Exercise 14

30/11/2021

Memory forensics

Memory forensics is forensic analysis of a computer's memory dump. Its primary application is investigation of advanced computer attacks which are stealthy enough to avoid leaving data on the computer's hard drive. Consequently, the memory (RAM) must be analysed for forensic information.

Visit https://en.wikipedia.org/wiki/Memory_forensics for information about the history of memory forensics.

Volatility is an open source memory forensics framework for incident response and malware analysis. It is written in Python and supports Microsoft Windows, Mac OS X, and Linux. See www.volatilityfoundation.org

Volatility supports investigations of a variety of memory images. It supports a variety of sample file formats and the ability to convert between these formats.

The Volatility software may be downloaded from here-

https://code.google.com/p/volatility/downloads/list

For performing analysis using Volatility we need to first set a profile to tell Volatility what operating system the dump came from, such as Windows XP, Vista, Linux flavours, etc.

Assume we have a memory dump with us and we do not know what operating system it belongs to, so we use the imageinfo plug-in to find this out.

For further info see

https://resources.infosecinstitute.com/memory-forensics-and-analysis-using-volatility/

RAM image name is hiberfil.sys.

Here we list are examples of usage of Volatility

vol.py imageinfo -f hiberfil.sys

vol.py pslist --profile=WinXPSP3x86 -f hiberfil.sys

vol.py pstree --profile=WinXPSP3x86 -f hiberfil.sys

vol.py -h to get the help.

Run different plugins and submit screen shots