Aplicación de filtros a consultas SQL

Descripción del proyecto

Como profesional de la seguridad en una gran organización, mi trabajo consiste en investigar los problemas de seguridad para ayudar a mantener el sistema seguro. Recientemente se descubrió algunos potenciales problemas de seguridad relacionados con los intentos de inicio de sesión y las máquinas de los empleados. En el siguiente trabajo se presentan la implementación de tareas de seguridad con SQL para filtrar algunos datos.

Recupera intentos de inicio de sesión fallidos después del horario laboral

Se descubrió un posible incidente de seguridad que se produjo después del horario laboral. Para investigarlo, consulte la tabla `log_in_attempts` y revise la actividad de inicio de sesión fuera del horario laboral. Utilice filtros en SQL para crear una consulta que identifique todos los intentos de inicio de sesión fallidos que se produjeron después de las 18:00.

La siguiente imagen muestra mi consulta y un fragmento del resultado:

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' 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 |
```

La consulta empieza seleccionando todas las columnas de la tabla `log_in_attempts`, por último, una cláusula `WHERE login_time > '18:00' AND success = FALSE` para de esta manera obtener solo los intentos de inicio de sesión fallidos que tuvieron lugar después de las 18:00 y filtrar los intentos de inicio de sesión fallidos.

Recupera intentos de inicio de sesión en fechas específicas

Un evento sospechoso tuvo fecha del 09-05-2022. Investigando este evento, revise todos los intentos de inicio de sesión que se produjeron ese día y el anterior, utilizado filtros en SQL para crear una consulta que identifique todos los intentos de inicio de sesión que se produjeron el 09-05-2022 o el 08-05-2022.

La siguiente imagen muestra mi consulta y un fragmento del resultado:

```
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 | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       0 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
```

La consulta empieza seleccionando todas las columnas de la tabla `log_in_attempts`, por último, una cláusula `WHERE login_date = '2022-05-09' OR login_date = '2022-05-08',` la primera condición satisface los intentos de inicio de sesión que se produjeron el 09-05-2022 y la segunda condición después del operador lógico `OR` incluye también todos los intentos de inicio de sesión que se produjeron el 08-05-2022

Recupera intentos de inicio de sesión fuera de México

Después de cierta actividad sospechosa de intentos de inicio de sesión, el equipo ha determinado que esta actividad no se originó en México. Se investigo los intentos de inicio de sesión que se produjeron fuera de México. Utilice filtros en SQL para crear una consulta que identifique todos los intentos de inicio de sesión que ocurrieron fuera de México

La siguiente imagen muestra mi consulta y un fragmento del resultado:

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT country LIKE 'MEX%';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       0 |
|        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 |       0 |
```

La consulta empieza seleccionando todas las columnas de la tabla `log_in_attempts`, por último, una cláusula `WHERE NOT country LIKE 'MEX%',` esto para filtrar por países que no son México. Usé `LIKE` con `MEX%` como el patrón de coincidencia, porque el conjunto de datos representa a México como `MEX` y/o `MEXICO`, el signo de porcentaje `'%'` representa cualquier número de caracteres no especificados que están a la derecha de los demás caracteres cuando se usan con `LIKE`.

Recupera empleados/as en Marketing

Se realizaron actualizaciones de seguridad en equipos específicos de empleados/as del departamento de Marketing. Consulte la tabla `employees`. Utilice filtros en SQL para crear una consulta que identifique a todos los empleados del departamento de Marketing para todas las oficinas del edificio Este.

La siguiente imagen muestra mi consulta y un fragmento del resultado:

```
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 |
```

La consulta empieza seleccionando todas las columnas de la tabla `employees`, por último, una cláusula `WHERE department = 'Marketing' AND office LIKE 'East%'`, la primera condición filtra por empleados en el departamento de Marketing y la segunda después del operador lógico `AND` filtra por empleados en el edificio Este. Usé `LIKE` con `'East%'` como el patrón de coincidencia, porque el conjunto de datos representa a Este como `East-X` seguido de diferentes números, el signo de porcentaje `'%'` representa cualquier número de caracteres no especificados que están a la derecha de los demás caracteres cuando se usan con `LIKE`.

Recupera empleados/as en Finanzas o Ventas

Se realizo una actualización de seguridad diferente en los equipos de los empleados de los departamentos de Ventas y Finanzas. Utilice filtros en SQL para crear una consulta que identifique a todos los empleados de los departamentos de Ventas o Finanzas.

La siguiente imagen muestra mi consulta y un fragmento del resultado:

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Finance' OR department = 'Sales';
+-------------+-------------+----------+------------+-------------+
| employee_id | device_id   | username | department | office      |
+-------------+-------------+----------+------------+-------------+
|        1003 | d394e816f943 | sgilmore | Finance    | South-153   |
|        1007 | h174i497j413 | wjaffrey | Finance    | North-406   |
|        1008 | i858j583k571 | abernard | Finance    | South-170   |
```

La consulta empieza seleccionando todas las columnas de la tabla `employees`, por último, una cláusula `WHERE department = 'Finance' OR department = 'Sales',` la primera condición filtra por empleados en el departamento de Marketing y la segunda después del operador lógico `OR` filtra por empleados en el en el departamento de ventas.

Recupera a todos/as los/las empleados/as que no trabajan en TI

Mi equipo necesito hacer una actualización más en los equipos de los empleados. Los empleados del departamento de Tecnología de la Información ya tenían esta actualización, pero los/ de todos los demás departamentos la necesitan. Utilice filtros en SQL para crear una consulta que identifique a todos/as los/las empleados/as que no pertenecen al departamento de TI.

La siguiente imagen muestra mi consulta y un fragmento del resultado:

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE NOT department = 'Information Technology';
+-------------+-------------+----------+-----------------+-------------+
| employee_id | device_id   | username | department      | office      |
+-------------+-------------+----------+-----------------+-------------+
|        1000 | a320b137c219 | elarson  | Marketing       | East-170    |
|        1001 | b239c825d303 | bmoreno  | Marketing       | Central-276 |
|        1002 | c116d593e558 | tshah    | Human Resources | North-434   |
```

La consulta empieza seleccionando todas las columnas de la tabla `employees`, por último, una cláusula `WHERE NOT department = 'Information Technology',` filtra por empleados/as que no trabajan en este departamento, con la ayuda del operador `NOT.`

Resumen

Se aplicaron filtros a consultas SQL para obtener información específica sobre los intentos de inicio de sesión y los equipos de los empleados. Se utlizaron dos tablas distintas, `log_in_attempts` para los averiguar los intentos de inicio de sesión y `employees` para saber información sobre los empleados. Usé los operadores `AND`, `OR` y `NOT` para filtrar la información específica que necesitaba para cada tarea, se utilizó `LIKE` y el comodín de signo de porcentaje (`%`) para filtrar por patrones de caracteres.