Volatility3—Cheat sheet

Command example

Vol.py –f <path to image> command

”vol.py -f "I:\TEMP\DESKTOP-1090PRO-20200708-114621.dmp" windows.psscan.PsScan ”

Windows Commands

windows.cmdline.CmdLine

Lists process command line arguments.

windows.dlllist.DllList

Lists the loaded modules in a particular windows memory image.

windows.dumpfiles.DumpFiles

Dumps cached file contents from Windows memory samples.

windows.filescan.FileScan

Scans for file objects present in a particular windows memory image.

windows.netscan.NetScan

Scans for network objects present in a particular windows memory image.

windows.registry.hivelist.HiveList

Lists the registry hives present in a particular memory image.

windows.registry.hivescan.HiveScan

Scans for registry hives present in a particular windows memory image.

windows.strings.Strings

Reads output from the strings command and indicates which process(es) each string belongs to.

MAC commands

mac.bash.Bash

Recovers bash command history from memory.

mac.ifconfig.Ifconfig

Lists loaded kernel modules

mac.list_files.List_Files

Lists all open file descriptors for all processes.

mac.lsmod.Lsmod

Lists loaded kernel modules.

mac.lsof.Lsof

Lists all open file descriptors for all processes.

mac.netstat.Netstat

Lists all network connections for all processes.

mac.proc_maps.Maps

Lists process memory ranges that potentially contain injected code.

mac.pslist.PsList

Lists the processes present in a particular mac memory image.

mac.pstree.PsTree

Plugin for listing processes in a tree based on their parent process ID.

mac.vfsevents.VFSevents

Lists processes that are filtering file system events

linux.lsof.Lsof

Lists all memory maps for all processes.

linux.malfind.Malfind

Lists process memory ranges that potentially contain injected code.

linux.proc.Maps

Lists all memory maps for all processes.

linux.pslist.PsList

Lists the processes present in a particular linux memory image.

linux.pstree.PsTree

Plugin for listing processes in a tree based on their parent process ID.

linux.bash.Bash

Recovers bash command history from memory.

linux.check_creds.Check_creds

Checks if any processes are sharing credential structures

linux.check_modules.Check_modules

Compares module list to sysfs info, if available

linux.check_syscall.Check_syscall

Check system call table for hooks