Apply filters to SQL queries

Project description

Investigate security issues to help keep the system secure. Some potential security issues that involve login attempts and employee machines have been recently discovered.

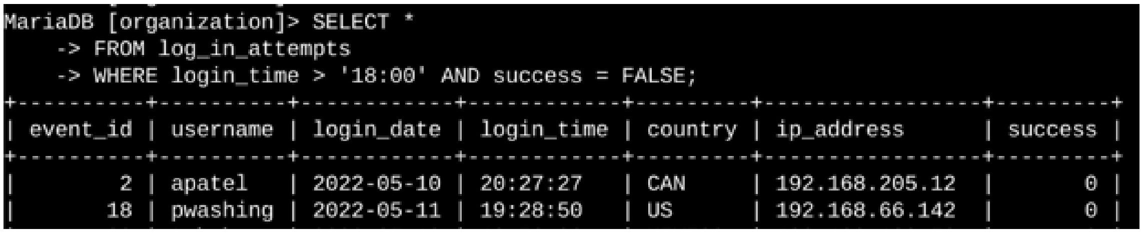
The task is to examine the organization’s data in their employees and log_in_attempts tables.

Retrieve after hours failed login attempts

Task: Your team is investigating failed login attempts that were made after business hours. You want to retrieve this information from the login activity. You’ll identify all unsuccessful attempts after 18:00.

Command used:

```
SELECT *
FROM log_in_attempts
WHERE login_time > '18:00' AND success = FALSE;
```



```
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 |
```

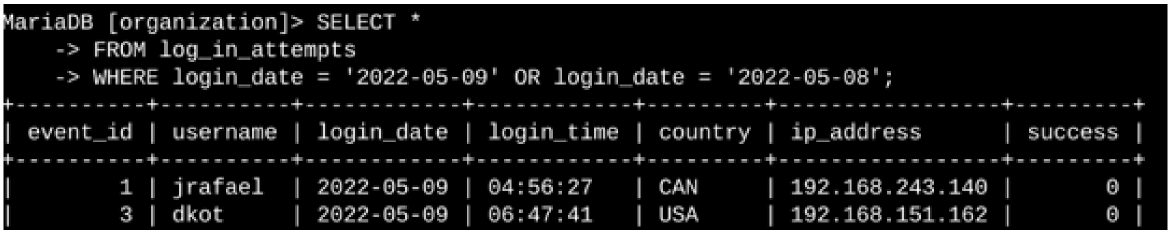
There are 19 failed login attempts that occurred after 18:00.

Retrieve login attempts on specific dates

Task: Your team is investigating a suspicious event that occurred on '2022-05-09'. You want to retrieve all login attempts that occurred on this day and the day before ('2022-05-08').

Command used:

```
SELECT *
FROM log_in_attempts
WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```



```
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 |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       0 |
```

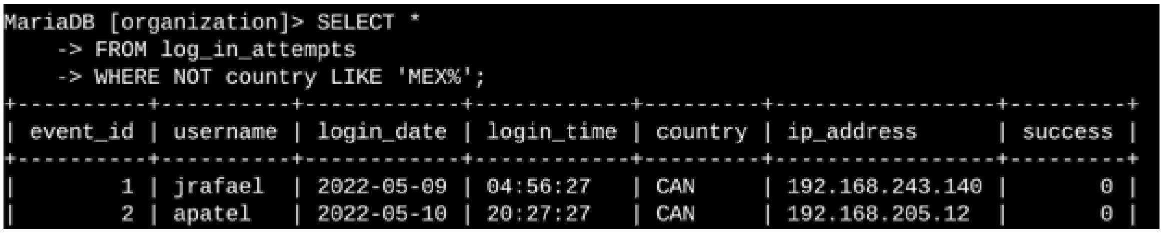
There are 75 login attempts in these two days.

Retrieve login attempts outside of Mexico

Task: Now, your team is investigating logins that did not originate in Mexico, and you need to find this information. Note that the country field includes entries with 'MEX' and 'MEXICO'. You should use the NOT and LIKE operators and the matching pattern 'MEX%'.

Command used:

```
SELECT *
FROM log_in_attempts
WHERE NOT country LIKE 'MEX%';
```



```
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 |       0 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
```

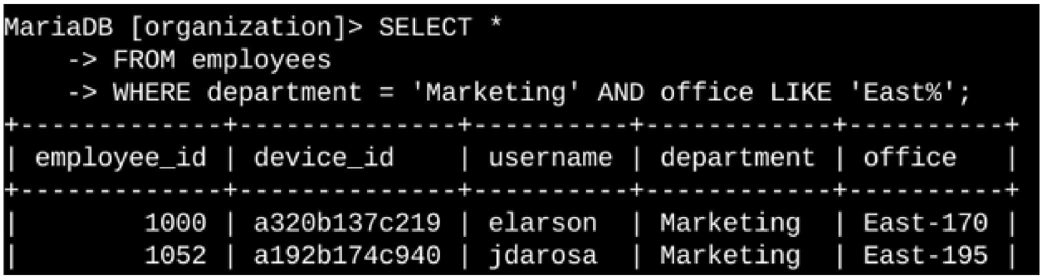
The number of login attempts outside of Mexico was 144.

Retrieve employees in Marketing

Task: Your team is updating employee machines, and you need to obtain the information about employees in the 'Marketing' department who are located in all offices in the East building (such as 'East-170' or 'East-320'). Find the name of the first employee in the Marketing Department.

Command used:

```
SELECT *
FROM employees
WHERE department = 'Marketing' AND office LIKE 'East%';
```



```
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 |
```

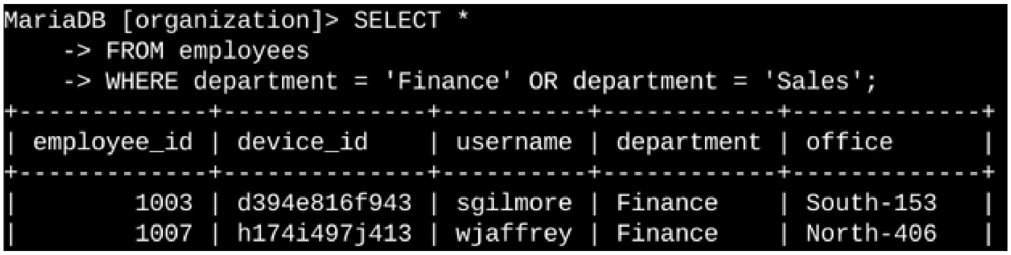
The username of the first employee in the Marketing department in the East building is elarson.

Retrieve employees in Finance or Sales

Task: Now, your team needs to perform a different update to the computers of all employees in the Finance or the Sales department, and you need to locate information on these employees. Find the name of the first employee in the Finance or Sales Department.

Command used:

```
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   |
```

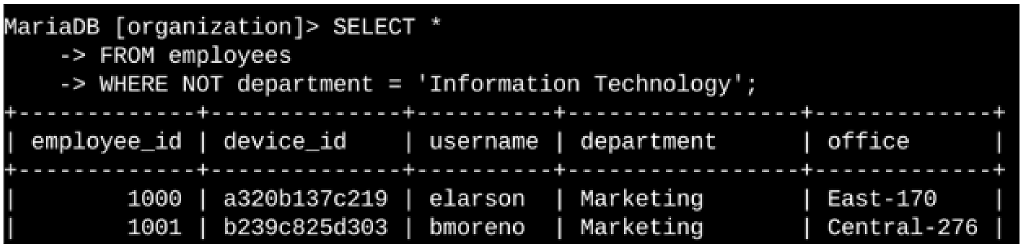
The username of the first employee in the Sales department is sgilmore.

Retrieve all employees not in IT

Task: Your team needs to make one more update. This update was already made to employee computers in the Information Technology department. The team needs information about employees who are not in that department. You should use the NOT operator to identify these employees.

Command used:

```
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 |
```

There are 161 employees who aren’t in the Information Technology department.

Summary

We successfully examined the logs given to us and provided the requested information. There was indeed suspicious activity. This is all the information we currently found; we will use other tools to dive deeper into the potential issue to confirm the safety of the company.

Note: We used the AND, OR, and NOT operators to filter the information required for each task. We also used LIKE and the percentage sign (%) wildcard to filter for patterns.