Volafox

Description

Volafox is an open source toolkit that you can use for Mac OS X and BSD forensics. The tool is python based and allows investigating security incidents and finding information for malwares and any malicious program on the system. Security analyst can have the following information using this tool:

- MAC Kernel version, CPU, and memory specification
- Mounted filesystems
- Kernel Extensions listing
- Process listing
- Task listing (Finding process hiding)
- Syscall table (Hooking detection)
- Mach trap table (Hooking detection)
- Network socket listing (Hash table)
- Open files listing by process
- Show Boot information
- EFI System Table, EFI Runtime Services
- Print a hostname

Installation

Volafox can be installed using the sources from github :
https://github.com/n0fate/volafox

Prerequisite

- Kernel Image(kernel)
- Memory Image

Usage

All the command are available on the tool description :
https://github.com/n0fate/volafox/blob/master/README.md

volafox: Mac OS X Memory Analysis Toolkit

project: http://code.google.com/p/volafox

support: 10.6-8; 32/64-bit kernel

*input: *.vmem (VMWare memory file), *.mmr (Mac Memory Reader, flattened x86, IA-32e)*

usage: python ./vol.py -i IMAGE [-o COMMAND [-vp PID][-x PID][-x KEXT_ID][-x TASKID]]

Options:

-o CMD : Print kernel information for CMD (below)

-p PID : List open files for PID (where CMD is "lsof")

-v : Print all files, including unsupported types (where CMD is "lsof")

-x PID/KID/TASKID : Dump process/task/kernel extension address space for PID/KID/Task ID (where CMD is "ps"/"kextstat"/"tasks")

COMMANDS:

system_profiler : Kernel version, CPU, and memory spec, Boot/Sleep/Wakeup time

mount : Mounted filesystems

kextstat : KEXT (Kernel Extensions) listing

ps : Process listing

tasks : Task listing (& Matching Process List)

systab : Syscall table (Hooking Detection)

mtt : Mach trap table (Hooking Detection)

netstat : Network socket listing (Hash table)

lsof : Open files listing by process (research, osxmem@gmail.com)

pestate : Show Boot information (experiment)

efiinfo : EFI System Table, EFI Runtime Services(experiment)

keychaindump : Dump master key candidates for decrypting keychain(Lion, ML)

```
$ python volafox.py -i MemoryImage.mem -s mach_kernel -o os_version
Memory Image: MemoryImage.mem
Kernel Image: mach_kernel
Information: os_version
Detail dawin kernel version: 10A432
```

This command displays the ProductBuildVersion that you can also find in /System/Library/CoreServices/SystemVersion.plist.

Here is some more information about the machine:

```
$ python volafox.py -i MemoryImage.mem -s mach_kernel -o machine_info
Memory Image: MemoryImage.mem
Kernel Image: mach_kernel
Information: machine_info

-= Mac OS X Basic Information =-
Major Version: 10
Minor Version: 0
Number of Physical CPUs: 2
Size of memory in bytes: 536870912 bytes
Size of physical memory: 536870912 bytes
Number of physical CPUs now available: 2
Max number of physical CPUs now possible: 2
Number of logical CPUs now available: 2
Max number of logical CPUs now possible: 2
```

Volafox can traverse the list of mounted file systems:

```
$ python volafox.py -i MemoryImage.mem -s mach_kernel -o mount_info
Memory Image: MemoryImage.mem
Kernel Image: mach_kernel
Information: mount_info

-= Mount List =-
list entry      fstypename    mount on name        mount from name
0304a290        hfs     /     /dev/disk0s2
03049948        devfs   /dev  devfs
03049000        autofs  /net  map -hosts
0403d520        autofs  /home map auto_home
```

```
00000000    vmhgfs/Volumes/VMware Shared Folders    .host:/
```

OS X maintains a doubly-linked list of processes; the list head is reachable via the kernproc symbol (see Mattieu Suiche's paper).

$ python volafox.py -i MemoryImage.mem -s mach_kernel -o proc_info

Memory Image: MemoryImage.mem
Kernel Image: mach_kernel
Information: proc_info

-= process list =-

list_entry_next	pid	ppid	process name	username
03290d20	0	0	kernel_task	
03290a80	1	0	launchdask	n0fate
032902a0	2	1	launchctlk	root
032907e0	10	1	kextddask	root
03290540	11	1	DirectoryService	root
03290000	12	1	notifydask	root
0359bd20	13	1	diskarbitrationd	root
0359ba80	14	1	configdask	root
0359b7e0	15	1	syslogdask	root
0359b540	16	1	distnotedk	root
0359b000	17	1	mDNSResponder	_mdnsresponder
0359b2a0	19	1	securitydk	_mdnsresponder
03a5a7e0	24	1	ntpdhdask	_mdnsresponder
03bc7d20	26	1	usbmuxdask	_usbmuxd
03bc7a80	30	1	mdschdask	_mdnsresponder
03bc77e0	31	1	loginwindow	n0fate
03bc72a0	32	1	KernelEventAgent	_mdnsresponder
03bc7000	34	1	hiddhdask	_mdnsresponder
03bdaa80	35	1	fseventsdk	_mdnsresponder
03befd20	37	1	dynamic_pager	_mdnsresponder
03bef7e0	42	1	autofsdask	_mdnsresponder
03a5a2a0	53	1	taskgatedk	_usbmuxd
03bdad20	54	1	coreservicesd	root
03a5a540	55	1	WindowServer	root
03bda540	57	1	vmware-tools-dae	_mdnsresponder
03a5a000	74	1	airportdsk	_atsserver
03befa80	78	1	coreaudiod	_coreaudiod
03bda2a0	79	1	launchdask	n0fate
03bef000	83	79	Dockhdask	n0fate
03bc7540	84	79	SystemUIServer	n0fate

```
04166d20    85    79    Finderask    n0fate
03bef2a0    92    79    fontddask    n0fate
041667e0    95    79    pboardask    n0fate
```

A process can be selected by its PID in order to display a few more details:

```
$ python volafox.py -i MemoryImage.mem -s mach_kernel -o proc_info -x 120
Memory Image: MemoryImage.mem
Kernel Image: mach_kernel
Information: proc_info
Dump PID: 120

-= process: 120=-
list_entry_next pid    ppid    process name        username
0085e758        120    1       backupdask    n0fate
task_ptr: 3bd81f4
vm_map_t: 41b2520
prev: 46145d8
next: 461402c
start: 100000000
end: 7fffffe00000
neutries: 3a
entries_pageable: 1
pmap_t: 3bf59f8
page directory pointer: 3bf5828
phys.address of dirbase: 4705c2400000000
object to pde: 1
ref count: 1
nx_enabled: 2
task_map: 0
pm_cr3: 0
pm_pdpt: 25c00000259
pm_pml4: 127df00000000000
```

Volafox also enumerates lists of kernel extensions and system calls. It will raise a flag if a syscall appears to be hooked.