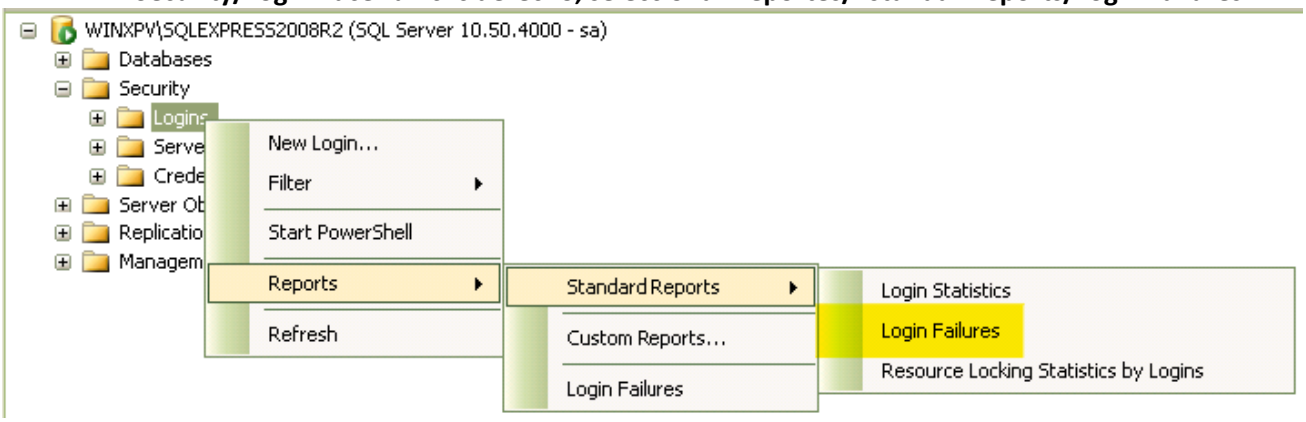
¿Cómo detectar un ataque a tu base de datos MS SQL Server?

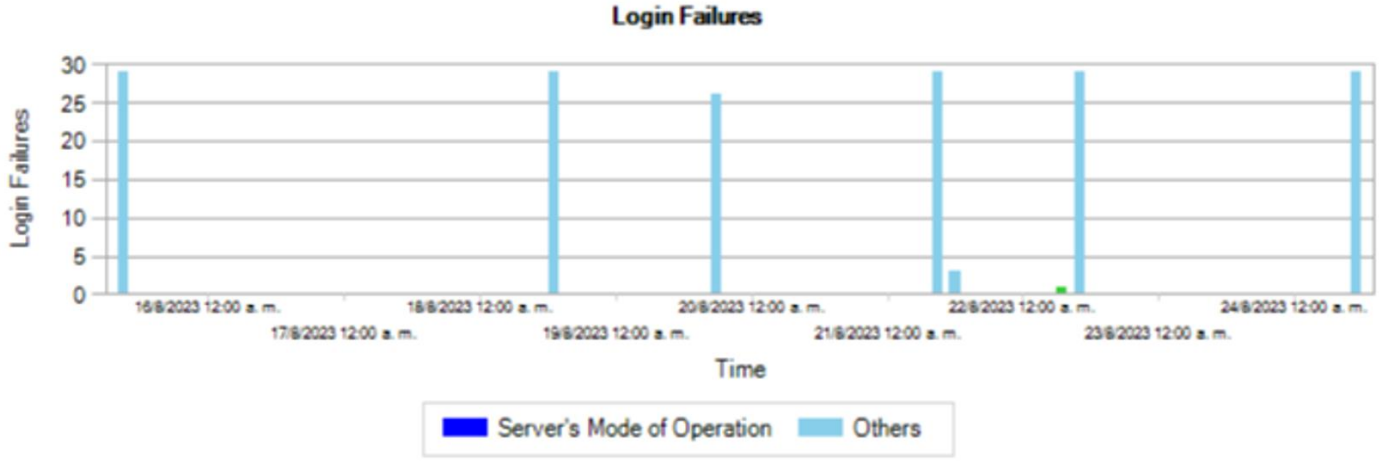
Pueden existir muchas formas de atacar tu SQL Server y distintos motivos para hacerlo. Por motivos varios es posible que necesiten estar autenticados, por lo que se debe vigilar las fallas en la autenticación a tu SQL Server. A continuación, algunas recomendaciones para hacerlo.

#1. Revisar fallas de autenticación con los reportes que vienen con la interfaz gráfica de "MS SQL Server":

1.1. En Security/Login hacer un clic derecho, seleccionar Reportes/Estándar Reports/Login Failures.



This report analyzes data captured in the Event Log and provides an historical summary of login failures on the Instance.



Login Failures by Users

Login failure details categorized according to users.

Login Failures by Reason of Failure

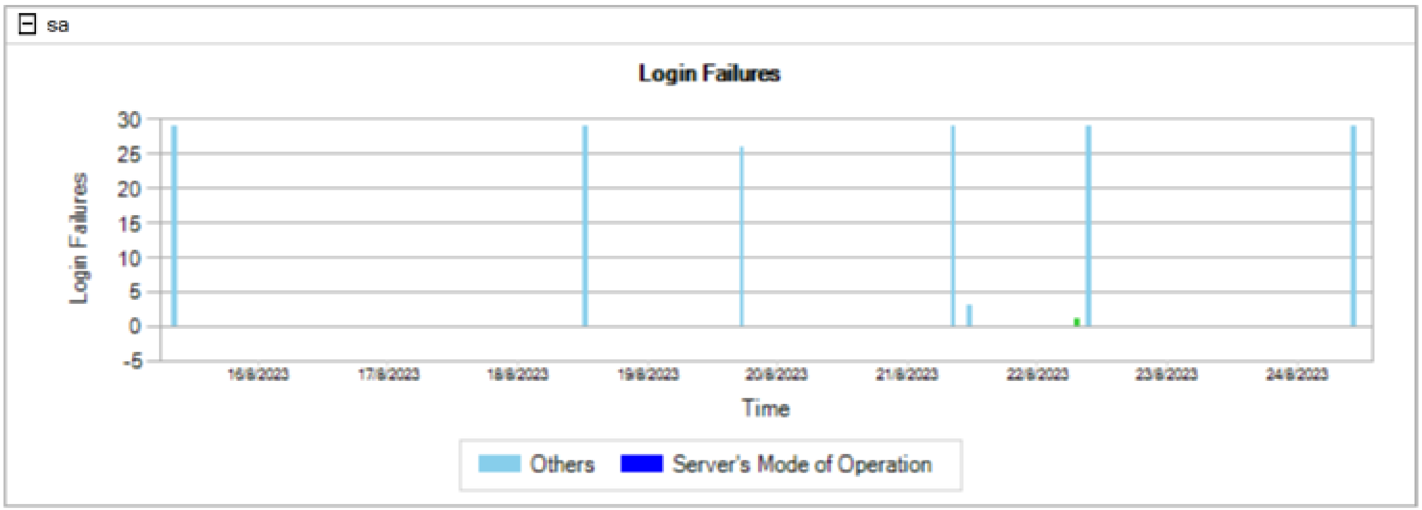
Login failure details categorized according to failure type/reason.

1.2. Buscando detalles "Login Failures by Users"

Se puede ver debajo que el usuario de SQL con fallas en autenticación es el "sa". Esto puede ser un ataque porque generalmente se utilizan cuentas de SQL distintas para acceder a las aplicaciones, no el "sa".

Login Failures by Users

Login failure details categorized according to users.



1.3. Buscando detalles "Login Failures by Reason of Failure"

Se puede apreciar que desde el equipo "DEVELOPERS-PC" han estado tratando de acceder al SQL Server del equipo de prueba mediante el Visual Studio.NET.

Login Failures by Reason of Failure

Login failure details categorized according to failure type/reason.

Login Failure Category

Others

Error No.	Login Name	Host Name	Application Name	Time	Error Message	NT User Name	NT Domain Name
18456	sa	DEVELOPERS-PC	Microsoft® Visual Studio®	2023-08-24 11:25:17	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]		
18456	sa	DEVELOPERS-PC	Microsoft® Visual Studio®	2023-08-24 11:25:17	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]		
18456	sa	DEVELOPERS-PC	Microsoft® Visual Studio®	2023-08-24 11:25:17	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]		
18456	sa	DEVELOPERS-PC	Microsoft® Visual Studio®	2023-08-24 11:25:17	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]		

#2. Revisar las fallas de autenticación mediante querys de SQL Server:

2.1. Query para leer el log de errores.

Se puede apreciar que esta consulta muestra la fecha-hora y la descripción de los errores filtrados por “login failed”.

```
EXEC sp_readerrorlog 0, 1, 'login failed'
```

	LogDate	ProcessInfo	Text
1	2023-08-22 10:10:27.230	Logon	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]
2	2023-08-22 10:10:27.270	Logon	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]
3	2023-08-22 10:10:27.310	Logon	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]
4	2023-08-22 10:10:27.340	Logon	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]
5	2023-08-22 10:10:27.440	Logon	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]
6	2023-08-22 10:10:27.470	Logon	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]
7	2023-08-22 10:10:27.500	Logon	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]
8	2023-08-22 10:10:27.540	Logon	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]

2.2. Query para leer el Trace de SQL:

En cambio aquí, además de la fecha-hora y la descripción, muestra el equipo o IP desde donde se realizó el intento de autenticación y la aplicación desde la que se realizó el intento fallido.

```
select te.name as [event],
       e.applicationname,
          e.textdata,
          e.starttime,
          e.databasename as db,
          e.loginname as [login],
          e.hostname as host
from fn_trace_gettable((select [path] from sys.traces where is_default = 1 and is_shutdown=0),
default) e
inner join sys.trace_events te on e.eventclass=te.trace_event_id
where e.eventclass = 20
order by e.starttime
```

	event	applicationname	textdata	starttime	db	login	host
1	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.237	master	sa	DEVELOPERS-PC
2	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.280	master	sa	DEVELOPERS-PC
3	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.310	master	sa	DEVELOPERS-PC
4	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.343	master	sa	DEVELOPERS-PC
5	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.443	master	sa	DEVELOPERS-PC
6	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.477	master	sa	DEVELOPERS-PC
7	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.507	master	sa	DEVELOPERS-PC
8	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.547	master	sa	DEVELOPERS-PC
9	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.577	master	sa	DEVELOPERS-PC
10	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.620	master	sa	DEVELOPERS-PC
11	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.670	master	sa	DEVELOPERS-PC
12	Audit Login Failed	Microsoft® Visual Studio®	Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 10.0.0.158]	2023-08-22 10:10:27.703	master	sa	DEVELOPERS-PC