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 involved login attempts and employee machines. My task is to examine the organization’s data in their employees and log_in_attempts tables. I used SQL filters to retrieve records from different datasets and used them to investigate the potential security issues.

Retrieve after hours failed login attempts

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

This SQL query was used to return all columns in the login attempts table that were after the time 6:00pm which failed. This allows me to check for any suspicious activity that occurred after the end of the work day. Using the AND operator means that both conditions have to be met to return the data that I want.

Retrieve login attempts on specific dates

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

This SQL query was used to return all columns in the login attempts table that were made within this date range. Using the OR operator means that both of these conditions or just one of them could be met.

Retrieve login attempts outside of Mexico

```
SELECT *
FROM log_in_attempts
WHERE NOT country LIKE ‘Mex%’;
```

This SQL query was used to return all login attempts made from countries besides Mexico. Using the NOT operator makes it more efficient to do instead of making a query for each country. Using the LIKE operator and % wildcard helped because some inputs for Mexico were written as Mexico or Mex.

Retrieve employees in Marketing

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

This SQL query was used to return the names of the employees that work in the marketing the part and are in the East office building. Using AND helps set that these conditions must be met simultaneously as well as using the LIKE operator and % wildcard let's you include all the specific rooms in the East building.

Retrieve employees in Finance or Sales

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

This SQL query was used to return the names of the employees that work in the Finance as well as the Sales departments. Using the OR operator is effective for this query because it lists our all the records.

Retrieve all employees not in IT

```
SELECT *
FROM employees
WHERE NOT department = 'Information Technology';
```

This SQL query was used to return the names of the employees outside the Information Technology department which is a more efficient way of querying the database as opposed to searching for each individual condition/department.

Summary

This assignment involved utilizing SQL queries to search through the employees and log_in_attempts database to investigate the potential of security issues. By looking through the log_in_attempts data based on specific times, dates, locations, and successes logins were made, this allowed me to check if there is any suspicious activity that was occurring. Additionally, since these tables are relational databases, it also helps with finding machines that are not currently up to date in their patch updates which is a necessary procedure to ensure vulnerabilities are minimized.