Apply filters to SQL queries

Completed by: Nida Azam

Project Description

When I started this project, my goal was to learn how to use SQL in a real cybersecurity situation. I had to investigate possible login issues and find patterns in data that could point to something suspicious. I used different SQL filters like AND, OR, and NOT to dig through data and make sense of what was happening. Doing this made me realize how powerful SQL is when it comes to analyzing real security events.

➢ *Retrieve after hours failed login attempts*

Query:

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

Explanation:

Here, I wanted to check for any failed login attempts that happened after work hours. I used `login_time > '18:00:00'` to get all logins after 6 PM and `success = FALSE` to only show the ones that failed. This helps find people who might be trying to access the system when no one's supposed to be working which is a red flag in cybersecurity.

➢ *Retrieve login attempts on specific dates*

Query:

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

Explanation:

In this one, I looked for all login attempts that happened on May 8 and 9, 2022. I used the `OR` operator to get both dates together. This is useful when something suspicious happens on a specific day and you want to see if anything strange also happened right before or after it.

➢ Retrieve login attempts outside of Mexico

Query:

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

Explanation:

This query helped me check login attempts that didn't come from Mexico. Some entries had `MEX` and some had `MEXICO`, so I used `LIKE '%MEX%'` to cover both. I also used `NOT` to exclude them. This kind of filter helps in tracking down login attempts from unexpected locations.

➢ Retrieve employees in Marketing

Query:

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

Explanation:

This query helped me find all employees who work in the Marketing department and are based in the East building. The `LIKE 'East%'` part finds all offices that start with the word East, like `East-170` or `East-320`. This kind of data is useful when certain departments or locations need special attention for security updates.

➢ Retrieve employees in Finance or Sales

Query:

```
SELECT *
```

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

Explanation:

For this one, I needed info about employees in either Finance or Sales. The `OR` operator made it easy to get both at once. It's simple but super useful when you need to pull data for more than one department together.

- *Retrieve all employees not in IT*

Query:

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

Explanation:

Here I filtered out everyone who's in the IT department since they already got their updates. I used `NOT LIKE` so that any department with "Information Technology" in its name wouldn't show up. This helps make sure the update only goes to people who still need it.

Summary

This whole project helped me understand how SQL can be used in cybersecurity investigations. I practiced using filters like `AND`, `OR`, `NOT`, and `LIKE` to pull out the exact data I needed. Doing this gave me a better idea of how real-world analysts use databases to spot unusual activity and manage security updates. I really enjoyed this part because it felt like solving small mysteries with logic and code.