Informe. Seguridad

Descripción del proyecto

Mi organización está trabajando para hacer que el sistema sea más seguro. Mi trabajo es garantizar que el sistema sea seguro, investigar todos los posibles problemas de seguridad y actualizar las computadoras de los empleados según sea necesario. Los siguientes pasos proporcionan ejemplos de cómo utilicé SQL con filtros para realizar tareas relacionadas con la seguridad.

Recuperar intentos fallidos de inicio de sesión fuera de horario

Hubo un posible incidente de seguridad que ocurrió fuera del horario comercial (después de las 18:00). Todos los intentos de inicio de sesión fuera del horario laboral que fallaron deben ser investigados.

El siguiente código demuestra cómo creé una consulta SQL para filtrar los intentos fallidos de inicio de sesión que ocurrieron fuera del horario comercial.

```
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 primera parte de la captura de pantalla es mi consulta y la segunda parte es una parte del resultado. Esta consulta filtra los intentos fallidos de inicio de sesión que ocurrieron después de las 18:00. Primero, comencé seleccionando todos los datos del `intentos de inicio de sesión` mesa. Luego, usé un `DÓNDE` cláusula con una `Y` operador para filtrar mis resultados para generar solo los intentos de inicio de sesión que ocurrieron después de las 18:00 y no tuvieron éxito. La primera condición es `hora_inicio de sesión > '18:00'`, que filtra los intentos de inicio de sesión que se produjeron después de las 18:00. La segunda condición es `éxito = FALSO`, que filtra los intentos fallidos de inicio de sesión.

Recuperar intentos de inicio de sesión en fechas específicas

Se produjo un evento sospechoso el 09/05/2022. Cualquier actividad de inicio de sesión que haya ocurrido el 9 de mayo de 2022 o el día anterior debe investigarse.

El siguiente código demuestra cómo creé una consulta SQL para filtrar los intentos de inicio de sesión que ocurrieron en fechas específicas.

```
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 primera parte de la captura de pantalla es mi consulta y la segunda parte es una parte del resultado. Esta consulta devuelve todos los intentos de inicio de sesión que se produjeron el 9 de mayo de 2022 o el 8 de mayo de 2022. Primero, comencé seleccionando todos los datos del `intentos de inicio de sesión` mesa. Luego, usé un `DÓNDE` cláusula con una `O` operador para filtrar mis resultados para generar solo los intentos de inicio de sesión que ocurrieron el 9 de mayo de 2022 o el 08 de mayo de 2022. La primera condición es `login_date = '2022-05-09'`, que filtra los inicios de sesión el 2022-05-09. La segunda condición es `login_date = '2022-05-08'`, que filtra los inicios de sesión el 8 de mayo de 2022.

Recuperar intentos de inicio de sesión fuera de México

Después de investigar los datos de la organización sobre los intentos de inicio de sesión, creo que hay un problema con los intentos de inicio de sesión que ocurrieron fuera de México. Estos intentos de inicio de sesión deben investigarse.

El siguiente código demuestra cómo creé una consulta SQL para filtrar los intentos de inicio de sesión que ocurrieron fuera de México.

```
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 primera parte de la captura de pantalla es mi consulta y la segunda parte es una parte del resultado. Esta consulta devuelve todos los intentos de inicio de sesión que ocurrieron en países distintos de México. Primero, comencé seleccionando todos los datos del `intentos de inicio de sesión` mesa. Luego, usé un `DÓNDE` cláusula con `NO` para filtrar por países distintos a México. yo usé `COMO` con `MEX%` como el patrón a coincidir porque el conjunto de datos representa a México como `MEX` y `MÉXICO`. El signo de porcentaje (`%`) representa cualquier número de caracteres no especificados cuando se usa con `COMO`.

Recuperar empleados en Marketing

Mi equipo quiere actualizar las computadoras de ciertos empleados del departamento de Marketing. Para hacer esto, tengo que obtener información sobre qué máquinas de los empleados actualizar.

El siguiente código demuestra cómo creé una consulta SQL para filtrar las máquinas de los empleados del departamento de Marketing en el edificio Este.

```
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 primera parte de la captura de pantalla es mi consulta y la segunda parte es una parte del resultado. Esta consulta devuelve todos los empleados del departamento de Marketing del edificio Este. Primero, comencé seleccionando todos los datos del `empleados` mesa. Luego, usé un `DÓNDE` cláusula con `Y` para filtrar por empleados que trabajan en el departamento de Marketing y en el edificio Este. yo usé `COMO` con `Este%` como el patrón a coincidir porque los datos en el `oficina` La columna representa el edificio Este con el número de oficina específico. La primera condición es la `departamento = 'Marketing'` porción, que filtra por empleados en el departamento de Marketing. La segunda condición es la `oficina COMO 'Este%'` porción, que filtra para los empleados en el edificio Este.

Recuperar empleados en Finanzas o Ventas

También es necesario actualizar las máquinas de los empleados de los departamentos de finanzas y ventas. Dado que se necesita una actualización de seguridad diferente, solo tengo que obtener información sobre los empleados de estos dos departamentos.

El siguiente código demuestra cómo creé una consulta SQL para filtrar las máquinas de los empleados de los departamentos de Finanzas o Ventas.

```
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 primera parte de la captura de pantalla es mi consulta y la segunda parte es una parte del resultado. Esta consulta devuelve todos los empleados de los departamentos de Finanzas y Ventas. Primero, comencé seleccionando todos los datos del `empleados` mesa. Luego, usé un `DÓNDE` cláusula con `O` para filtrar por empleados que están en los departamentos de Finanzas y Ventas. utilicé el `O` operador en lugar de `Y` porque quiero a todos los empleados que están en cualquiera de los departamentos. La primera condición es `departamento = 'Finanzas'`, que filtra por empleados del departamento de Finanzas. La segunda condición es `departamento = 'Ventas'`, que filtra por empleados del departamento de Ventas.

Recuperar a todos los empleados que no están en TI

Mi equipo necesita realizar una actualización de seguridad más para los empleados que no están en el departamento de Tecnología de la Información. Para realizar la actualización, primero tengo que obtener información sobre estos empleados.

A continuación se muestra cómo creé una consulta SQL para filtrar las máquinas de los empleados que no están en el departamento de Tecnología de la Información.

```
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 primera parte de la captura de pantalla es mi consulta y la segunda parte es una parte del resultado. La consulta devuelve todos los empleados que no están en el departamento de Tecnología de la Información. Primero, comencé seleccionando todos los datos del `empleados` mesa. Luego, usé un `DÓNDE` cláusula con `NO` para filtrar por empleados que no están en este departamento.

Resumen

Apliqué filtros a consultas SQL para obtener información específica sobre intentos de inicio de sesión y máquinas de empleados. Usé dos tablas diferentes, `intentos de inicio de sesión` y `empleados`. utilicé el `Y`, `O`, y `NO` operadores para filtrar la información específica necesaria para cada tarea. yo también usé `COMO` y el signo de porcentaje (`%`) comodín para filtrar patrones.