14. Obtener el control de un proceso

Tuesday, November 17, 2020 4:37 PM

Para hacer un script que nos permite tener el control de un proceso de Windows necesitamos manejar la siguiente función de la WinAPI:

- OpenProcess

  Abre un objeto existente de proceso local.
  Parámetros de entrada:
  - dwDesiredAccess - Es el acceso al objeto de proceso.
  - bInheritHandle - Si su valor es True, procesos creados por este proceso van a heredar el handle, de otro forma, el proceso no heredará el handle.
  - dwProcessId - El identificador del proceso local que será abierto.

  Valor de retorno: Si la función se realiza correctamente, el valor devuelto es un identificador abierto para el proceso especificado. Si se produce un error en la función, el valor devuelto es NULL.

OpenProcHandle.py

OpenPro...

Sección	Código
1	`import ctypes`
2	`k_handle = ctypes.WinDLL("Kernel32.dll")`
3	`PROCESS_ALL_ACCESS = (0x000F0000 | 0x00100000 | 0xFFF)`

4	`dwDesiredAccess = PROCESS_ALL_ACCESS`
	`bInheritHandle = False`
	`dwProcessId = ctypes.c_ulong(int(input("Process ID: ")))`

5	`response = k_handle.OpenProcess(dwDesiredAccess, bInheritHandle, dwProcessId)`

6	`error = k_handle.GetLastError()`
	`if error != 0:`
	`  print("Handle Not Created!")`
	`  print("Error Code: {0}".format(error))`
	`  exit(1)`

7	`if response <= 0:`
	`  print("Handle Not Created!")`
	`elif response >= 1:`
	`  print("Handle Created!")`

Explicación

1. Importamos ctypes
2. Creamos un handle para el Kernel32.dll
3. Definimos una variable para especificar el acceso completo (acorde a los permisos del usuario con los que usemos este script).
4. Definimos los valores de los 3 parámetros de entrada de la función OpenProcess.
5. Ejecutamos la función OpenProcess que almacenará en la variable response el resultado de intentar obtener el handle.
6. Guardamos en la variable error el código del último error, en caso de que no sea 0, significa que hubo algún error. Informamos al usuario y terminamos el script.

7. Si la respuesta obtenida en la variable response es igual o menor que 0, significa que la función no fue exitosa. Si la respuesta el mayor o igual a 1, si funcionó y ese valor es el identificador del proceso.