

Enviar y ejecutar un comando (cmdlet) de PowerShell entre dos equipos (cliente-servidor) de forma simple y sencilla mediante el protocolo UDP

Nadie dice que esto sea seguro... Esto permite ejecutar comandos remotamente...

Servidor que recibe y ejecuta

[crayon-6a9d83e2997f2385611675/]

Cliente que envía el cmdlet

[crayon-6a9d83e2997f9786095732/]

Resultado

Sin titulo1.ps1* X

```
1 ## Server
2
3 $ip = New-Object System.Net.IPEndPoint ([IPAddress]::Any,0)
4 $udp = New-Object System.Net.Sockets.UdpClient 2020
5
6 [Text.Encoding]::ASCII.GetString($udp.Receive([ref]$ip)) | iex
7
8 $udp.Close()
```

PS C:\Users\juan> ## Server

```
$ip = New-Object System.Net.IPEndPoint ([IPAddress]::Any,0)
$udp = New-Object System.Net.Sockets.UdpClient 2020

[Text.Encoding]::ASCII.GetString($udp.Receive([ref]$ip)) | iex

$udp.Close()
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
140	8	1972	5220		4048	0	AdminService
396	23	11348	17344	1.09	6768	1	ApplicationFrame
233	15	3376	1012	0.22	12452	1	AsusTPCenter
142	10	1612	1644	0.56	8888	1	AsusTPHelper
374	15	2080	940	1.37	8088	1	AsusTPLoader

Lín. 8 Col. 13120 %

Sin titulo1.ps1* X

```
1 ## Cliente
2
3 ## Cambiar la dirección IP por la dirección IP pública de la red
4
5 $ip = New-Object System.Net.IPEndPoint ([IPAddress]"127.0.0.1",2020)
6 $udp = New-Object System.Net.Sockets.UdpClient
7
8 $mensaje = [Text.Encoding]::ASCII.GetBytes('ps')
9
10 $udp.Send($mensaje,$mensaje.Length,$ip) | Out-Null
11
12 $udp.Close()
```

PS C:\Users\juan> ## Cliente

```
## Cambiar la dirección IP por la dirección IP pública de la red

$ip = New-Object System.Net.IPEndPoint ([IPAddress]"127.0.0.1",2020)
$udp = New-Object System.Net.Sockets.UdpClient

$mensaje = [Text.Encoding]::ASCII.GetBytes('ps')

$udp.Send($mensaje,$mensaje.Length,$ip) | Out-Null

$udp.Close()

PS C:\Users\juan>
```

Lín. 12 Col. 8120 %