Babatunde Qodri (cybersecurity analyst)

Project Overview: SQL-Based Data Filtering and Security Investigation in MariaDB

This project involved gaining practical experience with SQL commands to filter and analyze databases within the MariaDB shell. I executed SQL queries using operators such as `AND`, `OR`, and `NOT` to retrieve specific information from various datasets. Additionally, I conducted an in-depth investigation aimed at identifying potential security vulnerabilities within the system.

My primary task was to examine the organization's data, particularly focusing on the `employees` and `log_in_attempts` tables. Using SQL filters, I successfully retrieved and analyzed records to uncover potential security issues related to unauthorized login attempts and employee machine activities.

Explanation of SQL Queries Used in MariaDB Shell

In this project, I utilized various SQL commands within the MariaDB shell to filter and retrieve specific information from the database. The key operators and their respective purposes are as follows:

- **AND Operator**: Used to retrieve records of failed login attempts that occurred outside of regular business hours.
- **OR Operator**: Employed to identify records that meet one or more specified conditions.
- **LIKE Operator**: Applied to filter login attempts originating from locations in Mexico by matching patterns in the data.
- **NOT Operator**: Used to identify employees who are not part of the same department within the organization.

These queries were instrumental in extracting relevant information from the databases, allowing for a thorough analysis of the data.

Details on Using the LIKE Operator for Pattern Matching

As part of the cybersecurity investigation, I focused on identifying login attempts that did not originate from Mexico. After initially discovering several countries of origin differing from Mexico, I ran an SQL query to specifically retrieve login attempts excluding those from Mexico.

The SQL filter command used in the MariaDB shell was as follows:

```
SELECT *
FROM log_in_attempts
WHERE Country <> 'MEX' AND Country LIKE 'MEX%';
```

This query effectively filtered out records where the country of origin was not Mexico, allowing for a more targeted analysis of potential security concerns.

```
MariaDB [organization]> SELECT *   FROM log_in_attempts
  WHERE Country <> 'MEX' LIKE 'MEX%';
+----------+----------+------------+------------+------
---+-----------------+---------+
| event_id | username | login_date | login_time | count
ry | ip_address      | success |
+----------+----------+------------+------------+------
---+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN
   | 192.168.243.140 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN
   | 192.168.205.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA
   | 192.168.151.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA
   | 192.168.178.71  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANAD
A  | 192.168.86.232  |       0 |
|        6 | arutley  | 2022-05-12 | 17:00:59   | MEXIC
O  | 192.168.3.24    |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN
   | 192.168.170.243 |       1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US
   | 192.168.119.173 |       0 |
|        9 | yappiah  | 2022-05-11 | 13:47:29   | MEX
   | 192.168.59.136  |       1 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANAD
A  | 192.168.228.221 |       0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANAD
A  | 192.168.140.81  |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA
   | 192.168.100.158 |       1 |
```

Details on Filtering for Dates and Times

In the course of the investigation, we analyzed the timestamps associated with login attempts in the MariaDB shell to identify specific patterns. To determine the exact locations of employees and to retrieve failed login attempts on specified dates, we employed SQL queries using the `BETWEEN` and `AND` operators.

These commands allowed us to effectively filter the data by date and time, ensuring that we could isolate incidents that occurred on particular days or within specific time ranges.

```
MariaDB [organization]> SELECT *  FROM log_in_attempts
 WHERE login_time > '18:00' AND success = FALSE;
+----------+----------+------------+------------+------
---+-----------------+---------+
| event_id | username | login_date | login_time | count
ry | ip_address      | success |
+----------+----------+------------+------------+------
---+-----------------+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN
   | 192.168.205.12  |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US
   | 192.168.66.142  |       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXIC
O  | 192.168.109.50  |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXIC
O  | 192.168.27.57   |       0 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US
   | 192.168.45.93   |       0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US
   | 192.168.4.157   |       0 |
|       52 | cjackson | 2022-05-10 | 22:07:07   | CAN
   | 192.168.58.57   |       0 |
|       69 | wjaffrey | 2022-05-11 | 19:55:15   | USA
   | 192.168.100.17  |       0 |
|       82 | abernard | 2022-05-12 | 23:38:46   | MEX
   | 192.168.234.49  |       0 |
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANAD
A  | 192.168.132.153 |       0 |
|       96 | ivelasco | 2022-05-09 | 22:36:36   | CAN
   | 192.168.84.194  |       0 |
|      104 | asundara | 2022-05-11 | 18:38:07   | US
   | 192.168.96.200  |       0 |
```

Details on Using AND and OR to Filter on Multiple Conditions

During the cybersecurity investigation, we examined a suspicious event that took place on '2022-05-09'. To gain a broader context, we retrieved all login attempts that occurred on both this date and the previous day, '2022-05-08'.

Using the `OR` operator, we constructed an SQL query to filter the login attempts on these specific dates. The query used was as follows:

```
SELECT *
FROM log_in_attempts
```

```
WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

By replacing the dates with the relevant values, we were able to isolate the records needed for further analysis.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_date = '2022-05-09' OR login_date =
'2022-05-08';
+----------+----------+------------+------------+------
---+-----------------+---------+
| event_id | username | login_date | login_time | count
ry | ip_address      | success |
+----------+----------+------------+------------+------
---+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN
   | 192.168.243.140 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA
   | 192.168.151.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA
   | 192.168.178.71  |       0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US
   | 192.168.119.173 |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA
   | 192.168.100.158 |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA
   | 192.168.183.51  |       0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXIC
O  | 192.168.171.192 |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US
   | 192.168.33.137  |       1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANAD
A  | 192.168.123.105 |       1 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXIC
O  | 192.168.27.57   |       0 |
```

Details on Using NOT in Filters

As part of the cybersecurity investigation, we focused on identifying failed login attempts that occurred outside of regular business hours. Specifically, we filtered for unsuccessful attempts made after 18:00.

The SQL command used to perform this task was:

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

This query allowed us to isolate login attempts that were both unsuccessful and occurred after the close of business, highlighting potential security concerns.

```
MariaDB [organization]> SELECT *  FROM log_in_attempts
 WHERE login_time > '18:00' AND success = FALSE;
+----------+----------+------------+------------+------
---+-----------------+---------+
| event_id | username | login_date | login_time | count
ry | ip_address      | success |
+----------+----------+------------+------------+------
---+-----------------+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN
   | 192.168.205.12  |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US
   | 192.168.66.142  |       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXIC
O  | 192.168.109.50  |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXIC
O  | 192.168.27.57   |       0 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US
   | 192.168.45.93   |       0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US
   | 192.168.4.157   |       0 |
|       52 | cjackson | 2022-05-10 | 22:07:07   | CAN
   | 192.168.58.57   |       0 |
|       69 | wjaffrey | 2022-05-11 | 19:55:15   | USA
   | 192.168.100.17  |       0 |
|       82 | abernard | 2022-05-12 | 23:38:46   | MEX
   | 192.168.234.49  |       0 |
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANAD
A  | 192.168.132.153 |       0 |
|       96 | ivelasco | 2022-05-09 | 22:36:36   | CAN
   | 192.168.84.194  |       0 |
|      104 | asundara | 2022-05-11 | 18:38:07   | US
   | 192.168.96.200  |       0 |
```

Summary

At the conclusion of this activity, the cybersecurity analyst successfully executed a series of SQL queries to extract sensitive information from the organization's databases. Key activities included:

- Retrieving failed login attempts occurring after business hours
- Filtering login attempts on specific dates
- Identifying login attempts originating outside of Mexico
- Isolating employees in the marketing department
- Retrieving employees in the finance or sales departments
- Listing all employees not in the IT department