SCRIPT #16 · WINDOWS SERVER

Modifiche recenti alla Local Security Policy

Confronta la Local Security Policy corrente con una baseline salvata, evidenziando le differenze.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Permessi amministrativi, secedit (nativo)

Cosa fa questo script

Lo script esporta la configurazione corrente della Local Security Policy tramite secedit e la confronta con un file di baseline salvato in precedenza, riportando riga per riga le impostazioni che risultano cambiate rispetto al riferimento.

Come si usa

La prima volta, esegui lo script con -SalvaBaseline per creare il file di riferimento. Nelle esecuzioni successive, lo script confronta automaticamente lo stato attuale con quella baseline.

```
# prima esecuzione, crea la baseline:
.\Audit-ModificheLocalSecurityPolicy.ps1 -SalvaBaseline
# esecuzioni successive, confronta:
.\Audit-ModificheLocalSecurityPolicy.ps1
```

In quale contesto usarlo

Windows non mantiene uno storico nativo delle modifiche alla Local Security Policy: questo approccio a baseline e confronto e il modo piu semplice per accorgersi se qualcuno ha modificato impostazioni di sicurezza critiche (policy password, diritti utente, opzioni di sicurezza) senza che sia stato comunicato o documentato.

Codice completo

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

```
<#
.SYNOPSIS
    Confronta la Local Security Policy corrente con una baseline salvata.
#>
param(
    [switch]$SalvaBaseline,
    [string]$PercorsoBaseline = "C:\Report\LSP_Baseline.inf",
    [string]$PercorsoCorrente = "C:\Report\LSP_Corrente.inf"
)

secedit /export /cfg $PercorsoCorrente | Out-Null
```

```
if ($SalvaBaseline) {
    Copy-Item -Path $PercorsoCorrente -Destination $PercorsoBaseline -Force
    Write-Host "Baseline salvata in: $PercorsoBaseline" -ForegroundColor Green
    return
}

if (-not (Test-Path $PercorsoBaseline)) {
    Write-Host "Nessuna baseline trovata. Esegui prima lo script con -SalvaBaseline." -ForegroundColor Red
    return
}

$differenze = Compare-Object -ReferenceObject (Get-Content $PercorsoBaseline) -DifferenceObject (Get-Content $PercorsoCorrente)

if ($differenze) {
    Write-Host "[ATTENZIONE] Rilevate differenze rispetto alla baseline:" -ForegroundColor Red
    $differenze | ForEach-Object {
        $simbolo = if ($_.SideIndicator -eq "=>") {"+ (nuovo)"} else {"- (rimosso/cambiato)"}
        Write-Host "  $simbolo : $($_.InputObject)" -ForegroundColor Yellow
    }
} else {
    Write-Host "Nessuna differenza rispetto alla baseline." -ForegroundColor Green
}
```