SCRIPT #03 · CYBER SECURITY

Scansione porte aperte su un range di IP

Testa un elenco di porte comuni su un range di indirizzi IP, riportando quelle raggiungibili.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Connettivita di rete verso il range target

Cosa fa questo script

Lo script itera su un range di indirizzi IP e, per ciascuno, testa la raggiungibilita di un elenco di porte TCP comuni, producendo un report di quali combinazioni host/porta risultano aperte.

Come si usa

Specifica l'IP iniziale, l'IP finale e, opzionalmente, l'elenco di porte da testare (di default le piu comuni).

```
.\Scan-PorteAperte.ps1 -IPIniziale "192.168.1.1" -IPFinale "192.168.1.50"
```

In quale contesto usarlo

Utile per una prima mappatura di cosa e effettivamente esposto su una subnet, specialmente dopo l'introduzione di nuovi dispositivi in rete. Da usare solo su reti di propria competenza: una scansione di questo tipo su reti altrui puo violare policy di sicurezza o normative locali.

Codice completo

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

```
<#
.SYNOPSIS
    Testa un elenco di porte comuni su un range di indirizzi IP.
.NOTES
    Usare esclusivamente su reti di propria competenza.
#>
param(
    [Parameter(Mandatory=$true)]
    [string]$IPIniziale,
    [Parameter(Mandatory=$true)]
    [string]$IPFinale,
    [int[]]$Porte = @(21,22,23,25,80,443,445,3389,3306,1433),
    [string]$PercorsoCSV = "C:\Report\ScanPorte.csv"
)

function ConvertTo-UInt32 ([string]$ip) {
    $b = $ip.Split('.')
    return ([uint32]$b[0] -shl 24) + ([uint32]$b[1] -shl 16) + ([uint32]$b[2] -shl 8) + [uint32]$b[3]
}
function ConvertTo-IPString ([uint32]$num) {
    return "{0}.{1}.{2}.{3}" -f (($num -shr 24) -band 255), (($num -shr 16) -band 255), (($num -shr 8) -band 255), ($num `
        -band 255)
}

$start = ConvertTo-UInt32 $IPIniziale
$end = ConvertTo-UInt32 $IPFinale
```

```
$risultati = for ($i = $start; $i -le $end; $i++) {
    $ipCorrente = ConvertTo-IPString $i
    foreach ($porta in $Porte) {
        $test = Test-NetConnection -ComputerName $ipCorrente -Port $porta -WarningAction SilentlyContinue `
            -InformationLevel Quiet
        if ($test) {
            [PSCustomObject]@{ IP = $ipCorrente; Porta = $porta; Stato = "APERTA" }
        }
    }
}

$risultati | Export-Csv -Path $PercorsoCSV -NoTypeInformation -Encoding UTF8 -Delimiter ";"
Write-Host "Trovate $($risultati.Count) porte aperte nel range specificato." -ForegroundColor Yellow
```