Apply Filters to SQL Queries

Project Description

In this project, we use SQL queries to investigate potential security incidents by analyzing login attempts. We apply various filters to identify specific patterns, including failed logins after hours, suspicious logins on specific dates, and login attempts originating from outside a specific location. Additionally, we filter employee data to assist with security updates in specific departments and offices. This document demonstrates the use of SQL filtering techniques, including the LIKE keyword, date and time filtering, and the AND, OR, and NOT operators.

Retrieve After Hours Failed Login Attempts

Query:

```
SELECT *

FROM log_in_attempts

WHERE success = 0 AND TIME(login_time) > '18:00:00';
```

Explanation

This query retrieves all failed login attempts that occurred after 18:00. The success = 0 condition filters for failed attempts, while TIME(login_time) > '18:00:00' ensures that only logins after 6 PM are selected.

Retrieve Login Attempts on Specific Dates

Query:

```
SELECT *

FROM log_in_attempts

WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

Explanation

This query selects all login attempts made on May 8 and 9, 2022. The OR operator allows filtering for either date.

Retrieve Login Attempts Outside of Mexico

Query:

```
SELECT *

FROM log_in_attempts
```

WHERE country NOT LIKE 'MEX%' AND country NOT LIKE 'MEXICO';

Explanation

This query retrieves login attempts from countries other than Mexico. The NOT LIKE keyword is used to exclude values beginning with 'MEX' or exactly 'MEXICO'.

Retrieve Employees in Marketing Department in East Building

Query:

SELECT *

FROM employees

WHERE department = 'Marketing' AND office LIKE 'East-%';

Explanation

This query identifies employees working in the Marketing department at offices located in the East building. The LIKE keyword with 'East-%' matches any office name starting with 'East-'.

Retrieve Employees in Finance or Sales Departments

Query:

SELECT *

FROM employees

WHERE department = 'Finance' OR department = 'Sales';

Explanation

This query selects all employees who belong to either the Finance or Sales departments using the OR operator.

Retrieve All Employees Not in IT Department

Query:

SELECT *

FROM employees

WHERE department <> 'Information Technology';

Explanation

This query excludes employees from the Information Technology department by using the <> (not equal) operator.

Summary

This project demonstrates SQL filtering techniques for security investigations and employee data management. We identified failed login attempts after hours, suspicious logins on specific dates, and logins from non-Mexican locations. Additionally, we filtered employee data for security updates, specifically focusing on Marketing, Finance, Sales, and non-IT departments. These techniques are valuable for data analysis in security contexts.