:24:05 |
|      105 | dkot       | Friday    | May          |       0 | 2022-06-03 00:04:41 |
|      106 | jrafael    | Friday    | May          |       0 | 2022-06-03 00:07:02 |
|      107 | eraab      | Friday    | May          |       1 | 2022-06-03 00:17:02 |
|      108 | bisles     | Friday    | May          |       0 | 2022-06-03 00:22:22 |
|      109 | apatel     | Friday    | May          |       0 | 2022-06-03 00:24:05 |
|      110 | dkot       | Saturday  | May          |       0 | 2022-06-04 00:04:41 |
|      111 | jrafael    | Saturday  | May          |       0 | 2022-06-04 00:07:02 |
|      112 | eraab      | Saturday  | May          |       1 | 2022-06-04 00:17:02 |
|      113 | bisles     | Saturday  | May          |       0 | 2022-06-04 00:22:22 |
|      114 | apatel     | Saturday  | May          |       0 | 2022-06-04 00:24:05 |
|      115 | dkot       | Sunday    | May          |       0 | 2022-06-05 00:04:41 |
|      116 | jrafael    | Sunday    | May          |       0 | 2022-06-05 00:07:02 |
|      117 | eraab      | Sunday    | May          |       1 | 2022-06-05 00:17:02 |
|      118 | bisles     | Sunday    | May          |       0 | 2022-06-05 00:22:22 |
|      119 | apatel     | Sunday    | May          |       0 | 2022-06-05 00:24:05 |
|      120 | dkot       | Monday    | May          |       0 | 2022-06-06 00:04:41 |
|      121 | jrafael    | Monday    | May          |       0 | 2022-06-06 00:07:02 |
|      122 | eraab      | Monday    | May          |       1 | 2022-06-06 00:17:02 |
|      123 | bisles     | Monday    | May          |       0 | 2022-06-06 00:22:22 |
|      124 | apatel     | Monday    | May          |       0 | 2022-06-06 00:24:05 |
|      125 | dkot       | Tuesday   | May          |       0 | 2022-06-07 00:04:41 |
+----------+------------+-----------+--------------+---------+---------------------+
125 rows in set (0.074 sec)
```

Now, based on your first query, you find a need to expand the date range to include 2022-05-09 in your search.

2. Complete the SQL query to retrieve data for login attempts that were made on or after '2022-05-09'. Replace X with the correct operator:

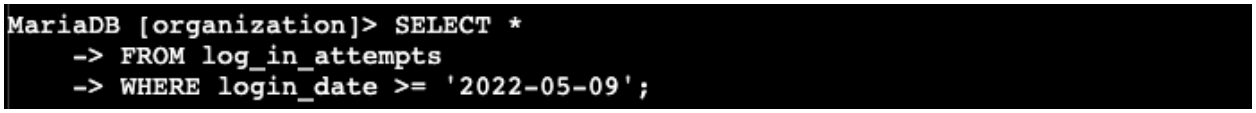
```
SELECT *

FROM log_in_attempts

WHERE login_date X '2022-05-09';
```

- **How many login attempts were made on or after 2022-05-09?**

  165



Task 2. Retrieve logins in a date range

In this task, you need to narrow the focus of the search. Login attempts made after 2022-05-11 shouldn't be included. Use the BETWEEN and AND operators to return results between '2022-05-09' and '2022-05-11'.

- Run the query to retrieve the required records. You must insert the required dates X and Y:

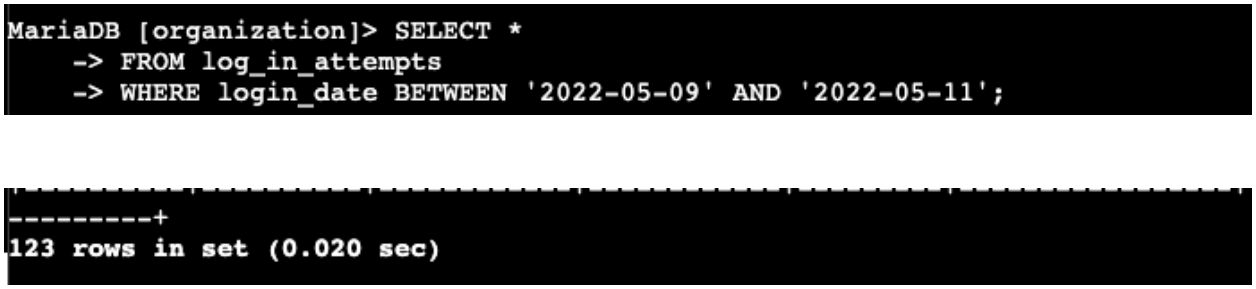
```
SELECT *

FROM log_in_attempts

WHERE login_date BETWEEN 'X' AND 'Y';
```

- **How many login attempts were made between 2022-05-09 and 2022-05-11?**

  123



Task 3. Investigate logins at certain times

In this task, you need to investigate logins that were made at certain times. To do this, filter the data in the log_in_attempts table by login time (login_time).

First, your organization's typical work hours begin at 07:00:00. Retrieve all login attempts made before 07:00:00 to learn more about the users who are logging in outside of typical hours.

1. Write a SQL query to retrieve data for login attempts made before '07:00:00'.

- **What is the username of the fifth record returned from this query?**

  Eraab

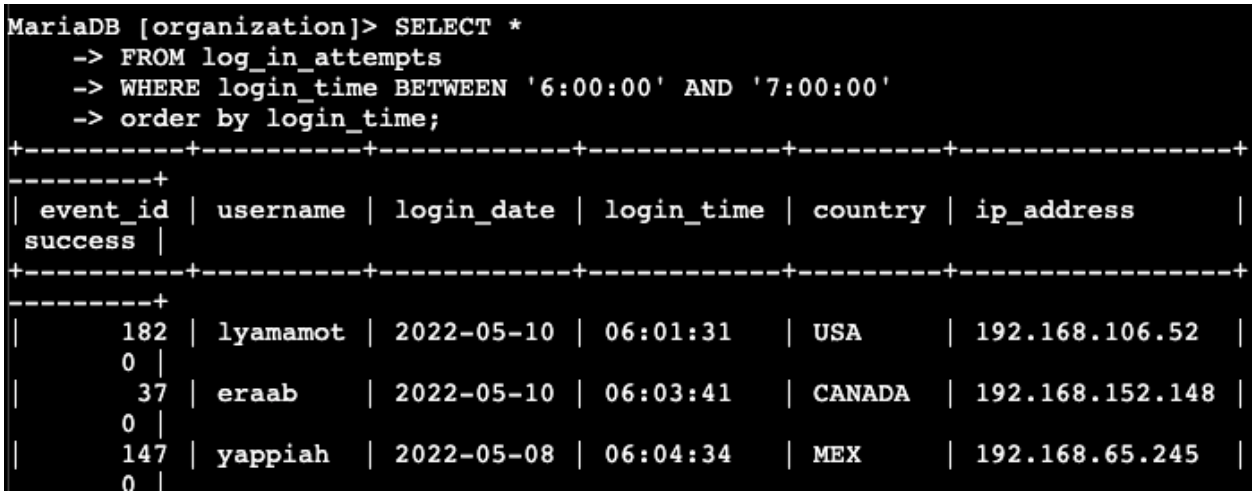
```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time < '7:00:00';
+----------+----------+------------+------------+---------+-----------------+
---------+
| event_id | username | login_date | login_time | country | ip_address      |
 success |
+----------+----------+------------+------------+---------+-----------------+
---------+
|        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 |
|        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 |
```

The query in the previous step returned more results than required.

2. Modify the query to return logins between '06:00:00' and '07:00:00'.

- **What time was the earliest login attempt between 06:00:00 and 07:00:00?**

  06:01:31



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time BETWEEN '6:00:00' AND '7:00:00'
    -> order by login_time;
+----------+----------+------------+------------+---------+----------------+
---------+
| event_id | username | login_date | login_time | country | ip_address      |
 success |
+----------+----------+------------+------------+---------+----------------+
---------+
|      182 | lyamamot | 2022-05-10 | 06:01:31   | USA     | 192.168.106.52  |
       0 |
|       37 | eraab    | 2022-05-10 | 06:03:41   | CANADA  | 192.168.152.148 |
       0 |
|      147 | yappiah  | 2022-05-08 | 06:04:34   | MEX     | 192.168.65.245  |
       0 |
```

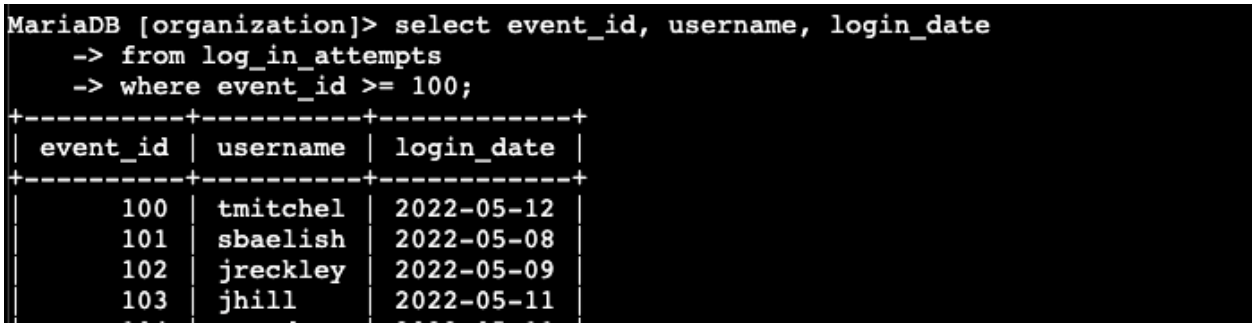
Task 4. Investigate logins by event ID

In this task, you need to investigate login attempts based on event ID numbers. With this query, you want to return only the event_id, username, and login_date fields from the log_in_attempts table.

1. Write a query to return login attempts with event_id greater than or equal to 100.

- **What is the login date of the third result returned by your query?**

  2022-05-09



```
MariaDB [organization]> select event_id, username, login_date
    -> from log_in_attempts
    -> where event_id >= 100;
+----------+----------+------------+
| event_id | username | login_date |
+----------+----------+------------+
|      100 | tmitchel | 2022-05-12 |
|      101 | sbaelish | 2022-05-08 |
|      102 | jreckley | 2022-05-09 |
|      103 | jhill    | 2022-05-11 |
```

The query in the previous step returned more data than required.

2. Modify the query to return only login attempts with event_id between 100 and 150.

- **What is the username of the seventh result returned by your query?**

  Tmitchel

```
MariaDB [organization]> select event_id, username, login_date
    -> from log_in_attempts
    -> where event_id between '100' and '150';
+----------+----------+------------+
| event_id | username | login_date |
+----------+----------+------------+
|      100 | tmitchel | 2022-05-12 |
|      101 | sbaelish | 2022-05-08 |
|      102 | jreckley | 2022-05-09 |
|      103 | jhill    | 2022-05-11 |
|      104 | asundara | 2022-05-11 |
|      105 | cjackson | 2022-05-12 |
|      106 | tmitchel | 2022-05-12 |
|      107 | bisles   | 2022-05-12 |
|      108 | daquino  | 2022-05-09 |
```