Volatility Commands for Basic Malware Analysis: Descriptions and Examples

HASCYBER

Hands-on Cybersecurity Tutorials

Stephen Hasford

Command	Description
banners.Banners	Attempts to identify potential linux banners in an image
configwriter.Configwriter	Runs the automagics and both prints and outputs configuration in the output directory.
frameworkinfo.FrameworkInfo	Plugin to list the various modular components of Volatility
isfinfo.IsfInfo	Determines information about the currently available ISF files, or a specific one
layerwriter.Layerwriter	Runs the automagics and writes out the primary layer produced by the stacker.
linux.bash.Bash	Recovers bash command history from memory.
linux.check_afinfo.Check_afinfo	Verifies the operation function pointers of network protocols.
linux.check_creds.Check._creds	Checks if any processes are sharing credential structures
linux.check_idt.Check_idt	Checks if the IDT has been altered
linux.check_modules.Check_modules	Compares module list to sysfs info, if available
linux.check_syscall.Check_syscall	Check system call table for hooks.
linux.elfs.Elfs	Lists all memory mapped ELF files for all processes.
linux.envars.Envars **linux.enwvars.Enwvars**	Lists processes with their environment variables
linux.iomem.IOMem	Generates an output similar to /proc/iomem on a running system.
linux.keyboard_notifiers.Keyboard_notifiers	Parses the keyboard notifier call chain
linux.kmsg.Kmsg	Kernel log buffer reader
linux.lsmod.Lsmod	Lists loaded kernel modules.
linux.lsof.Lsof	Lists all memory maps for all processes.
linux.malfind.Malfind	Lists process memory ranges that potentially contain injected code.
linux.mountinfo.MountInfo	Lists mount points on processes mount namespaces
linux.proc.Maps	Lists all memory maps for all processes.
linux.psaux.PsAux	Lists processes with their command line arguments
linux.pslist.PsList	Lists the processes present in a particular linux memory image.

linux.psscan.PsScan	Scans for processes present in a particular linux image.
linux.pstree.PsTree	Plugin for listing processes in a tree based on their parent process ID.
linux.sockstat.Sockstat	Lists all netwonk connections for all processes.
linux.tty_check.tty_check	Checks tty devices for hooks
mac.bash.Bash	Recovers bash command history from memory.
mac.check_Syscall.Check_Syscall	Check system call table for hooks.
mac.check_sysctl.Check_sysctl	Check sysctl handlers for hooks.
mac.check_trap_table.Check_trap_table	Check mach trap table for hooks.
mac. ifconfig.Ifconfig	Lists network interface information for all devices
mac. kauth_listeners.Kauth_listeners	Lists kauth listeners and their status
mac. kauth_scopes.Kauth.scopes	Lists kauth scopes and their status
mac.kevents.Kevents	Lists event handlers registered by processes
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.malfind.Malfind	Lists process memory ranges that potentially contain injected code.
mac.mount.Mount	A module containing a collection of plugins that produce data typically found in Mac's mount command
mac.netstat.Netstat	Lists all network connections for all processes.
mac.proc_maps.Maps	Lists process memory ranges that potentially contain injected code.
mac.psaux.Psaux	Recovers program command line arguments.
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.socket_filters.Socket_filters	Enumerates kernel socket filters.
mac.timers.Timers	Check for malicious kernel timers.
mac.trustedbsd.Trustedbsd	Checks for malicious trustedbsd modules
mac.ufsevents.VFSevents	Lists processes that are filtering file system events

Timeliner.Timeliner	Runs all relevant plugins that provide time related information and orders the results by time.
windows.bigpools.BigPools	List big page pools.
windows.callbacks.Callbacks	Lists kernel callbacks and notification routines.
windows.cmdline.CmdLine	Lists process command line arguments.
windows.crashinfo.Crashinfo	Lists the information from a Windows crash dump.
windows.devicetree.DeviceTree	Listing tree based on drivers and attached devices in a particular windows memory image.
windows.dillist.DllList	Lists the loaded modules in a particular windows memory image.
windows.driverirp.DriverIrp	List IRPs for drivers in a particular windows memory image.
windows.drivermodule.DriverModule	Determines if any loaded drivers were hidden by a rootkit
windows.driverscan.DriverScan	Scans for drivers present in a particular windows memory image.
windows.dumpfiles.DumpFiles	Dumps cached file contents from Windows memory samples.
windows.envars.Envars	Display process environment variables
windows.filescan.Filescan	Scans for file objects present in a particular windows memory image.
windows.getservicesids.GetServiceSIDs	Lists process token sids.
windows.getsids.GetSIDs	Print the SIDs owning each process
windows.handles.Handles	Lists process open handles.
windows.info.Info	Show OS & kernel details of the memory sample being analyzed.
windows.joblinks.Joblinks	Print process job link information
windows.ldrmodules.LdrModules	Lists the loaded modules in a particular windows memory image.
windows.malfind.Malfind	Lists process memory ranges that potentially contain injected code.
windows.mbrscan.MBRScan	Scans for and parses potential Master Boot Records (MBRs)
windows.memmap.Memmap	Prints the memory map
windows.modscan.Modscan	Scans for modules present in a particular windows memory image.
windows.modules.Modules	Lists the loaded kernel modules.
windows.mutantscan.MutantScan	Scans for mutexes present in a particular windows memory image.

windows.netscan.Netscan	Scans for network objects present in a particular windows memory image.
windows.netstat.NetStat	Traverses network tracking structures present in a particular windows memory image.
windows.poolscanner.Poolscanner	A generic pool scanner plugin.
windows.privileges.Privs	Lists process token privileges
windows.pslist.PsList	Lists the processes present in a particular windows memory image.
windows.psscan.Psscan	Scans for processes present in a particular windows memory image.
windows.pstree.PsTree	Plugin for listing processes in a tree based on their parent process ID.
windows.registry.certificates.Certificates	Lists the certificates in the registry's Certificate Store.
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.registry printkey.PrintKey	Lists the registry keys under a hive or specific key value.
windows.registry.userassist.UserAssist	Print userassist registry keys and information.
windows.sessions.Sessions	lists Processes with Session information extracted from Environmental Variables
windows.skeleton_key_check.Skeleton_Key_Check	Looks for signs of Skeleton Key malware
windows.ssdt.SSDT	Lists the system call table.
windows.statistics.Statistics	Lists statistics about the memory space.
windows.strings.Strings	Reads output from the strings command and indicates which process(es) each string belongs to.
windows.symlinkscan.Symlinkscan	Scans for links present in a particular windows memory image.
windows.vadinfo.VadInfo	Lists process memory ranges.
windows.wadwalk.Vadwalk	Walk the VAD tree.
windows.verinfo.VerInfo	Lists version information from PE files.
windows.wirtmap.VirtMap	Lists virtual mapped sections.

Examples of volatility command

- **python vol.py -f [filepath] windows.info.Info > [pathtosaveresult.txt]**

  Shows OS & kernel details of the memory sample being analysed.

- **python vol.py -f [filepath] windows.pstree.PsTree > [pathtosaveresult.txt]**

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

- **python vol.py -f [filepath] windows.netscan.NetScan > [pathtosaveresult.txt]**

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

- **python vol.py -f [filepath] windows.pslist.PsList > [pathtosaveresult.txt]**

  Lists the processes present in a particular windows memory image.

- **python vol.py -f [filepath] windows.dlllist.DllList > [pathtosaveresult.txt]**

  Lists the loaded modules in a particular windows memory image.

- **python vol.py -f [filepath] windows.netstat.NetStat > [pathtosaveresult.txt]**

  Shows traverses network tracking structures present in a particular windows memory image.

A Typical Volatility Command Example

```
python vol.py -f "C:\Users\hascyberX\Desktop\memdump.mem" windows.pslist.PsList > C:\Users\hascyberX\Desktop\processlist.txt
```

The command above will list the processes present in the memdump.mem image, save the result on the desktop as processlists.txt, which can be opened with Notepad++ to analyze the output results.

Please consider subscribing to my YouTube Channel Hascyber where you can find hands-on tutorials on cybersecurity. Thank you!