Portfolio Ciberseguridad. SQL & Filtros

Usted es un profesional de seguridad en una gran organización. Parte de su trabajo es investigar problemas de seguridad para ayudar a mantener el sistema seguro. Recientemente descubrió algunos problemas potenciales de seguridad que involucran intentos de inicio de sesión y máquinas de empleados.

Su tarea es examinar los datos de la organización en sus tablas employees y log_in_attempts. Deberá utilizar filtros SQL para recuperar registros de diferentes conjuntos de datos e investigar los posibles problemas de seguridad.

Table formats

This document describes how the tables used for this portfolio activity are organized. The `organization` database contains the following two tables:

- `log_in_attempts`
- `employees`

log_in_attempts

The `log_in_attempts` table has the following columns:

- `event_id`: The identification number assigned to each login event
- `username`: The username of the employee
- `login_date`: The date the login attempt was recorded
- `login_time`: The time the login attempt was recorded
- `country`: The country where the login attempt occurred
- `ip_address`: The IP address of that employee's machine
- `success`: The success of the login attempt; `FALSE` indicates a failed attempt

In the MariaDB shell, these columns are returned as:

```
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
```

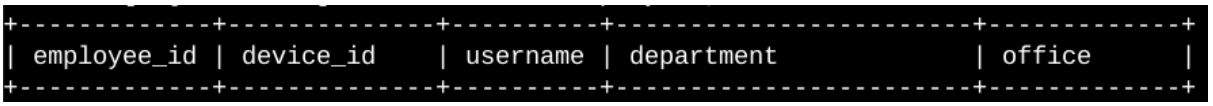
employees

The `employees` table has the following columns:

- `employee_id`: The identification number assigned to each employee
- `device_id`: The identification number assigned to each device used by the employee
- `username`: The username of the employee
- `department`: The department the employee is in

- `office`: The office the employee is located in

In the MariaDB shell, these columns are returned as:



```
+-------------+-------------+----------+-----------------------+-------------+
| employee_id | device_id    | username | department            | office      |
+-------------+-------------+----------+-----------------------+-------------+
```

- **Recuperar después de horas de intentos fallidos dde inicio de sesión**

Recientemente ha descubierto un posible incidente de seguridad ocurrido fuera del horario laboral. Para investigarlo, necesita consultar la tabla log_in_attempts y revisar 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 hora del intento de inicio de sesión se encuentra en la columna login_time. La columna success contiene un valor de 0 cuando un intento de inicio de sesión falló; puede utilizar un valor de 0 o FALSE en su consulta para identificar los intentos de inicio de sesión fallidos)

Describa su consulta y cómo funciona en la sección Recuperar tras horas de intentos de inicio de sesión fallidos de la plantilla Aplicar filtros a consultas SQL.

- **Recuperar los intentos de inicio de sesión en fechas concretas**

Un evento sospechoso ocurrió el 2022-05-09. Para investigar este evento, desea revisar todos los intentos de inicio de sesión que se produjeron ese día y el día anterior. Utilice filtros en SQL para crear una consulta que identifique todos los intentos de inicio de sesión que se produjeron el 2022-05-09 o el 2022-05-08. (La fecha del intento de inicio de sesión se encuentra en la columna login_date). (La fecha del intento de inicio de sesión se encuentra en la columna login_date)

Describa su consulta y cómo funciona en la sección Recuperar intentos de inicio de sesión en fechas específicas de la plantilla Aplicar filtros a consultas SQL.

- **Recuperar intentos de inicio de sesión fuera de Mexico**

Ha habido actividad sospechosa con intentos de inicio de sesión, pero el equipo ha determinado que esta actividad no se originó en México. Ahora, necesita investigar los intentos de inicio de sesión que ocurrieron fuera de México. Utilice filtros en SQL para crear una consulta que identifique todos los intentos de inicio de sesión que se produjeron fuera de México.Describa su consulta y cómo funciona en la sección Recuperar intentos de inicio de sesión en fechas específicas de la plantilla Aplicar filtros a consultas SQL.

- **Recuperar empleados en Marketing**

Su equipo desea realizar actualizaciones de seguridad en máquinas específicas de empleados en el departamento de Marketing. Usted es responsable de obtener información sobre estos equipos de empleados y necesitará consultar la tabla de empleados. Utilice filtros en SQL para crear una consulta que identifique a todos los empleados del departamento de Marketing de todas las oficinas del edificio Este.

(El departamento del empleado se encuentra en la columna departamento, que contiene valores que incluyen Marketing. La oficina se encuentra en la columna oficina. Algunos ejemplos de valores en esta columna son Este-170, Este-320 y Norte-434. Tendrá que utilizar la palabra clave LIKE con % para filtrar el edificio Este)

Describa su consulta y cómo funciona en la sección Recuperar empleados en Marketing de la plantilla Aplicar filtros a consultas SQL.

- **Recuperar empleados en Finanzas o Ventas**

Su equipo necesita ahora realizar una actualización de seguridad diferente en las máquinas para 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. (El departamento del empleado se encuentra en la columna departamento, que contiene valores que incluyen Ventas y Finanzas)

Describa su consulta y cómo funciona en la sección Recuperar empleados en Finanzas o Ventas de la plantilla Aplicar filtros a consultas SQL.

- **Recuperar a todos los empleados que no estén en IT**

Su equipo necesita realizar una actualización más en las máquinas de los empleados. Los empleados que pertenecen al departamento de tecnología de la información ya han recibido esta actualización, pero los empleados de todos los demás departamentos la necesitan. Utilice filtros en SQL para crear una consulta que identifique a todos los empleados que no pertenezcan al departamento de informática. (El departamento del empleado se encuentra en la columna departamento, que contiene valores que incluyen Tecnología de la información)

Describa su consulta y cómo funciona en la sección Recuperar todos los empleados que no pertenecen a TI de la plantilla Aplicar filtros a consultas SQL.

- **Finalizar documento**

Para finalizar el documento y dejar claro su propósito a los posibles empleadores, asegúrate de completar las secciones Descripción del proyecto y Resumen de la plantilla Aplicar filtros a consultas SQL.

En la sección Descripción del proyecto, ofrece una visión general del escenario y de lo que consigues mediante SQL. Escribe de dos a cuatro frases.

En la sección Resumen, proporcione un breve resumen de las tareas anteriores y conéctelas con el escenario. Escribe aproximadamente de dos a cuatro frases.