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\Prßctica 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 : 0xfffff880009ea000L
             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”

Obtener el historial de comandos con volatility2

Para obtener el historial de comandos de un usuario se utiliza el siguiente comando poniendo la ubicación del dump de memoria y el perfil que seleccionamos en el paso anterior:

```
.\vol.exe -f <Ruta_del_dump_de_memoria> --profile=<Perfil_Seleccionado>
consoles
```

Siguiendo el ejemplo anterior, se usaría el comando de la siguiente manera:

```
PS C:\Users\RUGGED\Documents\Práctica De Forense> .\vol.exe -f .\memory.raw --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6
**************************************************
ConsoleProcess: conhost.exe Pid: 6676
Console: 0xff286200 CommandHistorySize: 50
HistoryBufferCount: 4 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\System32\cmd.exe
Title: C:\Windows\System32\cmd.exe
AttachedProcess: cmd.exe Pid: 5132 Handle: 0x64
----
CommandHistory: 0xbefe0 Application: 7z.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0xbee00 Application: ftp.exe Flags: Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
Cmd #0 at 0xb51b0: anonymous
Cmd #1 at 0xb3a40: ls
Cmd #2 at 0xa6500: get Estudiantes.xlsx
Cmd #3 at 0xb2510: get Examen.pdf
Cmd #4 at 0xb51d0: quit
----
CommandHistory: 0xbac20 Application: nmap.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0xb6540 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 3 LastAdded: 2 LastDisplayed: 2
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
Cmd #0 at 0xba730: "C:\Program Files (x86)\Nmap\nmap.exe" --unprivileged -sV -T5 -p21 --script="*ftp*" acme-university.pri
Cmd #1 at 0xa6540: ftp acme-university.pri
Cmd #2 at 0xbfcd0: "C:\Program Files\7-Zip\7z.exe" a archivos-robados.7z Estudiantes.xlsx Examen.pdf -p
----
Screen 0x93000 X:80 Y:300
Dump:
Microsoft Windows [Versi?n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

E:\>"C:\Program Files (x86)\Nmap\nmap.exe" --unprivileged -sV -T5 -p21 --script=
"*ftp*" acme-university.pri
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-21 10:19 Hora est?ndar romanc
e
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for acme-university.pri (172.20.20.86)
```