

Obtener los nombres de las funciones exportadas de un archivo DLL con DUMPBIN desde PowerShell (explicación paso a paso del script)

[crayon-6a9d580b8ffce854582935/]



Explicación paso a paso del script

Listar funciones exportadas de un archivo DLL con DUMPBIN desde PowerShell

[crayon-6a9d580b8ffd3245246910/]

```
Sin título1.ps1* X
1 # Información sobre Microsoft COFF Binary File Dumper DUMPBIN
2 # https://msdn.microsoft.com/es-es/library/c1h23y6c.aspx
3
4 cd "C:\Program Files (x86)\Microsoft Visual Studio\2017\Community\VC\Tools\MSVC\14.13.26128\bin\Hostx86\x86"
5
6 # Listar funciones exportadas de un archivo DLL con DUMPBIN desde PowerShell
7 $content = &.dumpbin.exe /exports C:\windows\System32\zipfldr.dll
8
```



```
Dump of file C:\windows\System32\zipfldr.dll
File type: DLL

Section contains the following exports for ZIPFLDR.dll
00000000 characteristics
790FB848 time date stamp
0.00 version
1 ordinal base
3 number of functions
3 number of names

ordinal hint RVA      name
2 0 00014230 dllCanInloadNow
3 1 00006A10 dllGetClassObject
1 2 0000E40 RouteTheCall

Summary
2000 .data
1000 .didat
2000 .pdata
C000 .rdata
1000 .reloc
1C000 .rsrc
34000 .text

PS C:\Program Files (x86)\Microsoft Visual Studio\2017\Community\VC\Tools\MSVC\14.13.26128\bin\Hostx86\x86>
```

Procesar la información para obtener únicamente las funciones. Quitar líneas sin contenido

[crayon-6a9d580b8ffd5982876884/]



Crear un string de toda la información para poder extraer el contenido de las funciones

[crayon-6a9d580b8ffd7548873454/]



Con el contenido de las funciones extraer el nombre de las funciones

[crayon-6a9d580b8ffd9886218120/]

```
Sin titulo1.ps1 X
1 # Con el contenido de las funciones extraer el nombre de las funciones
2 # Convertir un array a CSV con PowerShell
3 $data = $funciones.split(";").Replace(" ", "").Replace(" ", "").Replace(" ", "") | ConvertFrom-Csv
4 # Mostrar el nombre de las funciones
5 $data.name
6 |

PS C:\Program Files (x86)\Microsoft Visual Studio\2017\Community\VC\Tools\MSVC\14.13.26128\bin\Hostx86\x86> # Con el contenido de las funciones extraer el nombre de las funciones
# Convertir un array a CSV con PowerShell
# Convertir un array a CSV con PowerShell
$data = $funciones.split(";").Replace(" ", "").Replace(" ", "").Replace(" ", "") | ConvertFrom-Csv
# Mostrar el nombre de las funciones
$data.name

D:\CanInloadNow
D:\GetClassObject
RouteTheCall

PS C:\Program Files (x86)\Microsoft Visual Studio\2017\Community\VC\Tools\MSVC\14.13.26128\bin\Hostx86\x86>
```

Completado Lin. 6 Col. 1 100 %