SCRIPT #11 · CYBER SECURITY

Tentativi di accesso RDP falliti

Analizza il log eventi per tentativi di accesso RDP falliti, un vettore di attacco molto comune.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Permessi di lettura sul log di sicurezza

Cosa fa questo script

Lo script filtra gli eventi di logon fallito (Event ID 4625) limitandosi a quelli con tipo di logon 10, specifico per le connessioni Remote Desktop, raggruppando i risultati per indirizzo IP di origine per evidenziare pattern di attacco.

Come si usa

Esegui specificando quante ore indietro analizzare.

```
.\Report-RDPFalliti.ps1 -OreIndietro 24
```

In quale contesto usarlo

RDP esposto direttamente su Internet e uno dei vettori di attacco piu sfruttati per compromissioni e ransomware. Questo script e utile sia come controllo diagnostico su server con RDP esposto (situazione comunque da evitare quando possibile, preferendo VPN o Zero Trust Network Access) sia come verifica generale su server interni.

Codice completo

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

```
<#
.SYNOPSIS
    Analizza il log eventi per tentativi di accesso RDP falliti (logon type 10).
#>
param(
    [int]$OreIndietro = 24,
    [string]$PercorsoCSV = "C:\Report\RDPFalliti.csv"
)

$dataLimite = (Get-Date).AddHours(-$OreIndietro)

$eventi = Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4625; StartTime=$dataLimite} -ErrorAction SilentlyContinue

$risultati = foreach ($e in $eventi) {
    $xml = [xml]$e.ToXml()
    $dati = $xml.Event.EventData.Data
    $logonType = ($dati | Where-Object {$_.Name -eq 'LogonType'}).'#text'

    if ($logonType -eq '10') {
        [PSCustomObject]@{
            Orario    = $e.TimeCreated
            Account   = ($dati | Where-Object {$_.Name -eq 'TargetUserName'}).'#text'
```

```
            IPOrigine = ($dati | Where-Object {$_.Name -eq 'IpAddress'}).'#text'
        }
    }
}

$riepilogo = $risultati | Group-Object IPOrigine | Sort-Object Count -Descending |
    Select-Object @{N="IPOrigine";E={$_.Name}}, Count

$riepilogo | Export-Csv -Path $PercorsoCSV -NoTypeInformation -Encoding UTF8 -Delimiter ";"
Write-Host `
    "Trovati $($risultati.Count) tentativi RDP falliti da $($riepilogo.Count) IP diversi nelle ultime $OreIndietro ore." `
    -ForegroundColor $(if($risultati.Count -gt 0){"Yellow"}else{"Green"})
```