

# BRIEF CONTENTS

Acknowledgments . . . . .	xvii
Introduction . . . . .	xix
Chapter 0: Tools of the Tradecraft . . . . .	xxvii
<b>PART I: OFFENSIVE SECURITY DEVELOPMENT . . . . .</b>	<b>1</b>
Chapter 1: Web Application Exploits . . . . .	3
Chapter 2: Authentication Attacks . . . . .	49
Chapter 3: Custom Malware Development and Distribution. . . . .	97
<b>PART II: OFFENSIVE SECURITY ENGINEERING . . . . .</b>	<b>155</b>
Chapter 4: Automating Offensive Security Infrastructure Deployment . . . . .	157
Chapter 5: Applying Network Fundamentals to C2 Implementation . . . . .	179
Chapter 6: Reverse VPN Tunneling. . . . .	191
Chapter 7: Managing Infrastructure for Offensive Security Operations . . . . .	205
<b>PART III: OFFENSIVE SECURITY IN THE REAL WORLD . . . . .</b>	<b>221</b>
Chapter 8: Exploitation with Metasploit . . . . .	225
Chapter 9: Deploying a Dropbox. . . . .	243
Chapter 10: Phishing Attack with C2 Redirectors . . . . .	255
Chapter 11: Multiplayer C2 Configuration . . . . .	285
Resources . . . . .	297
Index . . . . .	299