Apply filters to SQL queries

Project description

In this project, I'm a security professional at a large organization. Part of my job is to investigate security issues to help keep the system secure. I recently discovered some potential security issues that involve login attempts and employee machines.

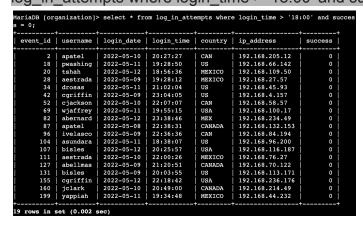
The task is to examine the organization's data in their employees and log_in_attempts tables. I need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

Here I'm getting familiar with the data in the tables.



Retrieve after hours failed login attempts

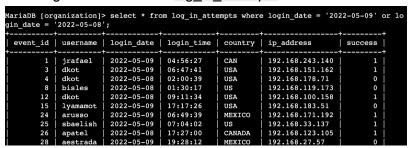
I'm investigating the failed login attempts that were made after business hours. I want to retrieve this information from the login activity by using the following code select * from log in attempts where login time > '18:00' and success = 0;



Retrieve login attempts on specific dates

The following code demonstrates how I created a SQL query to filter for login attempts that occurred on specific dates.

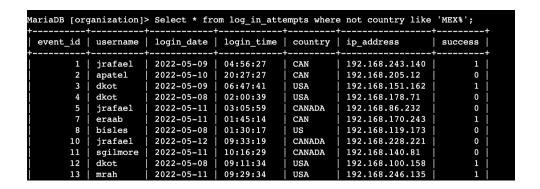
The first part of the screenshot is my query, and the second part is a portion of the output. This query returns all login attempts that occurred on 2022-05-09 or 2022-05-08. First, I started by selecting all data from the log in attempts table



Retrieve login attempts outside of Mexico

After investigating the organization's data on login attempts, I believe there is an issue with the login attempts that occurred outside of Mexico. These login attempts should be investigated.

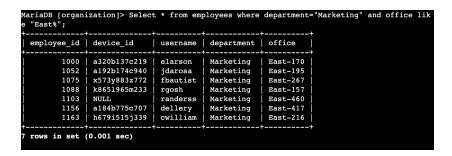
The following code demonstrates how I created a SQL query to filter for login attempts outside of Mexico.



Retrieve employees in Marketing

My team wants to update the computers for certain employees in the Marketing department. To do this, I have to get information on which employee machines to update.

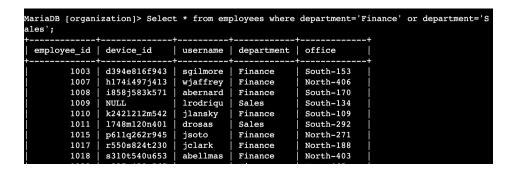
The following code demonstrates how I created a SQL query to filter for employee machines from employees in the Marketing department in the East building.



Retrieve employees in Finance or Sales

The machines for employees in the Finance and Sales departments also need to be updated. Since a different security update is needed, I have to get information on employees only from these two departments.

The following code demonstrates how I created a SQL query to filter for employee machines from employees in the Finance or Sales departments.



Retrieve all employees not in IT

My team needs to make one more security update on employees who are not in the Information Technology department. To make the update, I first have to get information on these employees.

The following demonstrates how I created a SQL query to filter for employee machines from employees not in the Information Technology department.



Summary

I applied filters to SQL queries to get specific information on login attempts and employee machines. I used two different tables, $log_in_attempts$ and employees. I used the AND, OR, and NOT operators to filter for the specific information needed for each task. I also used LIKE and the percentage sign (%) wildcard to filter for patterns.