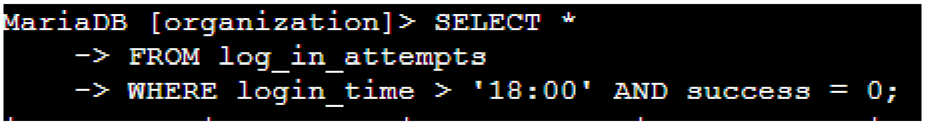
Apply filters to SQL queries

Project description

I used SQL queries with filters (including WHERE, OR, NOT, and LIKE) to investigate potential security issues by retrieving and narrowing down records from the **employees** and **log_in_attempts** tables**.** Specifically, I identified suspicious and policy-relevant login activity by filtering for certain users, dates/times. Locations and outcomes, and I cross-referenced these results with employee details such as department and office location. This allowed me to isolate the most relevant records, determine which employees and machines were involved, and support incident analysis with clear, targeted datesets.

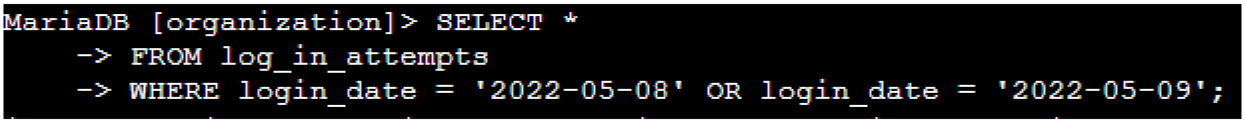
Retrieve after hours failed login attempts



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = 0;
```

Explanation:
This query returns all records from log_in_attempts where the login attempt happened after 6:00 PM (login_time > '18:00') and the attempt was unsuccessful (success = 0). Using AND makes sure both conditions must be true, which helps isolate potentially suspicious after-hours failed logins.

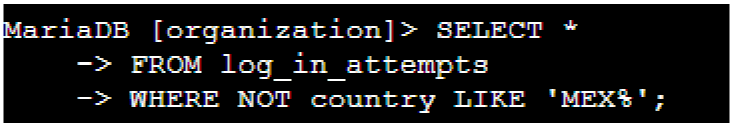
Retrieve login attempts on specific dates



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-08' OR login_date = '2022-05-09';
```

Explanation:
This query retrieves all login attempts that occurred on either 2022-05-09 or 2022-05-08. The OR operator includes rows that match at least one of the two dates, which is useful for reviewing activity on the suspicious day and the day before.

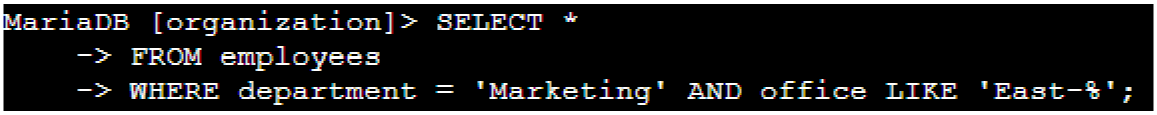
Retrieve login attempts outside of Mexico



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT country LIKE 'MEX%';
```

Explanation:
This query returns all login attempts where the country value does not contain the pattern MEX. Using LIKE '%MEX%' matches any value containing “MEX” anywhere in the text (covering both MEX and MEXICO). Adding NOT excludes those Mexico-based attempts, leaving only login attempts that occurred outside Mexico.

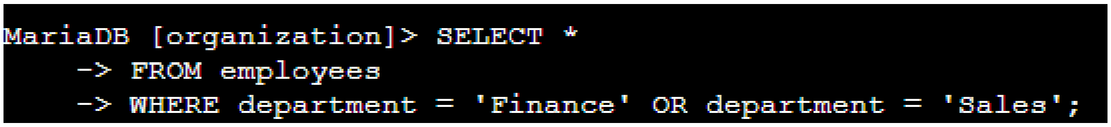
Retrieve employees in Marketing



```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Marketing' AND office LIKE 'East-%';
```

Explanation:
This query pulls employees whose department contains Marketing and whose office location is in the East building. department LIKE '%Marketing%' matches values that include the word “Marketing,” even if the field contains extra text. office LIKE 'East%' matches office values that start with “East” (such as East-170, East-320). Using AND ensures employees meet both conditions.

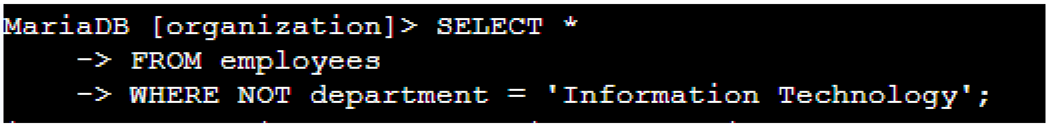
Retrieve employees in Finance or Sales



```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Finance' OR department = 'Sales';
```

Explanation:
This query retrieves employees in either the Finance department or the Sales department. The OR operator includes employees that match one department or the other, which is useful when your update applies to multiple departments.

Retrieve all employees not in IT



```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE NOT department = 'Information Technology';
```

Explanation:
This query returns all employees whose department does not include “Information Technology.” NOT LIKE excludes IT employees (who already received the update), leaving employees from all other departments who still need the update.

Summary

In this investigation, I used SQL filtering techniques to isolate relevant records from the **employees** and **log_in_attempts** tables. I identified potentially suspicious activity by querying **after-hours failed logins**, isolating **login attempts on specific dates**, and filtering attempts **outside of Mexico**. I also retrieved targeted employee groups by filtering departments and office locations (Marketing in East offices, Finance/Sales staff, and all employees not in IT). These queries helped narrow large datasets into actionable subsets for security review and incident reporting.