Apply Filters to SQL Queries

Name: Hridhima Karmakar

Project Description:

In this activity, I practiced applying filters to SQL queries to extract specific data from a cybersecurity incident log database. I used conditional filtering with WHERE, pattern matching with LIKE, logical operators like AND, OR, and NOT, and filtered data based on timestamps. This skill is crucial when investigating anomalies, tracing attacks, or analyzing system logs.

Task 1: Using LIKE to Search for Patterns

Objective: Find all users whose email addresses end in "@internal.com"

Query:

```
SELECT user_id, email
FROM users
WHERE email LIKE '%@internal.com';
```

Explanation:
The % symbol is a wildcard that matches any number of characters. This query retrieves email addresses that end with "@internal.com", which may be used to identify internal staff accounts.

Task 2: Filtering by Date and Time

Objective: Get all login attempts made after January 1, 2024

Query:

```
SELECT user_id, login_time
FROM login_attempts
WHERE login_time > '2024-01-01';
```

Explanation:
The WHERE clause filters results to include only records with a login_time later than the specified date, which is helpful for time-based incident analysis.

Task 3: Filtering with AND and OR

Objective: Identify users who either logged in after January 1, 2024 or whose email contains "admin"

Query:

```
SELECT user_id, email, login_time
FROM users
WHERE login_time > '2024-01-01' OR email LIKE '%admin%';
```

Explanation:
The OR operator allows retrieval of records that meet either condition. This helps identify both recent logins and administrative accounts in one query.

Task 4: Using NOT in Filters

Objective: Find users who are not part of the "external_users" group

Query:

```
SELECT user_id, group_name
FROM users
WHERE NOT group_name = 'external_users';
```

Explanation:
The NOT keyword is used to exclude records that match a specific value. This is useful when focusing on internal users or excluding specific categories from analysis.

Summary

This exercise demonstrated how SQL filtering can be used to extract targeted, relevant data in a cybersecurity context. I used:

- LIKE for pattern matching (e.g., internal emails),
- date-based filtering for tracking activity timelines,
- logical operators AND, OR, and NOT to refine results based on multiple conditions.

Mastering these SQL filtering techniques will help me quickly investigate incidents, spot unusual patterns, and generate meaningful insights from large datasets.