Apply filters to SQL queries

Project description

You are a security professional at a large organization. Part of your job is to investigate security issues to help keep the system secure. You recently discovered some potential security issues that involve login attempts and employee machines.

Your task is to examine the organization's data in their employees and log_in_attempts tables. You'll need to use SQL filters to retrieve records from different datasets and 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 query will output login attempts past regular office hours of 6PM that have failed to help show unusual activity in the office.

Retrieve login attempts on specific dates

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

This query will return all login attempts that occurred on either May 8th 2022 or May 9th 2022.

Retrieve login attempts outside of Mexico

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

This query will return any logins that occurred outside of Mexico.

Retrieve employees in Marketing

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

This query will return us all employees that work in Marketing and that work in any of the East office buildings.

Retrieve employees in Finance or Sales

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

This query will simply return us all employees that work either in Finance or Sales.

Retrieve all employees not in IT

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

This last query will show us all employees excluding IT employees.

Summary

In this mini project, we explored SQL queries to investigate potential security issues within an organization's login attempts and employee records. As a security professional, I used SQL filters to retrieve specific datasets that could indicate unusual or suspicious activities.