

Contents

A NOTE FROM THE EXECUTIVE EDITORS	xi
ABOUT THE AUTHORS	xiii
CONTRIBUTORS	xv
CHAPTER 1 CYBER SECURITY FUNDAMENTALS	1
1.1 Network and Security Concepts	1
1.1.1 Information Assurance Fundamentals	1
1.1.1.1 Authentication	1
1.1.1.2 Authorization	2
1.1.1.3 Nonrepudiation	3
1.1.1.4 Confidentiality	3
1.1.1.5 Integrity	4
1.1.1.6 Availability	5
1.1.2 Basic Cryptography	6
1.1.3 Symmetric Encryption	11
1.1.3.1 Example of Simple Symmetric Encryption with Exclusive OR (XOR)	12
1.1.3.2 Improving upon Stream Ciphers with Block Ciphers	14
1.1.4 Public Key Encryption	16
1.1.5 The Domain Name System (DNS)	20
1.1.5.1 Security and the DNS	24
1.1.6 Firewalls	25
1.1.6.1 History Lesson	25
1.1.6.2 What's in a Name?	25
1.1.6.3 Packet-Filtering Firewalls	27
	V

	1.1.6.4	Stateful Firewalls	28
	1.1.6.5	Application Gateway Firewalls	29
	1.1.6.6	Conclusions	29
	1.1.7	Virtualization	30
	1.1.7.1	In the Beginning, There Was Blue ...	31
	1.1.7.2	The Virtualization Menu	31
	1.1.7.3	Full Virtualization	33
	1.1.7.4	Getting a Helping Hand from the Processor	34
	1.1.7.5	If All Else Fails, Break It to Fix It	35
	1.1.7.6	Use What You Have	35
	1.1.7.7	Doing It the Hard Way	36
	1.1.7.8	Biting the Hand That Feeds	37
	1.1.7.9	Conclusion	38
	1.1.8	Radio-Frequency Identification	38
	1.1.8.1	Identify What?	39
	1.1.8.2	Security and Privacy Concerns	41
1.2		Microsoft Windows Security Principles	43
	1.2.1	Windows Tokens	43
	1.2.1.1	Introduction	43
	1.2.1.2	Concepts behind Windows Tokens	43
	1.2.1.3	Access Control Lists	46
	1.2.1.4	Conclusions	47
	1.2.2	Window Messaging	48
	1.2.2.1	Malicious Uses of Window Messages	49
	1.2.2.2	Solving Problems with Window Messages	51
	1.2.3	Windows Program Execution	51
	1.2.3.1	Validation of Parameters	52
	1.2.3.2	Load Image, Make Decisions	55
	1.2.3.3	Creating the Process Object	56
	1.2.3.4	Context Initialization	57
	1.2.3.5	Windows Subsystem Post Initialization	58
	1.2.3.6	Initial Thread ... Go!	60
	1.2.3.7	Down to the Final Steps	61
	1.2.3.8	Exploiting Windows Execution for Fun and Profit	63
	1.2.4	The Windows Firewall	64
		References	70
CHAPTER 2		ATTACKER TECHNIQUES AND MOTIVATIONS	75
	2.1	How Hackers Cover Their Tracks (Antiforensics)	75
	2.1.1	How and Why Attackers Use Proxies	75

2.1.1.1	Types of Proxies	76
2.1.1.2	Detecting the Use of Proxies	78
2.1.1.3	Conclusion	79
2.1.2	Tunneling Techniques	80
2.1.2.1	HTTP	81
2.1.2.2	DNS	83
2.1.2.3	ICMP	85
2.1.2.4	Intermediaries, Steganography, and Other Concepts	85
2.1.2.5	Detection and Prevention	86
2.2	Fraud Techniques	87
2.2.1	Phishing, Smishing, Vishing, and Mobile Malicious Code	87
2.2.1.1	Mobile Malicious Code	88
2.2.1.2	Phishing against Mobile Devices	89
2.2.1.3	Conclusions	91
2.2.2	Rogue Antivirus	92
2.2.2.1	Following the Money: Payments	95
2.2.2.2	Conclusion	95
2.2.3	Click Fraud	96
2.2.3.1	Pay-per-Click	97
2.2.3.2	Click Fraud Motivations	98
2.2.3.3	Click Fraud Tactics and Detection	99
2.2.3.4	Conclusions	101
2.3	Threat Infrastructure	102
2.3.1	Botnets	102
2.3.2	Fast-Flux	107
2.3.3	Advanced Fast-Flux	111
	References	116

CHAPTER 3 EXPLOITATION 119

3.1	Techniques to Gain a Foothold	119
3.1.1	Shellcode	119
3.1.2	Integer Overflow Vulnerabilities	124
3.1.3	Stack-Based Buffer Overflows	128
3.1.3.1	Stacks upon Stacks	128
3.1.3.2	Crossing the Line	130
3.1.3.3	Protecting against Stack-Based Buffer Overflows	132
3.1.3.4	Addendum: Stack-Based Buffer Overflow Mitigation	132
3.1.4	Format String Vulnerabilities	133
3.1.5	SQL Injection	138
3.1.5.1	Protecting against SQL Injection	140
3.1.5.2	Conclusion	141
3.1.6	Malicious PDF Files	142
3.1.6.1	PDF File Format	143

	3.1.6.2	Creating Malicious PDF Files	144
	3.1.6.3	Reducing the Risks of Malicious PDF Files	145
	3.1.6.4	Concluding Comments	147
	3.1.7	Race Conditions	147
	3.1.7.1	Examples of Race Conditions	148
	3.1.7.2	Detecting and Preventing Race Conditions	151
	3.1.7.3	Conclusion	152
	3.1.8	Web Exploit Tools	152
	3.1.8.1	Features for Hiding	153
	3.1.8.2	Commercial Web Exploit Tools and Services	154
	3.1.8.3	Updates, Statistics, and Administration	157
	3.1.8.4	Proliferation of Web Exploit Tools Despite Protections	158
	3.1.9	DoS Conditions	159
	3.1.10	Brute Force and Dictionary Attacks	164
	3.1.10.1	Attack	168
	3.2	Misdirection, Reconnaissance, and Disruption Methods	171
	3.2.1	Cross-Site Scripting (XSS)	171
	3.2.2	Social Engineering	176
	3.2.3	WarXing	182
	3.2.4	DNS Amplification Attacks	186
	3.2.4.1	Defeating Amplification	190
	References		191
CHAPTER 4	MALICIOUS CODE		195
	4.1	Self-Replicating Malicious Code	195
	4.1.1	Worms	195
	4.1.2	Viruses	198
	4.2	Evading Detection and Elevating Privileges	203
	4.2.1	Obfuscation	203
	4.2.2	Virtual Machine Obfuscation	208
	4.2.3	Persistent Software Techniques	213
	4.2.3.1	Basic Input–Output System (BIOS)/Complementary Metal-Oxide Semiconductor (CMOS) and Master Boot Record (MBR) Malicious Code	213
	4.2.3.2	Hypervisors	214
	4.2.3.3	Legacy Text Files	214
	4.2.3.4	Autostart Registry Entries	215
	4.2.3.5	Start Menu “Startup” Folder	217
	4.2.3.6	Detecting Autostart Entries	217

4.2.4	Rootkits	219
4.2.4.1	User Mode Rootkits	219
4.2.4.2	Kernel Mode Rootkits	221
4.2.4.3	Conclusion	223
4.2.5	Spyware	223
4.2.6	Attacks against Privileged User Accounts and Escalation of Privileges	227
4.2.6.1	Many Users Already Have Administrator Permissions	228
4.2.6.2	Getting Administrator Permissions	229
4.2.6.3	Conclusion	230
4.2.7	Token Kidnapping	232
4.2.8	Virtual Machine Detection	236
4.2.8.1	Fingerprints Everywhere!	237
4.2.8.2	Understanding the Rules of the Neighborhood	238
4.2.8.3	Detecting Communication with the Outside World	240
4.2.8.4	Putting It All Together	241
4.2.8.5	The New Hope	243
4.2.8.6	Conclusion	243
4.3	Stealing Information and Exploitation	243
4.3.1	Form Grabbing	243
4.3.2	Man-in-the-Middle Attacks	248
4.3.2.1	Detecting and Preventing MITM Attacks	251
4.3.2.2	Conclusion	252
4.3.3	DLL Injection	253
4.3.3.1	Windows Registry DLL Injection	254
4.3.3.2	Injecting Applications	256
4.3.3.3	Reflective DLL Injections	258
4.3.3.4	Conclusion	259
4.3.4	Browser Helper Objects	260
4.3.4.1	Security Implications	261

References	264
------------	-----

CHAPTER 5 DEFENSE AND ANALYSIS TECHNIQUES 267

5.1	Memory Forensics	267
5.1.1	Why Memory Forensics Is Important	267
5.1.2	Capabilities of Memory Forensics	268
5.1.3	Memory Analysis Frameworks	268
5.1.4	Dumping Physical Memory	270
5.1.5	Installing and Using Volatility	270
5.1.6	Finding Hidden Processes	272
5.1.7	Volatility Analyst Pack	275
5.1.8	Conclusion	275

5.2	Honeypots	275
5.3	Malicious Code Naming	281
5.3.1	Concluding Comments	285
5.4	Automated Malicious Code Analysis Systems	286
5.4.1	Passive Analysis	287
5.4.2	Active Analysis	290
5.4.3	Physical or Virtual Machines	291
5.5	Intrusion Detection Systems	294
	References	301
CHAPTER 6	DEFENSE SPECIAL FILE INVESTIGATION TOOLS	305
INDEX		315