

Contents

Introduction	xvii
--------------------	------

I An Introduction to Memory Forensics 1

1 Systems Overview.....	3
<i>Digital Environment</i>	3
<i>PC Architecture</i>	4
<i>Operating Systems</i>	17
<i>Process Management</i>	18
<i>Memory Management</i>	20
<i>File System</i>	24
<i>I/O Subsystem</i>	25
<i>Summary</i>	26
2 Data Structures	27
<i>Basic Data Types</i>	27
<i>Summary</i>	43
3 The Volatility Framework	45
<i>Why Volatility?</i>	45
<i>What Volatility Is Not</i>	46
<i>Installation</i>	47
<i>The Framework</i>	51
<i>Using Volatility</i>	59
<i>Summary</i>	67
4 Memory Acquisition.....	69
<i>Preserving the Digital Environment</i>	69
<i>Software Tools</i>	79
<i>Memory Dump Formats</i>	95
<i>Converting Memory Dumps</i>	106
<i>Volatile Memory on Disk</i>	107
<i>Summary</i>	114

II Windows Memory Forensics 115

5	Windows Objects and Pool Allocations	117
	<i>Windows Executive Objects</i>	117
	<i>Pool-Tag Scanning</i>	129
	<i>Limitations of Pool Scanning</i>	140
	<i>Big Page Pool</i>	142
	<i>Pool-Scanning Alternatives</i>	146
	<i>Summary</i>	148
6	Processes, Handles, and Tokens	149
	<i>Processes</i>	149
	<i>Process Tokens</i>	164
	<i>Privileges</i>	170
	<i>Process Handles</i>	176
	<i>Enumerating Handles in Memory</i>	181
	<i>Summary</i>	187
7	Process Memory Internals	189
	<i>What's in Process Memory?</i>	189
	<i>Enumerating Process Memory</i>	193
	<i>Summary</i>	217
8	Hunting Malware in Process Memory	219
	<i>Process Environment Block</i>	219
	<i>PE Files in Memory</i>	238
	<i>Packing and Compression</i>	245
	<i>Code Injection</i>	251
	<i>Summary</i>	263
9	Event Logs	265
	<i>Event Logs in Memory</i>	265
	<i>Real Case Examples</i>	275
	<i>Summary</i>	279
10	Registry in Memory	281
	<i>Windows Registry Analysis</i>	281
	<i>Volatility's Registry API</i>	292
	<i>Parsing Userassist Keys</i>	295

<i>Detecting Malware with the Shimcache</i>	297
<i>Reconstructing Activities with Shellbags</i>	298
<i>Dumping Password Hashes</i>	304
<i>Obtaining LSA Secrets</i>	305
<i>Summary</i>	307
11 Networking	309
<i>Network Artifacts</i>	309
<i>Hidden Connections</i>	323
<i>Raw Sockets and Sniffers</i>	325
<i>Next Generation TCP/IP Stack</i>	327
<i>Internet History</i>	333
<i>DNS Cache Recovery</i>	339
<i>Summary</i>	341
12 Windows Services	343
<i>Service Architecture</i>	343
<i>Installing Services</i>	345
<i>Tricks and Stealth</i>	346
<i>Investigating Service Activity</i>	347
<i>Summary</i>	366
13 Kernel Forensics and Rootkits	367
<i>Kernel Modules</i>	367
<i>Modules in Memory Dumps</i>	372
<i>Threads in Kernel Mode</i>	378
<i>Driver Objects and IRPs</i>	381
<i>Device Trees</i>	386
<i>Auditing the SSDT</i>	390
<i>Kernel Callbacks</i>	396
<i>Kernel Timers</i>	399
<i>Putting It All Together</i>	402
<i>Summary</i>	406
14 Windows GUI Subsystem, Part I	407
<i>The GUI Landscape</i>	407
<i>GUI Memory Forensics</i>	410
<i>The Session Space</i>	410
<i>Window Stations</i>	416
<i>Desktops</i>	422

<i>Atoms and Atom Tables</i>	429
<i>Windows</i>	435
<i>Summary</i>	452
15 Windows GUI Subsystem, Part II	453
<i>Window Message Hooks</i>	453
<i>User Handles</i>	459
<i>Event Hooks</i>	466
<i>Windows Clipboard</i>	468
<i>Case Study: ACCDFISA Ransomware</i>	472
<i>Summary</i>	476
16 Disk Artifacts in Memory	477
<i>Master File Table</i>	477
<i>Extracting Files</i>	493
<i>Defeating TrueCrypt Disk Encryption</i>	503
<i>Summary</i>	510
17 Event Reconstruction	511
<i>Strings</i>	511
<i>Command History</i>	523
<i>Summary</i>	536
18 Timelining	537
<i>Finding Time in Memory</i>	537
<i>Generating Timelines</i>	539
<i>Gh0st in the Enterprise</i>	543
<i>Summary</i>	573
III Linux Memory Forensics	575
19 Linux Memory Acquisition	577
<i>Historical Methods of Acquisition</i>	577
<i>Modern Acquisition</i>	579
<i>Volatility Linux Profiles</i>	583
<i>Summary</i>	589
20 Linux Operating System	591
<i>ELF Files</i>	591

Linux Data Structures	603
Linux Address Translation	607
procfs and sysfs	609
Compressed Swap	610
Summary	610
21 Processes and Process Memory	611
Processes in Memory	611
Enumerating Processes	613
Process Address Space	616
Process Environment Variables	625
Open File Handles	626
Saved Context State	630
Bash Memory Analysis	630
Summary	635
22 Networking Artifacts	637
Network Socket File Descriptors	637
Network Connections	640
Queued Network Packets	643
Network Interfaces	646
The Route Cache	650
ARP Cache	652
Summary	655
23 Kernel Memory Artifacts	657
Physical Memory Maps	657
Virtual Memory Maps	661
Kernel Debug Buffer	663
Loaded Kernel Modules	667
Summary	673
24 File Systems in Memory	675
Mounted File Systems	675
Listing Files and Directories	681
Extracting File Metadata	684
Recovering File Contents	691
Summary	695

25	Userland Rootkits	697
	<i>Shellcode Injection</i>	698
	<i>Process Hollowing</i>	703
	<i>Shared Library Injection</i>	705
	<i>LD_PRELOAD Rootkits</i>	712
	<i>GOT/PLT Overwrites</i>	716
	<i>Inline Hooking</i>	718
	<i>Summary</i>	719
26	Kernel Mode Rootkits	721
	<i>Accessing Kernel Mode</i>	721
	<i>Hidden Kernel Modules</i>	722
	<i>Hidden Processes</i>	728
	<i>Elevating Privileges</i>	730
	<i>System Call Handler Hooks</i>	734
	<i>Keyboard Notifiers</i>	735
	<i>TTY Handlers</i>	739
	<i>Network Protocol Structures</i>	742
	<i>Netfilter Hooks</i>	745
	<i>File Operations</i>	748
	<i>Inline Code Hooks</i>	752
	<i>Summary</i>	754
27	Case Study: Phalanx2	755
	<i>Phalanx2</i>	755
	<i>Phalanx2 Memory Analysis</i>	757
	<i>Reverse Engineering Phalanx2</i>	763
	<i>Final Thoughts on Phalanx2</i>	772
	<i>Summary</i>	772

IV Mac Memory Forensics

28	Mac Acquisition and Internals	775
	<i>Mac Design</i>	775
	<i>Memory Acquisition</i>	780
	<i>Mac Volatility Profiles</i>	784
	<i>Mach-O Executable Format</i>	787
	<i>Summary</i>	791

29	Mac Memory Overview	793
	<i>Mac versus Linux Analysis</i>	793
	<i>Process Analysis</i>	794
	<i>Address Space Mappings</i>	799
	<i>Networking Artifacts</i>	804
	<i>SLAB Allocator</i>	808
	<i>Recovering File Systems from Memory</i>	811
	<i>Loaded Kernel Extensions</i>	815
	<i>Other Mac Plugins</i>	818
	<i>Mac Live Forensics</i>	819
	<i>Summary</i>	821
30	Malicious Code and Rootkits	823
	<i>Userland Rootkit Analysis</i>	823
	<i>Kernel Rootkit Analysis</i>	828
	<i>Common Mac Malware in Memory</i>	838
	<i>Summary</i>	844
31	Tracking User Activity	845
	<i>Keychain Recovery</i>	845
	<i>Mac Application Analysis</i>	849
	<i>Summary</i>	858
	Index	859