Apply filters to SQL queries

Project description

In this cybersecurity scenario I will play the role of an analyst who uses SQL to obtain specific information about employees, their machines, and the departments they belong to. The data acquired from these queries could be used to investigate potential security issues and to update computers.

Retrieve after hours failed login attempts

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = '0';
```

In this query, I started by selecting all columns (represented by the * symbol) from the log_in_attempts table. Then, using the WHERE filter I specified that I wanted all logs where the login time was past 6pm and where the login attempt failed which is represented by a 0 in the success column.

Retrieve login attempts on specific dates

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

In this query I started by selecting all columns from the login attempts table. Then, using the WHERE filter I specified that I wanted only the logs where the date was equal to May 8th 2022 or May 9th 2022. The OR filter allows me to specify that logs only have to satisfy one of the WHERE filter arguments.

Retrieve login attempts outside of Mexico

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT country LIKE 'MEX%';
```

In this query I started by selecting all columns from the login attempts table. In this case, I wanted all logs that were not from Mexico. I used the WHERE filter and the NOT filter to specify

that I did not want any logs that contained Mexico in the country column. Also, because the country column represents Mexico as “MEX” and “MEXICO”, I had to specifically filter using LIKE that any entry that contains any string with “MEX” is not allowed.

Retrieve employees in Marketing

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department='Marketing' AND office LIKE 'East%';
```

In this query I started by selecting all columns from the employees table. Then using the WHERE filter I specified that I only wanted logs from the Marketing department and from the east offices. Because the east building offices also contain unique numbers, I used the LIKE filter and the percentage wildcard to specify that any office log starting with east should count.

Retrieve employees in Finance or Sales

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department='Finance' OR department='Sales';
```

In this query I selected all columns from the employees table. Then I specified that I only wanted the logs where the department is finance or sales using the OR filter.

Retrieve all employees not in IT

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE NOT department='Information Technology';
```

In this query I started by selecting all columns from the employees table. Then, using the WHERE and NOT filter I specified that I wanted all logs that did not contain “Information Technology” as the department.

Summary

As previously demonstrated, SQL filters such as AND, OR, NOT, and LIKE are useful to find specific information from a database that can be used to solve cybersecurity issues. SQL is a powerful tool that can be used by cybersecurity analysts to quickly navigate through massive amounts of data to acquire useful insights about security issues.