

BRIEF CONTENTS

FOREWORD

xv

ACKNOWLEDGMENTS

xvii

Foreword xv

Acknowledgments xvii

Introduction xix

PART I: RED TEAMING FUNDAMENTALS 1

Chapter 1: Principles of Application Design and Development. 3

Chapter 2: Evasion Strategies 21

PART II: HANDS-ON EVASIVE TOOL DEVELOPMENT 35

Chapter 3: Enumerating with Traffic Redirection. 37

Chapter 4: Developing Command-and-Control Implants 65

Chapter 5: Creating Lateral Exploits with Worms 97

Chapter 6: Enumerating Locally Without LOLBins 117

Chapter 7: Bypassing Detection with Hybrid Packing 137

Chapter 8: Staging and Exfiltrating Data Covertly 159

PART III: TESTING AND VALIDATION 179

Chapter 9: Building Detection Tools 181

Chapter 10: Executing Controlled Reveals. 201

Appendix: Technical Prerequisites 221

Index 231