Diana Kelsch

Apply filters to SQL queries

Project description:

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

My task is to examine the organization's data in their **employees** and **log_in_attempts** tables. I will use SQL filters to retrieve records from different datasets and investigate the potential security issues.

Retrieve after hours failed login attempts

I recently discovered a potential security incident that occurred after business hours. To investigate this, I need to query the **log_in_attempts** table and review after hours login activity. I will be using filters in SQL to create queries that identify all failed login attempts that occurred after 18:00.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00:00' and success = FALSE;
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | 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   | MEXICO  | 192.168.109.50  |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 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   | CANADA  | 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 |
|      107 | bisles   | 2022-05-12 | 20:25:57   | USA     | 192.168.116.187 |       0 |
|      111 | aestrada | 2022-05-10 | 22:00:26   | MEXICO  | 192.168.76.27   |       0 |
|      127 | abellmas | 2022-05-09 | 21:20:51   | CANADA  | 192.168.70.122  |       0 |
|      131 | bisles   | 2022-05-09 | 20:03:55   | US      | 192.168.113.171 |       0 |
|      155 | cgriffin | 2022-05-12 | 22:18:42   | USA     | 192.168.236.176 |       0 |
|      160 | jclark   | 2022-05-10 | 20:49:00   | CANADA  | 192.168.214.49  |       0 |
|      199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO  | 192.168.44.232  |       0 |
+----------+----------+------------+------------+---------+-----------------+---------+
19 rows in set (0.051 sec)
```

Using the command:

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

I was able to determine there were 19 failed login attempts that occurred after 18:00

Retrieve login attempts on specific dates

A suspicious event occurred on 2022-05-09. To investigate this event, I want to review all login attempts which occurred on this day and the day before. Using filters in SQL I will create a query that identifies all login attempts that occurred on 2022-05-09 or 2022-05-08.

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

Using the command:

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

I was able to determine there were 75 login attempts on these two days.

Retrieve login attempts outside of Mexico

There's been suspicious activity with login attempts, but the team has determined that this activity didn't originate in Mexico. I need to investigate login attempts that occurred outside of Mexico.

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

```
144 rows in set (0.037 sec)
```

Using the command:

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

I was able to determine that 144 login attempts did not originate in Mexico.

Retrieve employees in Marketing

The team wants to perform security updates on specific employee machines in the Marketing department. I am responsible for getting information on these employee machines and will need to query the **employees** table. Using filters in SQL I will create a query that identifies all employees in the Marketing department for all offices in the East building.

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'marketing' AND office LIKE 'EAST%';
+-------------+--------------+----------+------------+----------+
| employee_id | device_id    | username | department | office   |
+-------------+--------------+----------+------------+----------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195 |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267 |
|        1088 | k8651965m233 | rgosh    | Marketing  | East-157 |
|        1103 | NULL         | randerss | Marketing  | East-460 |
|        1156 | a184b775c707 | dellery  | Marketing  | East-417 |
|        1163 | h679i515j339 | cwilliam | Marketing  | East-216 |
+-------------+--------------+----------+------------+----------+
7 rows in set (0.022 sec)
```

Using the command:

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

I was able to determine there were 7 employee machines in the marketing department at the East building.

Retrieve employees in Finance or Sales

The team now needs to perform a different security update on machines for employees in the Sales and Finance departments and I need to locate information on these employees.

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

Using the command:

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

I was able to determine there were 71 employees in these departments located in different offices.

Retrieve all employees not in IT

The team needs to make one more update to employee machines. The employees who are in the Information Technology department already had this update, but employees in all other departments need it.

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

Using the command:

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

I was able to determine that 161 employees are not in the Information Technology department

**All of the screen shots with the results were not included for sizing purposes*

Diana Kelsch

SUMMARY

I applied filters to SQL queries to get specific information on login attempts and employee machines. I used two different tables**, log_in_attempts** and **employees**. I used the **AND**, **OR,** and **NOT** operators to filter for the specific information needed for each task. I also used **LIKE** and the **(%)** wildcard to filter for patterns.