Contents at a Glance

Introduction 1

Part 1: Building the Foundation for Security Testing 5

CHAPTER 1: Introduction to Vulnerability and Penetration Testing 7

CHAPTER 2: Cracking the Hacker Mindset 25

CHAPTER 3: Developing Your Security Testing Plan 37

CHAPTER 4: Hacking Methodology 49

Part 2: Putting Security Testing in Motion 59

CHAPTER 5: Information Gathering 61

CHAPTER 6: Social Engineering 69

CHAPTER 7: Physical Security 87

CHAPTER 8: Passwords 99

Part 3: Hacking Network Hosts 129

CHAPTER 9: Network Infrastructure Systems 131

CHAPTER 10: Wireless Networks 165

CHAPTER 11: Mobile Devices 193

Part 4: Hacking Operating Systems 205

CHAPTER 12: Windows 207

CHAPTER 13: Linux and macOS 233

Part 5: Hacking Applications 257

CHAPTER 14: Communication and Messaging Systems 259

CHAPTER 15: Web Applications and Mobile Apps 283

CHAPTER 16: Databases and Storage Systems 309

Part 6: Security Testing Aftermath 321

CHAPTER 17: Reporting Your Results 323

CHAPTER 18: Plugging Your Security Holes 329

CHAPTER 19: Managing Security Processes 337

Part 7: The Part of Tens 345
CHAPTER 20: Ten Tips for Getting Security Buy-In 347
CHAPTER 21: Ten Reasons Hacking Is the Only Effective Way to Test 353
CHAPTER 22: Ten Deadly Mistakes 357

Appendix: Tools and Resources 363

Index 379