

Volatility2 para novatos

Para poder usar Volatility2 en nuestro equipo necesitamos Python 2.XX, si se tiene la versión 3 pueden haber problemas a la hora de ejecutar comandos.

Primeros pasos

Cuando tenemos un dump de memoria lo primero que debemos hacer es identificar el sistema operativo ya que en función de sobre cual estemos haciendo el análisis forense es posible que necesitemos un perfil u otro. Para revisar la información del dump de memoria se usa el siguiente comando:

```
.\vol.exe -f <Ruta_del_dump_de_memoria> imageinfo
```

Un ejemplo real de la ejecución del comando sería el siguiente:

```
PS C:\Users\RUGGED\Documents\Práctica De Forense> .\vol.exe -f .\memory.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
      AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (C:\Users\RUGGED\Documents\Práctica De Forense\memory.raw)
      PAE type : No PAE
      DTB : 0x187000L
      KDBG : 0xf800027fd0a0L
      Number of Processors : 2
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0xfffff800027fed00L
      KPCR for CPU 1 : 0xfffff800009ea000L
      KUSER_SHARED_DATA : 0xfffff78000000000L
      Image date and time : 2024-03-21 09:42:22 UTC+0000
      Image local date and time : 2024-03-21 10:42:22 +0100
```

En este caso podemos ver que se recomiendan varios perfiles, por lo que seleccionaremos uno de ellos y procederemos en el futuro con este. En este caso se elige el perfil "Win7SP1x64"

From:
<https://www.knoppia.net/> - Knoppia

Permanent link:
https://www.knoppia.net/doku.php?id=master_cs:analisys_forense:volatility2&rev=1747256227

Last update: 2025/05/14 20:57

