Table of Contents

AUTHORS' STATEMENT ..... **V**

PREFACE ..... **VII**

ACKNOWLEDGMENTS ..... **X**

HOW TO USE THE BOOK ..... **XI**

Companion website (http://redteam.guide) XI

TABLE OF CONTENTS **12**

INTRODUCTION **15**

Red Teams in Security Testing 31
Red Teaming Organizations 37
Key Chapter Takeaways 40
Homework 40

ENGAGEMENT PLANNING **41**

Cost and Funding 41
Scope 41
Duration 42
Personnel Labor Cost 43
Equipment and Software Cost 44
Travel Cost 44
Pre- and Post-Engagement Cost 44
Frequency 45
Engagement Notifications 47
Roles and Responsibilities 49
Rules of Engagement (ROE) 55
Managing Risk 58
Threat Planning 60
Threat Profile 63
Creating a Threat Profile by Decomposing a Threat 68
A review of a blackhat's tradecraft 72
Threat Perspective 78
Threat Scenario 80
Threat Emulation 82
Scenario Models 83
Indicators of Compromise 85

Engagement Concepts 88
Deconfliction 94
Data Handling 98
Key Chapter Takeaways 103
Homework 103

ENGAGEMENT EXECUTION 104

Data Repository 104
Data Collection 108
Tradecraft 114
General Guidance 114
Execution Concepts 122
Tools and Tool Examples 128
Command and Control (C2) 136
Key Chapter Takeaways 150
Homework 150

ENGAGEMENT CULMINATION 151

Sanitization and Cleanup 151
Operator Log Verification 153
Pre-Report Briefings 154
Key Chapter Takeaways 161
Homework 161

ENGAGEMENT REPORTING 162

Attack Flow Diagrams 163
Observations vs. Findings 165
Risk Rating and Metrics 166
Risk Matrices Comparison 167
Attack Narrative 178
Key Chapter Takeaways 184
Homework 184

SUMMARY 185

CONCLUSION 187

APPENDIX A: EXAMPLE TEMPLATES 188

APPENDIX B: THOUGHT EXERCISES 189

Adversarial Mindset Challenge 189
Mindset Challenge Comments and Answers 195

APPENDIX C: DECOMPOSING A THREAT EXERCISE 199

DESCRIPTION 199
EXERCISE SCENARIO 199
GOAL 199
RESOURCES 200
BEGIN THE EXERCISE 200
CREATE A THREAT PROFILE 205
POSSIBLE SOLUTION 206

GLOSSARY OF TERMS 208