SCRIPT #02 · CYBER SECURITY

Utenti locali con privilegi amministrativi

Interroga piu computer e riporta i membri del gruppo Administrators locale su ciascuno.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Accesso WinRM/PowerShell Remoting sui computer target

Cosa fa questo script

Lo script si collega in remoto a un elenco di computer (da file di testo) e recupera i membri del gruppo Administrators locale su ciascuno, producendo un report che permette di individuare rapidamente account con privilegi elevati su piu macchine.

Come si usa

Prepara un file di testo con un nome computer per riga, poi esegui lo script indicandone il percorso.

```
.\Report-AdminLocaliMultipli.ps1 -ListaComputer "C:\Dati\computer.txt"
```

In quale contesto usarlo

Fondamentale per individuare account (soprattutto personali) che risultano amministratori locali su troppe macchine, una configurazione che, se un singolo account viene compromesso, amplifica enormemente il raggio d'azione di un attaccante tramite movimento laterale.

Codice completo

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

```
<#
.SYNOPSIS
    Interroga più computer e riporta i membri del gruppo Administrators locale su ciascuno.
#>
param(
    [Parameter(Mandatory=$true)]
    [string]$ListaComputer,
    [string]$PercorsoCSV = "C:\Report\AdminLocali.csv"
)

$computer = Get-Content -Path $ListaComputer

$risultati = foreach ($pc in $computer) {
    try {
        $membri = Invoke-Command -ComputerName $pc -ScriptBlock {
            Get-LocalGroupMember -Group "Administrators" | Select-Object Name, ObjectClass
        } -ErrorAction Stop
```

```
        foreach ($m in $membri) {
            [PSCustomObject]@{
                Computer = $pc
                Membro   = $m.Name
                Tipo     = $m.ObjectClass
                Stato    = "OK"
            }
        }
    }
    catch {
        [PSCustomObject]@{
            Computer = $pc
            Membro   = "N/D"
            Tipo     = "N/D"
            Stato    = "NON RAGGIUNGIBILE: $_"
        }
    }
}

$risultati | Export-Csv -Path $PercorsoCSV -NoTypeInformation -Encoding UTF8 -Delimiter ";"
Write-Host "Report generato per $($computer.Count) computer in: $PercorsoCSV" -ForegroundColor Green
```