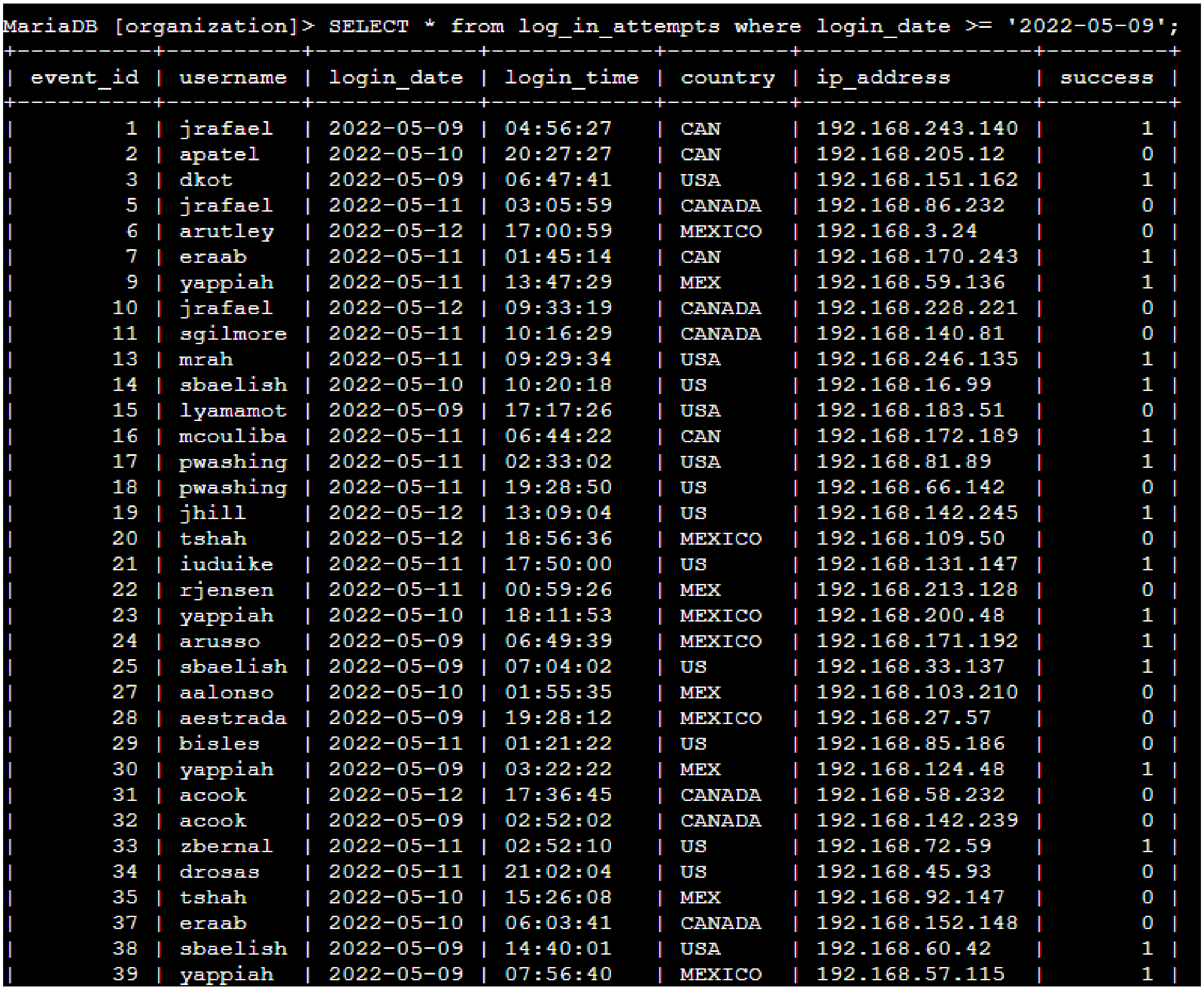
5- Activity Apply more filters in SQL

Task 1: Retrieve Login Attempts After a Certain Date

Objective:
Investigate a recent security incident by gathering information on login attempts made after May 9, 2022.

Query Used:
`SELECT * FROM log_in_attempts WHERE login_date >= '2022-05-09';`

Outcome:
The query returned 165 login attempts that occurred on or after May 9, 2022. The `>=` operator was used to include the specified date and all subsequent dates in the results.



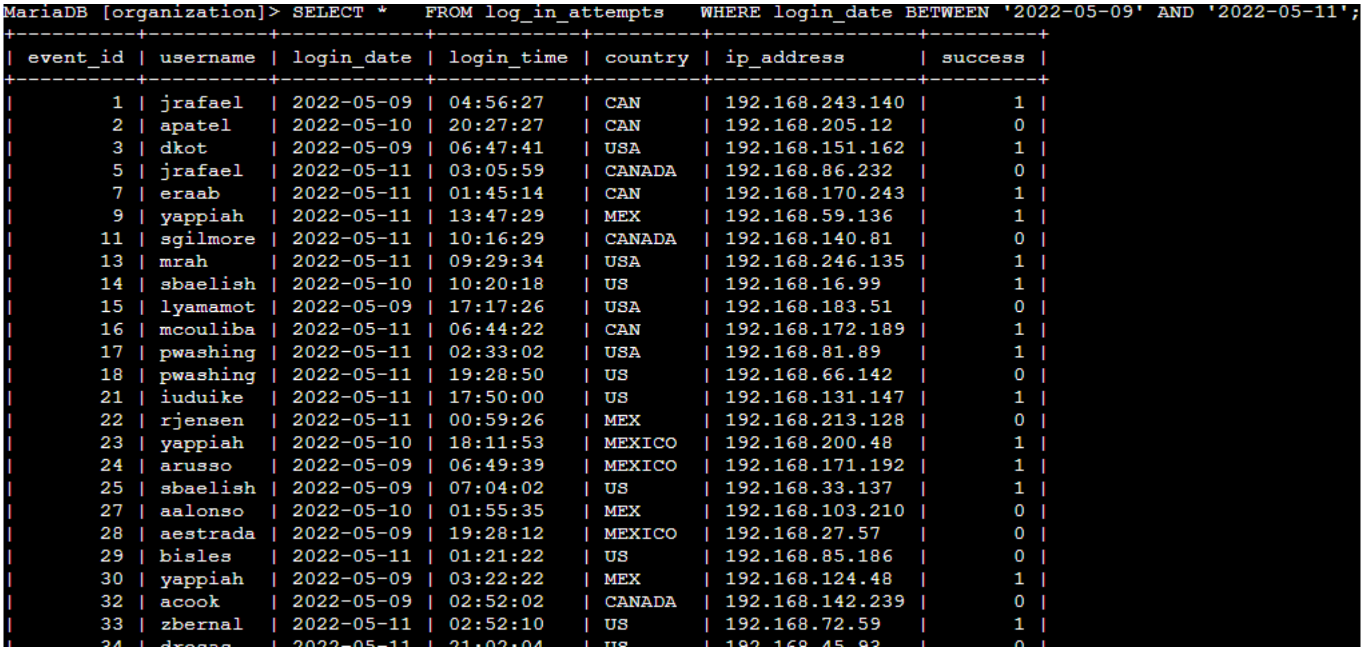
```
MariaDB [organization]> SELECT * from log_in_attempts where login_date >= '2022-05-09';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        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 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |       0 |
|        6 | arutley  | 2022-05-12 | 17:00:59   | MEXICO  | 192.168.3.24    |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243 |       1 |
|        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 |
|       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 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50  |       0 |
|       21 | iuduike  | 2022-05-11 | 17:50:00   | US      | 192.168.131.147 |       1 |
|       22 | rjensen  | 2022-05-11 | 00:59:26   | MEX     | 192.168.213.128 |       0 |
|       23 | yappiah  | 2022-05-10 | 18:11:53   | MEXICO  | 192.168.200.48  |       1 |
|       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 |
|       27 | aalonso  | 2022-05-10 | 01:55:35   | MEX     | 192.168.103.210 |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |       0 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.186  |       0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.48  |       1 |
|       31 | acook    | 2022-05-12 | 17:36:45   | CANADA  | 192.168.58.232  |       0 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.239 |       0 |
|       33 | zbernal  | 2022-05-11 | 02:52:10   | US      | 192.168.72.59   |       1 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93   |       0 |
|       35 | tshah    | 2022-05-10 | 15:26:08   | MEX     | 192.168.92.147  |       0 |
|       37 | eraab    | 2022-05-10 | 06:03:41   | CANADA  | 192.168.152.148 |       0 |
|       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 |
```

Task 2: Retrieve Login Attempts Within a Date Range

Objective:
Narrow down the investigation by focusing on login attempts made within a specific date range, specifically between May 9, 2022, and May 11, 2022.

Query Used:
`SELECT * FROM log_in_attempts WHERE login_date BETWEEN '2022-05-09' AND '2022-05-11';`

Outcome:
The query identified 123 login attempts that occurred within the specified date range. The `BETWEEN` and `AND` operators effectively captured all logins within the two dates.



```
MariaDB [organization]> SELECT *   FROM log_in_attempts   WHERE login_date BETWEEN '2022-05-09' AND '2022-05-11';
+----------+----------+------------+------------+---------+-----------------+---------+
| 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 |
|        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 |
|        9 | yappiah  | 2022-05-11 | 13:47:29   | MEX     | 192.168.59.136  |       1 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.81  |       0 |
|       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 |
|       21 | iuduike  | 2022-05-11 | 17:50:00   | US      | 192.168.131.147 |       1 |
|       22 | rjensen  | 2022-05-11 | 00:59:26   | MEX     | 192.168.213.128 |       0 |
|       23 | yappiah  | 2022-05-10 | 18:11:53   | MEXICO  | 192.168.200.48  |       1 |
|       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 |
|       27 | aalonso  | 2022-05-10 | 01:55:35   | MEX     | 192.168.103.210 |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |       0 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.186  |       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 |
|       33 | zbernal  | 2022-05-11 | 02:52:10   | US      | 192.168.72.59   |       1 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93   |       0 |
```

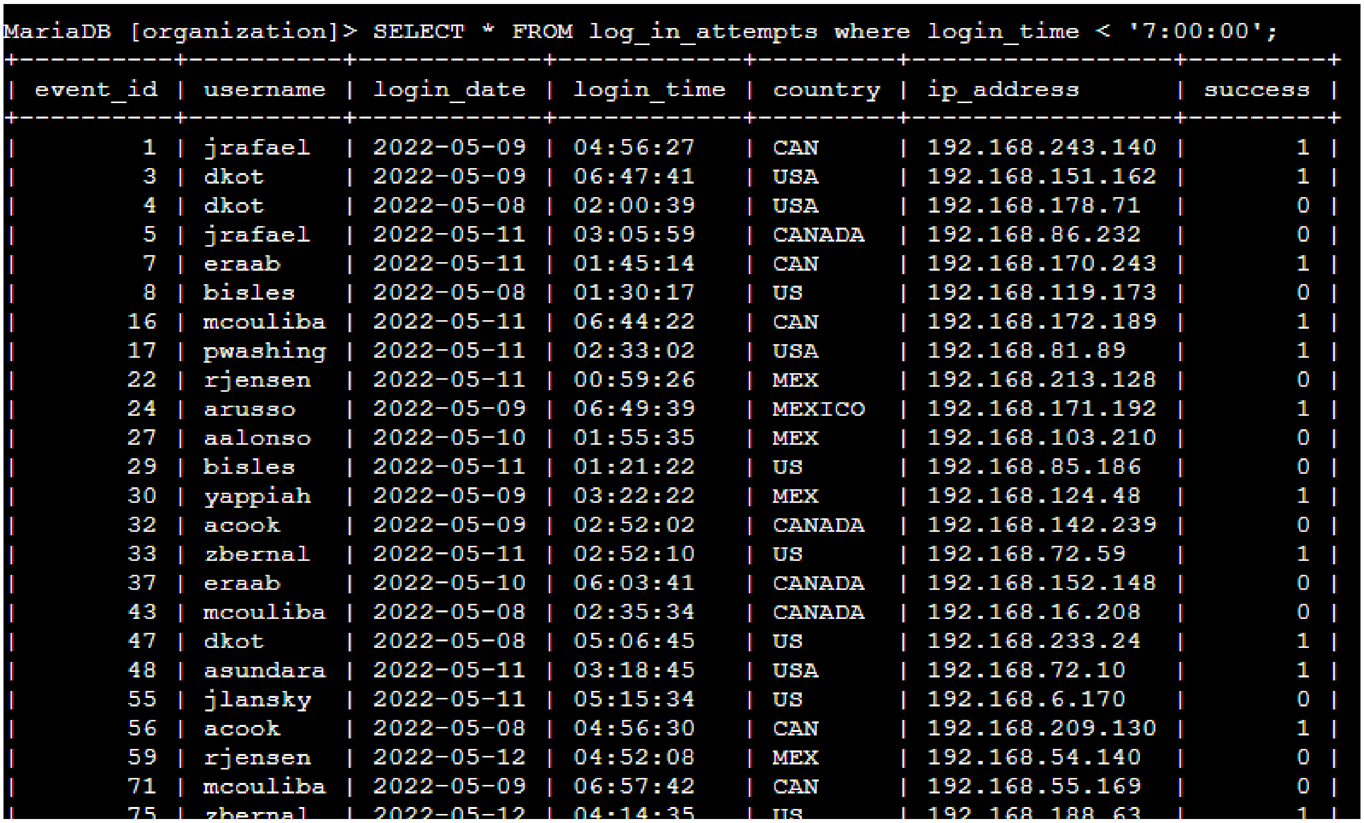
### Task 3: Investigate Login Attempts at Specific Times

Objective:
Examine login attempts that occurred outside of typical work hours, as well as those within a specific hour range, to identify any unusual login patterns.

1- **Login Attempts Before Work Hours:**

Query:
`SELECT * FROM log_in_attempts WHERE login_time < '07:00:00';`

Outcome:
The query retrieved all login attempts made before 07:00:00, with the fifth record belonging to the user `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 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |       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 |
|       22 | rjensen  | 2022-05-11 | 00:59:26   | MEX     | 192.168.213.128 |       0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.192 |       1 |
|       27 | aalonso  | 2022-05-10 | 01:55:35   | MEX     | 192.168.103.210 |       0 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.186  |       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 |
|       33 | zbernal  | 2022-05-11 | 02:52:10   | US      | 192.168.72.59   |       1 |
|       37 | eraab    | 2022-05-10 | 06:03:41   | CANADA  | 192.168.152.148 |       0 |
|       43 | mcouliba | 2022-05-08 | 02:35:34   | CANADA  | 192.168.16.208  |       0 |
|       47 | dkot     | 2022-05-08 | 05:06:45   | US      | 192.168.233.24  |       1 |
|       48 | asundara | 2022-05-11 | 03:18:45   | USA     | 192.168.72.10   |       1 |
|       55 | jlansky  | 2022-05-11 | 05:15:34   | US      | 192.168.6.170   |       0 |
|       56 | acook    | 2022-05-08 | 04:56:30   | CAN     | 192.168.209.130 |       1 |
|       59 | rjensen  | 2022-05-12 | 04:52:08   | MEX     | 192.168.54.140  |       0 |
|       71 | mcouliba | 2022-05-09 | 06:57:42   | CAN     | 192.168.55.169  |       0 |
|       75 | zbernal  | 2022-05-12 | 04:14:35   | US      | 192.168.188.63  |       1 |
```

2- Login Attempts Between 06:00:00 and 07:00:00:

Query:
SELECT * FROM log_in_attempts WHERE login_time BETWEEN '06:00:00' AND '07:00:00' ORDER BY login_time;

Outcome:
The earliest login attempt within this range was at 06:01:31. The `ORDER BY` clause was used to quickly identify the earliest login time.

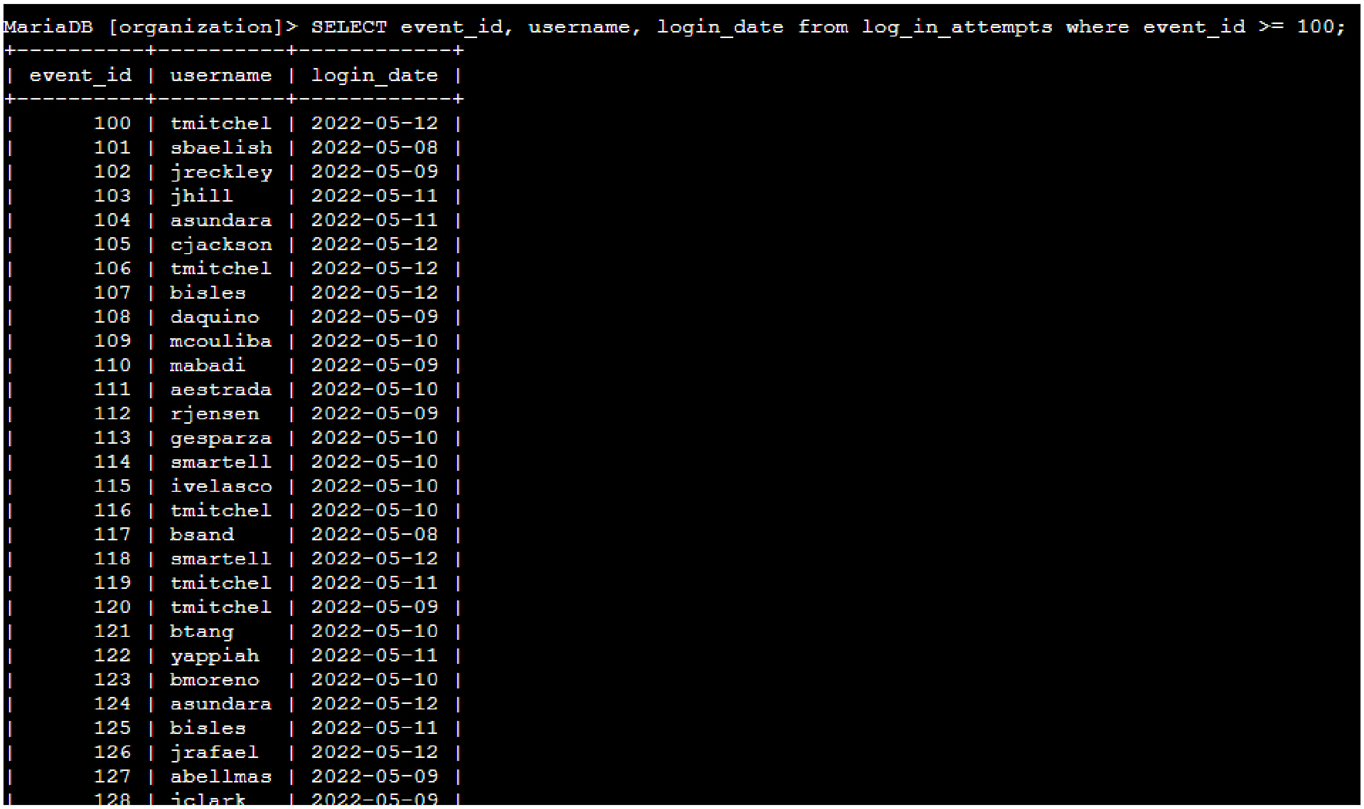
Task 4: Investigate Login Attempts by Event ID

Objective:
Analyze login attempts by focusing on specific event IDs, ensuring that only the necessary data fields are retrieved.

1- Retrieve Login Attempts with Event IDs Greater Than or Equal to 100:

Query:
SELECT event_id, username, login_date FROM log_in_attempts WHERE event_id >= 100;

Outcome:
The login date of the third result returned by this query was May 9, 2022.

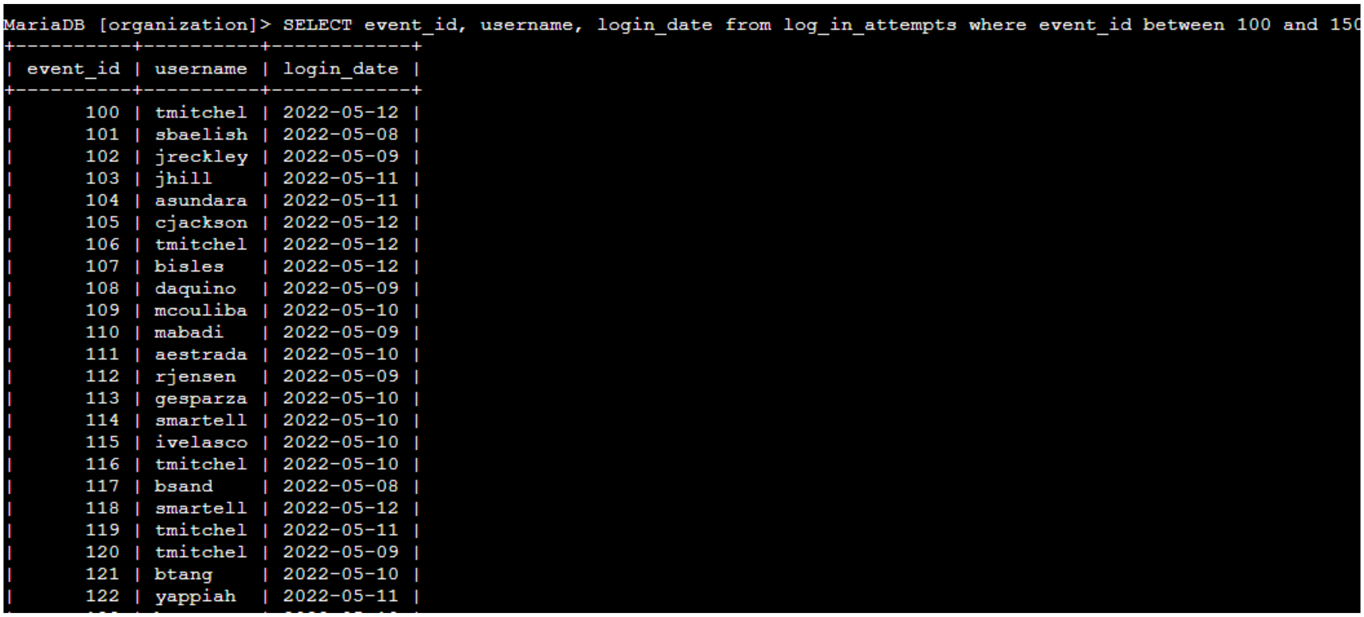


```
MariaDB [organization]> SELECT event_id, username, login_date from log_in_attempts where event_id >= 100;
+----------+----------+------------+
| event_id | username | login_date |
+----------+----------+------------+
|      100 | tmitchel | 2022-05-12 |
|      101 | sbaelish | 2022-05-08 |
|      102 | jreckley | 2022-05-09 |
|      103 | jhill    | 2022-05-11 |
|      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 |
|      109 | mcouliba | 2022-05-10 |
|      110 | mabadi   | 2022-05-09 |
|      111 | aestrada | 2022-05-10 |
|      112 | rjensen  | 2022-05-09 |
|      113 | gesparza | 2022-05-10 |
|      114 | smartell | 2022-05-10 |
|      115 | ivelasco | 2022-05-10 |
|      116 | tmitchel | 2022-05-10 |
|      117 | bsand    | 2022-05-08 |
|      118 | smartell | 2022-05-12 |
|      119 | tmitchel | 2022-05-11 |
|      120 | tmitchel | 2022-05-09 |
|      121 | btang    | 2022-05-10 |
|      122 | yappiah  | 2022-05-11 |
|      123 | bmoreno  | 2022-05-10 |
|      124 | asundara | 2022-05-12 |
|      125 | bisles   | 2022-05-11 |
|      126 | jrafael  | 2022-05-12 |
|      127 | abellmas | 2022-05-09 |
|      128 | jclark   | 2022-05-09 |
```

2- Refine the Query to Focus on a Specific Range of Event IDs:

Query:
SELECT event_id, username, login_date FROM log_in_attempts WHERE event_id BETWEEN 100 AND 150;

Outcome:
The query refined the results to focus on event IDs between 100 and 150, with the seventh result being associated with the username `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 |
|      109 | mcouliba | 2022-05-10 |
|      110 | mabadi   | 2022-05-09 |
|      111 | aestrada | 2022-05-10 |
|      112 | rjensen  | 2022-05-09 |
|      113 | gesparza | 2022-05-10 |
|      114 | smartell | 2022-05-10 |
|      115 | ivelasco | 2022-05-10 |
|      116 | tmitchel | 2022-05-10 |
|      117 | bsand    | 2022-05-08 |
|      118 | smartell | 2022-05-12 |
|      119 | tmitchel | 2022-05-11 |
|      120 | tmitchel | 2022-05-09 |
|      121 | btang    | 2022-05-10 |
|      122 | yappiah  | 2022-05-11 |
```

Reflection:

This project involved using SQL queries to perform a detailed investigation of login activities in response to a potential security incident. The tasks highlighted my ability to filter and analyze large datasets to extract meaningful insights, which are crucial for maintaining organizational security.