SCRIPT #13 · ACTIVE DIRECTORY

Delega Kerberos non vincolata

Individua account con delega Kerberos non vincolata, configurazione ad alto rischio.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Modulo ActiveDirectory

Cosa fa questo script

Lo script cerca tra utenti e computer del dominio quelli con l'attributo TrustedForDelegation impostato su vero, una configurazione che permette a quell'oggetto di impersonare altri utenti verso qualsiasi servizio.

Come si usa

Esegui semplicemente lo script. Un risultato con zero righe, evidenziato in verde in console, e il risultato atteso e desiderabile nella maggior parte degli ambienti moderni.

```
.\Report-DelegaNonVincolata.ps1
```

In quale contesto usarlo

Script di audit di sicurezza da eseguire periodicamente, particolarmente rilevante alla luce del modello a livelli (Tiering Model): ogni oggetto con questa configurazione, se non giustificato da una reale necessita applicativa documentata, va rivisto e, quando possibile, sostituito con delega vincolata o basata su risorsa.

Codice completo

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

```
<#
.SYNOPSIS
    Individua account con delega Kerberos non vincolata, configurazione ad alto rischio.
#>
param(
    [string]$PercorsoCSV = "C:\Report\DelegaNonVincolata.csv"
)

Import-Module ActiveDirectory

$utenti = Get-ADUser -Filter {TrustedForDelegation -eq $true} -Properties TrustedForDelegation, DisplayName
$computer = Get-ADComputer -Filter {TrustedForDelegation -eq $true} -Properties TrustedForDelegation

$risultati = @()
$risultati += $utenti | Select-Object @{N="Nome";E={$_.DisplayName}}, @{N="Tipo";E={"Utente"}}, SamAccountName
$risultati += $computer | Select-Object @{N="Nome";E={$_.Name}}, @{N="Tipo";E={"Computer"}}, `
    @{N="SamAccountName";E={$_.SamAccountName}}

$risultati | Export-Csv -Path $PercorsoCSV -NoTypeInformation -Encoding UTF8 -Delimiter ";"
Write-Host "Trovati $($risultati.Count) oggetti con delega non vincolata." -ForegroundColor $(if($risultati.Count `
    -gt 0){"Red"}else{"Green"})
```