

services to clients. She is responsible for Tangible Security's Commercial Division, where she leads the following business lines: penetration testing, including red and purple team operations; hardware hacking; product and supply chain security; governance, risk management, and compliance; incident response and digital forensics. Linda also leads a team of virtual Chief Information Security Officers (CISOs) in providing expert guidance to many organizations. Prior to her current position, Linda was the Vice President of Operations for N2 Net Security. Before that, she co-founded and served as Chief Operating Officer (COO) for Executive Instruments, an information security research and consulting firm.

Michael Baucom currently works for Tangible Security as the VP of Tangible Labs. While at Tangible he has worked on a wide variety of projects, including software security assessments, SDLC consulting, tool development, and penetration tests. Prior to working at Tangible Security, he served in the Marine Corps as a ground radio repairman. Additionally, he worked for IBM, Motorola, and Broadcom in several capacities, including test engineering, device driver development, and system software development for embedded systems. In addition to his work activities, Michael has been a trainer at Black Hat, speaker at several conferences, and technical editor for *Gray Hat Hacking: The Ethical Hacker's Handbook*. His current interests are in automating pen-test activities, embedded system security, and mobile phone security.

Chris Eagle is a senior lecturer in the computer science department at the Naval Postgraduate School in Monterey, California. A computer engineer/scientist for more than 30 years, he has authored several books, served as the chief architect for DARPA's Cyber Grand Challenge, frequently speaks at security conferences, and has contributed several popular open source tools to the security community.

The late **Shon Harris** is greatly missed. She was the president of Logical Security, a security consultant, a former engineer in the Air Force's Information Warfare unit, an instructor, and an author. She authored the best-selling *CISSP Exam Guide* (currently in its seventh edition), along with many other books. Shon consulted for a variety of companies in many different industries. Shon taught computer and information security to a wide range of clients, including RSA, Department of Defense, Department of Energy, West Point, National Security Agency (NSA), Bank of America, Defense Information Systems Agency (DISA), BMC, and many more. Shon was recognized as one of the top 25 women in the Information Security field by *Information Security Magazine*.

Disclaimer: The views expressed in this book are those of the authors and not of the U.S. government or any company mentioned herein.

About the Technical Editor

Heather Linn has over 20 years in the security industry and has held roles in corporate security, penetration testing, and as part of a hunt team. She has contributed to open source frameworks, including Metasploit, and has contributed to course materials on forensics, penetration testing, and information security taught around the globe.

Heather has presented at many security conferences, including multiple BSides conferences, local ISSA chapter conferences, and student events aimed at providing realistic expectations for new students entering the information security field.

CONTENTS AT A GLANCE

Part I	Preparation	
Chapter 1	Why Gray Hat Hacking? Ethics and Law	3
Chapter 2	Programming Survival Skills.....	15
Chapter 3	Next-Generation Fuzzing	47
Chapter 4	Next-Generation Reverse Engineering	67
Chapter 5	Software-Defined Radio	89
Part II	Business of Hacking	
Chapter 6	So You Want to Be a Pen Tester?.....	111
Chapter 7	Red Teaming Operations.....	127
Chapter 8	Purple Teaming	143
Chapter 9	Bug Bounty Programs.....	157
Part III	Exploiting Systems	
Chapter 10	Getting Shells Without Exploits	181
Chapter 11	Basic Linux Exploits.....	199
Chapter 12	Advanced Linux Exploits.....	225
Chapter 13	Windows Exploits.....	253
Chapter 14	Advanced Windows Exploitation	289
Chapter 15	PowerShell Exploitation.....	321
Chapter 16	Next-Generation Web Application Exploitation	341
Chapter 17	Next-Generation Patch Exploitation.....	363

Part IV Advanced Malware Analysis

Chapter 18 Dissecting Mobile Malware..... 389

Chapter 19 Dissecting Ransomware 417

Chapter 20 ATM Malware 443

Chapter 21 Deception: Next-Generation Honeypots..... 465

Part V Internet of Things

Chapter 22 Internet of Things to Be Hacked..... 497

Chapter 23 Dissecting Embedded Devices..... 511

Chapter 24 Exploiting Embedded Devices 529

Chapter 25 Fighting IoT Malware..... 549

Index..... 575

CONTENTS

Preface xxv

Acknowledgments xxvii

Introduction xxix

Part I Preparation

Chapter 1 Why Gray Hat Hacking? Ethics and Law 3

Know Your Enemy 3

 The Current Security Landscape 4

 Recognizing an Attack 5

The Gray Hat Way 5

 Emulating the Attack 6

 Frequency and Focus of Testing 9

Evolution of Cyberlaw 10

 Understanding Individual Cyberlaws 10

Summary 13

References 13

Chapter 2 Programming Survival Skills 15

C Programming Language 15

 Basic C Language Constructs 15

 Sample Program 22

 Compiling with gcc 23

Computer Memory 24

 Random Access Memory 24

 Endian 25

 Segmentation of Memory 25

 Programs in Memory 26

 Buffers 27

 Strings in Memory 27

 Pointers 27

 Putting the Pieces of Memory Together 28

Intel Processors 28

 Registers 29

Assembly Language Basics 30

 Machine vs. Assembly vs. C 30

 AT&T vs. NASM 30

 Addressing Modes 33

 Assembly File Structure 33

 Assembling 34