SCRIPT #14 · DATABASE (SQL SERVER / MYSQL)

Login SQL Server potenzialmente a rischio

Verifica se l'account sa e attivo e quali login hanno la password scaduta.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Modulo SqlServer

Cosa fa questo script

Lo script controlla se l'account amministrativo predefinito 'sa' risulta attivo, e verifica lo stato di scadenza password di tutti i login SQL configurati.

Come si usa

Esegui lo script indicando l'istanza da controllare.

```
.\Report-LoginRischiosi.ps1 -ServerSQL "SQL01"
```

In quale contesto usarlo

L'account 'sa' attivo, specialmente se con password debole o mai cambiata, e uno dei bersagli piu comuni negli attacchi automatizzati contro istanze SQL Server esposte. Disabilitarlo (usando un account amministrativo nominale al suo posto) e una delle misure di hardening piu semplici e piu spesso trascurate.

Codice completo

Il codice è lo stesso del file Report-LoginRischiosi.ps1: per usarlo scarica il file dalla pagina invece di copiarlo da questo PDF.

```
<#
.SYNOPSIS
    Verifica se l'account 'sa' è attivo e quali login SQL hanno la password scaduta.
#>
param(
    [string]$ServerSQL = "localhost",
    [string]$PercorsoCSV = "C:\Report\LoginRischiosi.csv"
)
Import-Module SqlServer -ErrorAction SilentlyContinue

$query = @"
SELECT name AS Login, is_disabled AS Disabilitato,
       CASE WHEN name = 'sa' AND is_disabled = 0 THEN 1 ELSE 0 END AS SAAttivo,
       LOGINPROPERTY(name, 'IsExpired') AS PasswordScaduta
FROM sys.sql_logins
"@

$risultati = Invoke-Sqlcmd -ServerInstance $ServerSQL -Query $query
$risultati | Export-Csv -Path $PercorsoCSV -NoTypeInformation -Encoding UTF8 -Delimiter ";"
$saAttivo = ($risultati | Where-Object {$_.SAAttivo -eq 1}).Count
Write-Host `
    "Controllati $($risultati.Count) login SQL. Account 'sa' attivo: $(if($saAttivo -gt 0){'SI - da verificare'}else{'NO'})" `
    -ForegroundColor $(if($saAttivo -gt 0){"Red"}else{"Green"})
```