Volatility 3 Overview

Volatility 3 – The most widely used framework for extracting digital artifacts from volatile memory (RAM)

Typically, Volatilty 3 is designed to work with raw memory dump files, with extensions such as .mem,.dmp,.bin, raw. It can also be used on VM snapshots (.vmem,.vbox) and the Windows hibernation file (hiberfil.sys)

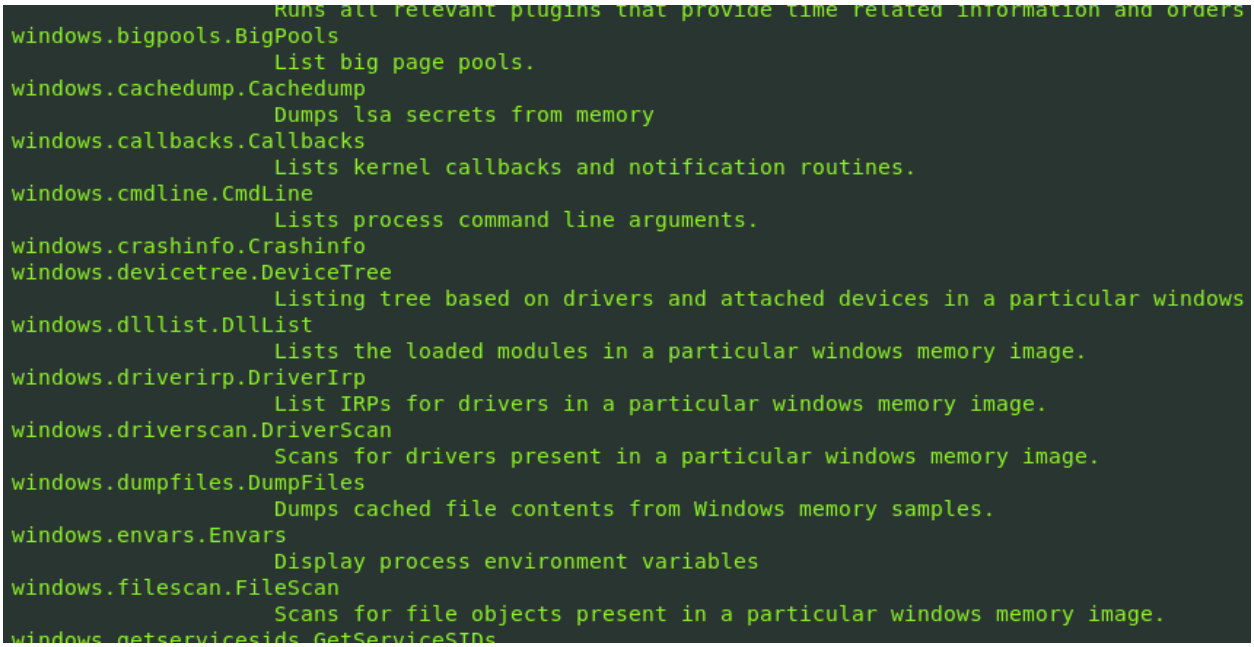
Example command:

```
raven@remnux:~/Desktop$ vol3 -f Dump_me.mem windows.pslist
```

Pass volatility a dump file with the -f flag and choose a plugin you want the use to analyze the mem dump.

NOTE: If you are using a version of volatility preceding Volatility 3 you will need an Operating System profile to be added to the command. Ex: --profile= Win10x64_19041
Luckily Volatility 3 skips this step, it uses symbol-based analysis and automated detection to recognize the OS and version without requiring manual specifications

Vol3 –h will list plugins available



Make sure operating system matches the OS of the machine the memory dump came from

Worth noting you don't need to call the last module of the plugin. Ex windows.dlllist will work, instead of windows.dlllist.DllList (what is shown in the picture above)

Vol3 github

https://github.com/volatilityfoundation/volatility3/tree/develop