

Apply filters to SQL queries

Project description

As a security professional, I use SQL queries to investigate potential security issues within an organization. This document demonstrates my ability to filter and retrieve specific data from the employees and log_in_attempts tables, utilizing various SQL operators such as AND, OR, NOT, and LIKE to conduct thorough security investigations.

Retrieve after hours failed login attempts

To identify all failed login attempts that occurred after 18:00, I used the following SQL query:

```
SELECT *  
FROM log_in_attempts  
WHERE login_time > '18:00:00'  
AND success = 0;
```

This query selects all records from the log_in_attempts table where the login_time is after 18:00 and the success column equals 0, indicating a failed login attempt.

Retrieve login attempts on specific dates

To review all login attempts that occurred on 2022-05-09 or 2022-05-08, I used the following SQL query:

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

This query selects all records from the log_in_attempts table where the login_date is either 2022-05-09 or 2022-05-08, allowing for the investigation of incidents on those specific dates.

Retrieve login attempts outside of Mexico

To identify all login attempts that occurred outside of Mexico, I used the following SQL query:

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

AND country NOT LIKE 'MEXICO';

This query selects all records from the log_in_attempts table where the country column does not start with 'MEX' or equal 'MEXICO', filtering out login attempts from Mexico.

Retrieve employees in Marketing

To get information on employee machines in the Marketing department located in the East building, I used the following SQL query:

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

This query selects all records from the employees table where the department is 'Marketing' and the office column starts with 'East', ensuring we retrieve only those employees in the Marketing department located in the East building.

Retrieve employees in Finance or Sales

To identify all employees in the Sales or Finance departments, I used the following SQL query:

```
SELECT *  
FROM employees  
WHERE department = 'Sales'  
OR department = 'Finance';
```

This query selects all records from the employees table where the department is either 'Sales' or 'Finance', retrieving employees from both departments.

Retrieve all employees not in IT

To find all employees not in the Information Technology department, I used the following SQL query:

```
SELECT *  
FROM employees  
WHERE department <> 'Information Technology';
```

This query selects all records from the employees table where the department is not 'Information Technology', filtering out employees from the IT department.

Summary

In this exercise, I applied SQL queries to filter and retrieve specific data crucial for investigating potential security issues within an organization. By using operators such as AND, OR, NOT, and LIKE, I effectively filtered login attempts and employee data to support security investigations and updates. These skills are essential for maintaining secure and efficient operations within any organization.