Apply filters to SQL queries

Project description

I am 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. My task is to examine the organization's data in their employees and log\_in\_attempts tables. I will need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

Retrieve after hours failed login attempts

  
  
Using this SQL query with the filter AND, I was able to look through all failed login attempts that occured after 6 p.m.This query works by selecting all the data from the log\_in\_attempts table. The query then removes any login\_time before 6 p.m. and any successful logins from the output.  
  
Since 18:00 is a numeric string, single quotation marks, ('), are placed on either side.  
Since the 0 in success = 0 is a Boolean, single quotation marks are not needed. In addition, the 0 means FALSE. A 1 would be TRUE  
  
Wanting to get a chronological timeframe of login\_times, I decided to use the ORDER BY clause

Retrieve login attempts on specific dates



A suspicious event occured on 2022-05-09. To investigate this event, I wanted to review all login attempts which occured on this day and the day before.

Using the OR filter, the data I got back was either from 2022-05-09 or 2022-05-08

Retrieve login attempts outside of Mexico



The team has determined that the suspicious login attempts did not originate in Mexico. Therefore, I needed to filter out any data with Mexico. Since our database uses abbreviations, filtering with the percent (%) wildcard will work best.

WHERE NOT country LIKE 'Mex%'; tells the database to not bring back anything in the country row that starts with 'Mex'. Since 'Mex' is the abbreviation of Mexico, we will not see any login attempts from that country.

Retrieve employees in Marketing



My team wants to perform security updates on specific employee machines in the Marketing department.

Using the AND filter, I was able to limit searching in the employees table to only those in the Marketing department and also located in the east office. In order to get every individual office number, I needed to use the LIKE "east%" wildcard. Using this I was able to get back information on every office number located in the east building.

Retrieve employees in Finance or Sales



My team now needs to perform a different security update on machines for employees in the Sales and Finance departments. Since I needed both departments to be outputted, I decided to use the OR filter.

Retrieve all employees not in IT



My team needs to make one more update to employee machines. We know that the employees in the Information Technology already had the update, but everyone else needs it. Since we need to remove anyone from IT, I decided to use the NOT filter.

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.