Certified Ethical Hacker (CEH) Version 9 Cert Guide

Second Edition

Michael Gregg

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

Certified Ethical Hacker (CEH) Version 9 Cert Guide, Second Edition

ISBN-13: 978-0-7897-5691-6
ISBN-10: 0-7897-5691-9
Library of Congress Control Number: 2017932316
Printed in the United States of America
First Printing: April 2017

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Acquisitions Editor
Michelle Newcomb

Development Editor
Ellie C. Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Bill McManus

Indexer
Ken Johnson

Proofreader
Gill Editorial Services

Technical Editor
Brock Pearson

Publishing Coordinator
Vanessa Evans

Cover Designer
Chuti Prasertsith

Compositor
Studio Galou

Contents at a Glance

Introduction xxi

CHAPTER 1 An Introduction to Ethical Hacking 3

CHAPTER 2 The Technical Foundations of Hacking 45

CHAPTER 3 Footprinting and Scanning 87

CHAPTER 4 Enumeration and System Hacking 149

CHAPTER 5 Malware Threats 195

CHAPTER 6 Sniffers, Session Hijacking, and Denial of Service 249

CHAPTER 7 Web Server Hacking, Web Applications, and Database Attacks 299

CHAPTER 8 Wireless Technologies, Mobile Security, and Attacks 355

CHAPTER 9 IDS, Firewalls, and Honeypots 397

CHAPTER 10 Physical Security and Social Engineering 441

CHAPTER 11 Cryptographic Attacks and Defenses 481

CHAPTER 12 Cloud Computing and Botnets 525

CHAPTER 13 Final Preparation 545

Glossary 549

Index 573

Online Content:

Glossary

APPENDIX A: Answers to the "Do I Know This Already?" Quizzes and Review Questions

APPENDIX B: Memory Tables

APPENDIX C: Memory Tables Answer Key

Contents

Introduction xxi

Chapter 1 An Introduction to Ethical Hacking 3

"Do I Know This Already?" Quiz 3

Foundation Topics 6

Security Fundamentals 6

Goals of Security 6

Risk, Assets, Threats, and Vulnerabilities 8

Backing Up Data to Reduce Risk 11

Defining an Exploit 11

Risk Assessment 12

Security Testing 13

No-Knowledge Tests (Black Box) 13

Full-Knowledge Testing (White Box) 14

Partial-Knowledge Testing (Gray Box) 14

Types of Security Tests 14

Hacker and Cracker Descriptions 16

Who Attackers Are 18

Ethical Hackers 19

Required Skills of an Ethical Hacker 20

Modes of Ethical Hacking 21

Test Plans—Keeping It Legal 24

Test Phases 25

Establishing Goals 26

Getting Approval 27

Ethical Hacking Report 28

Vulnerability Research—Keeping Up with Changes 29

Ethics and Legality 29

Overview of U.S. Federal Laws 30

Compliance Regulations 33

Payment Card Industry Data Security Standard (PCI-DSS) 34

Summary 35

Exam Preparation Tasks 35

Review All Key Topics 36

Define Key Terms 36
Hands-On Labs 36
Lab 1-1 Examining Security Policies 37
Review Questions 37
Suggested Reading and Resources 42

Chapter 2 The Technical Foundations of Hacking 45

"Do I Know This Already?" Quiz 45
Foundation Topics 48
The Attacker's Process 48
Performing Reconnaissance and Footprinting 48
Scanning and Enumeration 49
Gaining Access 50
Escalation of Privilege 51
Maintaining Access 51
Covering Tracks and Planting Backdoors 51
The Ethical Hacker's Process 52
NIST SP 800-15 53
Operationally Critical Threat, Asset, and Vulnerability Evaluation 53
Open Source Security Testing Methodology Manual 54
Security and the Stack 54
The OSI Model 54
Anatomy of TCP/IP Protocols 57
The Application Layer 59
The Transport Layer 63
The Internet Layer 66
The Network Access Layer 75
Summary 76
Exam Preparation Tasks 77
Review All Key Topics 77
Complete the Tables from Memory 77
Define Key Terms 78
Exercises 78
2.1 Install a Sniffer and Perform Packet Captures 78
2.2 List the Protocols, Applications, and Services Found at Each Layer of the Stack 79

Review Questions 80
Suggested Reading and Resources 84

Chapter 3 Footprinting and Scanning 87

"Do I Know This Already?" Quiz 87
Foundation Topics 90
Overview of the Seven-Step Information-Gathering Process 90
Information Gathering 90
Documentation 91
The Organization's Website 91
Job Boards 93
Employee and People Searches 94
EDGAR Database 97
Google Hacking 98
Usenet 103
Registrar Query 104
DNS Enumeration 107
Determining the Network Range 112
Traceroute 113
Identifying Active Machines 115
Finding Open Ports and Access Points 116
Nmap 123
SuperScan 127
THC-Amap 127
Hping 128
Port Knocking 128
War Driving 129
OS Fingerprinting 129
Active Fingerprinting Tools 131
Fingerprinting Services 133
Default Ports and Services 133
Finding Open Services 133
Mapping the Network Attack Surface 135
Manual Mapping 135
Automated Mapping 136

Summary 137
Exam Preparation Tasks 138
Review All Key Topics 138
Define Key Terms 138
Complete the Tables from Memory 139
Command Reference to Check Your Memory 139
Exercises 140
3.1 Performing Passive Reconnaissance 140
3.2 Performing Active Reconnaissance 141
Review Questions 142
Suggested Reading and Resources 147
Chapter 4 Enumeration and System Hacking 149
"Do I Know This Already?" Quiz 149
Foundation Topics 152
Enumeration 152
Windows Enumeration 152
Windows Security 155
NetBIOS and LDAP Enumeration 155
NetBIOS Enumeration Tools 158
SNMP Enumeration 160
Linux/UNIX Enumeration 161
NTP Enumeration 162
SMTP Enumeration 163
DNS Enumeration 163
System Hacking 164
Nontechnical Password Attacks 164
Technical Password Attacks 164
Password Guessing 165
Automated Password Guessing 167
Password Sniffing 167
Keylogging 168
Privilege Escalation and Exploiting Vulnerabilities 169
Exploiting an Application 170
Exploiting a Buffer Overflow 170

Owning the Box 172
Windows Authentication Types 173
Cracking Windows Passwords 175
Linux Authentication and Passwords 177
Cracking Linux Passwords 180
Hiding Files and Covering Tracks 181
Rootkits 182
File Hiding 184
Summary 185
Exam Preparation Tasks 186
Review All Key Topics 186
Define Key Terms 187
Complete the Tables from Memory 187
Command Reference to Check Your Memory 187
Exercise 188
4.1 NTFS File Streaming 188
Review Questions 189
Suggested Reading and Resources 193
Chapter 5 Malware Threats 195
"Do I Know This Already?" Quiz 195
Foundation Topics 197
Viruses and Worms 197
Types and Transmission Methods of Viruses 198
Virus Payloads 200
History of Viruses 201
Well-Known Viruses 202
Virus Tools 204
Trojans 205
Trojan Types 205
Trojan Ports and Communication Methods 206
Trojan Goals 208
Trojan Infection Mechanisms 208
Effects of Trojans 210

Trojan Tools 210
Distributing Trojans 213
Covert Communication 217
Tunneling via the Internet Layer 218
Tunneling via the Transport Layer 220
Tunneling via the Application Layer 221
Port Redirection 223
Keystroke Logging and Spyware 225
Hardware Keyloggers 226
Software Keyloggers 226
Spyware 227
Malware Countermeasures 228
Detecting Malware 228
Antivirus 231
Analyzing Malware 234
Static Analysis 234
Dynamic Analysis 236
Summary 239
Exam Preparation Tasks 239
Review All Key Topics 240
Define Key Terms 240
Command Reference to Check Your Memory 240
Exercises 241
5.1 Finding Malicious Programs 241
5.2 Using Process Explorer 242
Review Questions 243
Suggested Reading and Resources 247
Chapter 6 Sniffers, Session Hijacking, and Denial of Service 249
"Do I Know This Already?" Quiz 249
Foundation Topics 252
Sniffers 252
Passive Sniffing 253
Active Sniffing 253

Address Resolution Protocol 254
ARP Poisoning and MAC Flooding 255
Tools for Sniffing 262
Wireshark 262
Other Sniffing Tools 265
Sniffing and Spoofing Countermeasures 266
Session Hijacking 267
Transport Layer Hijacking 267
Identify and Find an Active Session 268
Predict the Sequence Number 269
Take One of the Parties Offline 270
Take Control of the Session 270
Application Layer Hijacking 271
Session Sniffing 271
Predictable Session Token ID 271
Man-in-the-Middle Attacks 272
Man-in-the-Browser Attacks 272
Client-Side Attacks 272
Session Replay Attacks 274
Session Fixation Attacks 274
Session Hijacking Tools 274
Preventing Session Hijacking 277
Denial of Service and Distributed Denial of Service 278
DoS Attack Techniques 280
Bandwidth Attacks 280
SYN Flood Attacks 281
ICMP Attacks 281
Peer-to-Peer Attacks 282
Program- and Application-Level Attacks 282
Permanent DoS Attacks 283
Distributed Denial of Service 284
DDoS Tools 285
DoS and DDOS Countermeasures 287

Summary 290
Exam Preparation Tasks 291
Review All Key Topics 291
Define Key Terms 291
Exercises 292
6.1 Scanning for DDoS Programs 292
6.2 Using SMAC to Spoof Your MAC Address 292
Review Questions 293
Suggested Reading and Resources 297
Chapter 7 Web Server Hacking, Web Applications, and Database Attacks 299
"Do I Know This Already?" Quiz 299
Foundation Topics 302
Web Server Hacking 302
Scanning Web Servers 304
Banner Grabbing and Enumeration 304
Web Server Vulnerability Identification 309
Attacking the Web Server 309
DoS/DDoS Attacks 310
DNS Server Hijacking and DNS Amplification Attacks 310
Directory Traversal 311
Man-in-the-Middle Attacks 313
Website Defacement 313
Web Server Misconfiguration 313
HTTP Response Splitting 314
Web Server Password Cracking 314
IIS Vulnerabilities 315
Automated Exploit Tools 316
Securing Web Servers 318
Web Application Hacking 320
Unvalidated Input 321
Parameter/Form Tampering 321
Injection Flaws 322
Cross-Site Scripting and Cross-Site Request Forgery Attacks 323

Hidden Field Attacks 325
Other Web Application Attacks 326
Attacking Web-Based Authentication 328
Web-Based Password Cracking and Authentication Attacks 329
Cookies 333
URL Obfuscation 334
Intercepting Web Traffic 335
Securing Web Applications 337
Database Hacking 339
Identifying SQL Servers 340
SQL Injection Vulnerabilities 341
SQL Injection Hacking Tools 344
Summary 345
Exam Preparation Tasks 346
Review All Key Topics 346
Exercise 346
7.1 Review CVEs and Buffer Overflows 346
Review Questions 347
Suggested Reading and Resources 352
Chapter 8 Wireless Technologies, Mobile Security, and Attacks 355
"Do I Know This Already?" Quiz 355
Foundation Topics 358
Wireless Technologies 358
Wireless History 358
Satellite TV 358
Cordless Phones 359
Mobile Device Operation and Security 360
Mobile Device Concerns 362
Mobile Device Platforms 363
Android 364
iOS 366
Windows Phone 367
BlackBerry 367
Mobile Device Management and Protection 368

Bluetooth 368
Wireless LANs 370
Wireless LAN Basics 370
Wireless LAN Frequencies and Signaling 372
Wireless LAN Security 373
Wireless LAN Threats 376
Eavesdropping 378
Configured as Open Authentication 378
Rogue and Unauthorized Access Points 379
Denial of Service (DoS) 380
Wireless Hacking Tools 381
Discover Wi-Fi Networks 381
Perform GPS Mapping 383
Wireless Traffic Analysis 383
Launch Wireless Attacks 383
Crack and Compromise the Wi-Fi Network 384
Securing Wireless Networks 384
Defense in Depth 384
Site Survey 386
Robust Wireless Authentication 388
Misuse Detection 389
Summary 389
Exam Preparation Tasks 390
Review All Key Topics 390
Define Key Terms 390
Review Questions 391
Suggested Reading and Resources 394
Chapter 9 IDS, Firewalls, and Honeypots 397
"Do I Know This Already?" Quiz 397
Foundation Topics 400
Intrusion Detection Systems 400
IDS Types and Components 400
Pattern Matching and Anomaly Detection 403
Snort 404

IDS Evasion 407
Flooding 408
Insertion and Evasion 408
Session Splicing 408
Shellcode Attacks 409
Other IDS Evasion Techniques 409
IDS Evasion Tools 411
Firewalls 412
Firewall Types 412
Network Address Translation 413
Packet Filters 414
Application and Circuit-Level Gateways 416
Stateful Inspection 416
Identifying Firewalls 417
Bypassing Firewalls 421
Honeypots 428
Types of Honeypots 429
Detecting Honeypots 430
Summary 431
Exam Preparation Tasks 432
Review All Key Topics 432
Define Key Terms 432
Review Questions 433
Suggested Reading and Resources 437
Chapter 10 Physical Security and Social Engineering 441
"Do I Know This Already?" Quiz 441
Foundation Topics 444
Physical Security 444
Threats to Physical Security 444
Physical Security for Documentation and Storage Media 448
Equipment Controls 449
Locks 449
Fax Machines 454
Area Controls 456

Location Data and Geotagging 456
Facility Controls 458
Personal Safety Controls 461
Fire Prevention, Detection, and Suppression 461
Physical Access Controls 462
Authentication 462
Defense in Depth 463
Social Engineering 463
Six Types of Social Engineering 464
Person-to-Person Social Engineering 464
Computer-Based Social Engineering 465
Phishing, Social Networking, and Targeted Attacks 465
Reverse Social Engineering 468
Policies and Procedures 468
Employee Hiring and Termination Policies 469
Help Desk Procedures and Password Change Policies 469
Employee Identification 469
Privacy Policies 470
Governmental and Commercial Data Classification 470
User Awareness 471
Summary 473
Exam Preparation Tasks 473
Review All Key Topics 473
Define Key Terms 474
Exercise 474
10.1 Encrypting Data at Rest for Added Physical Security 474
Review Questions 475
Suggested Reading and Resources 479

Chapter 11 Cryptographic Attacks and Defenses 481

"Do I Know This Already?" Quiz 482
Foundation Topics 484
Functions of Cryptography 484
History of Cryptography 485
Algorithms 487

Symmetric Encryption 488
Data Encryption Standard (DES) 489
Advanced Encryption Standard (AES) 492
Rivest Cipher 492
Asymmetric Encryption (Public Key Encryption) 492
RSA 493
Diffie-Hellman 494
ElGamal 494
Elliptic Curve Cryptography (ECC) 494
Hashing 495
Digital Signature 496
Steganography 497
Digital Certificates 502
Public Key Infrastructure 503
Trust Models 504
Single-Authority Trust 505
Hierarchical Trust 505
Web of Trust 506
Protocols, Applications, and Attacks 506
Encryption Cracking and Tools 509
Weak Encryption 512
Encryption-Cracking Tools 514
Summary 515
Exam Preparation Tasks 515
Review All Key Topics 515
Define Key Terms 516
Exercises 516
11.1 Examining an SSL Certificate 516
11.2 Using PGP 517
11.3 Using a Steganographic Tool to Hide a Message 518
Review Questions 518
Suggested Reading and Resources 523

Chapter 12 Cloud Computing and Botnets 525
"Do I Know This Already?" Quiz 525
Foundation Topics 528
Cloud Computing 528
Cloud Computing Issues and Concerns 530
Cloud Computing Attacks 532
Cloud Computing Security 533
Botnets 533
Botnet Countermeasures 536
Summary 539
Exam Preparation Tasks 539
Review All Key Topics 539
Define Key Terms 540
Exercise 540
12.1 Scanning for DDoS Programs 540
Review Questions 541
Suggested Reading and Resources 543
Chapter 13 Final Preparation 545
Hands-on Activities 545
Suggested Plan for Final Review and Study 545
Summary 547
Glossary 549
Index 573

Online Content:

Glossary
Appendix A Answers to the "Do I Know This Already?" Quizzes and Review Questions
Appendix B: Memory Tables
Appendix C: Memory Tables Answer Key

About the Author

Michael Gregg (CISSP, SSCP, CISA, MCSE, MCT, CTT+, A+, N+, Security+, CCNA, CASP, CISA, CISM, CEH, CHFI, and GSEC) is the founder and president of Superior Solutions, Inc., a Houston, Texas-based IT security consulting firm. Superior Solutions performs security assessments and penetration testing for Fortune 1000 firms. The company has performed security assessments for private, public, and governmental agencies. Its Houston-based team travels the country to assess, audit, and provide training services.

Michael is responsible for working with organizations to develop cost-effective and innovative technology solutions to security issues and for evaluating emerging technologies. He has more than 20 years of experience in the IT field and holds two associate's degrees, a bachelor's degree, and a master's degree. In addition to co-authoring the first, second, and third editions of *Security Administrator Street Smarts*, Michael has written or co-authored 14 other books, including *Build Your Own Security Lab: A Field Guide for Network Testing* (Wiley, 2008); *Hack the Stack: Using Snort and Ethereal to Master the 8 Layers of an Insecure Network* (Syngress, 2006); *Certified Ethical Hacker Exam Prep 2* (Que, 2006); and *Inside Network Security Assessment: Guarding Your IT Infrastructure* (Sams, 2005).

Michael has been quoted in newspapers such as the *New York Times* and featured on various television and radio shows, including NPR, ABC, CBS, Fox News, and others, discussing cyber security and ethical hacking. He has created more than a dozen IT security training classes. He has created and performed video instruction on many security topics, such as cyber security, CISSP, CISA, Security+, and others.

When not consulting, teaching, or writing, Michael enjoys 1960s muscle cars and has a slot in his garage for a new project car.

You can reach Michael by email at MikeG@thesolutionfirm.com.

Dedication

In loving memory of my mother-in-law, Elvira Estrello Cuellar, who always stood behind me, encouraged me, and prayed that all my dreams would come true.

Acknowledgments

I would like to offer a big thank-you to Christine, for her help and understanding during the long hours that such a project entails. I also want to thank Curley, Betty, and all of my family. A special thanks to the people of Pearson IT Certification, who helped make this project a reality.

Finally, I would like to acknowledge all the dedicated security professionals who contributed "In the Field" elements for this publication. They include Darla Bryant, Jim Cowden, Laura Chappell, Clement Dupuis, Rodney Fournier, Pete Herzog, Bryce Galbraith, Steve Kalman, George Mays, Shawn Merdinger, Mark "Fat Bloke" Osborn, Donald L. Pipkin, Shondra Schneider, and Allen Taylor.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *Certified Ethical Hacker (CEH) Version 9 Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789756916 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

The EC-Council Certified Ethical Hacker (CEH) exam has become the leading ethical hacking certification available today. CEH is recognized by both employers and the industry as providing candidates with a solid foundation of hands-on security testing skills and knowledge. The CEH exam covers a broad range of security concepts to prepare candidates for the technologies that they are likely to be working with if they move into a role that requires hands-on security testing.

Let's talk some about what this book is. It offers you the information for what you need to know to pass the exam. It's highly recommend that you spend time with the tools and software discussed in the book. You should also complete a number of practice tests to become more comfortable with the type of questions that you will see on the exam and get used to completing 125 questions in four hours. Depending on your personal study habits or learning style, you might benefit from buying this book *and* taking a class.

Cert Guides are meticulously crafted to give you the best possible learning experience for the particular characteristics of the technology covered and the actual certification exam. The instructional design implemented in the Cert Guides reflects the nature of the CEH certification exam. The Cert Guides provide you with the factual knowledge base you need for the exams, and then take it to the next level with exercises and exam questions that require you to engage in the analytic thinking needed to pass the CEH exam.

EC-Council recommends that the typical candidate for this exam have a minimum of 2 years of experience in IT security. In addition, EC-Council recommends that candidates have preexisting knowledge of networking, TCP/IP, and basic computer knowledge.

Now let's briefly discuss what this book is not. It is not a book designed to teach you advanced hacking techniques or the latest hack. This book's goal is to prepare you for the CEH 312-50 exam, and it is targeted to those with some networking, OS, and systems knowledge. It provides basics to get you started in the world of ethical hacking and prepare you for the exam. Those wanting to become experts in this field should be prepared for additional reading, training, and practical experience.

How to Use This Book

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. Therefore, this book does not try to help you pass the exams only by memorization but by truly learning and understanding the topics.

The book includes many features that provide different ways to study so you can be ready for the exam. If you understand a topic when you read it but do not study it any further, you probably will not be ready to pass the exam with confidence. The features included in this book give you tools that help you determine what you know, review what you know, better learn what you don't know, and be well prepared for the exam. These tools include

- **"Do I Know This Already?" Quizzes:** Each chapter begins with a quiz that helps you determine the amount of time you need to spend studying that chapter. The answers are provided in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions," available for download on the companion website.
- **Foundation Topics:** These are the core sections of each chapter. They explain the tools, hacking concepts, and their configuration for the topics in that chapter.
- **Exam Preparation Tasks:** This section lists a series of study activities that you should complete after reading the "Foundation Topics" section. Each chapter includes the activities that make the most sense for studying the topics in that chapter. The activities include
  - **Review All Key Topics:** The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The Review All Key Topics activity lists the key topics from the chapter and their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic. Review these topics carefully.
  - **Define Key Terms:** Although certification exams might be unlikely to ask a question such as "Define this term," the CEH 312-50 exam requires you to learn and know a lot of tools and how they are used. This section lists some of the most important terms from the chapter, asking you to write a short definition and compare your answer to the Glossary.
  - **Complete the Tables from Memory:** Like most certification guides from Pearson IT Certification, this book purposefully organizes information into tables and lists for easier study and review. Rereading these tables can prove very useful before the exam. However, it is easy to skim over the tables without paying attention to every detail, especially when you remember having seen the table's contents when reading the chapter.

    Instead of simply reading the tables in the various chapters, Appendix B, "Memory Tables," and Appendix C, "Memory Tables Answer Key," provide another review tool. Appendix B lists partially completed versions of many of the tables from the book. You can open Appendix B (a PDF on

the companion website page to this book) and print the appendix. For review, attempt to complete the tables.

Appendix C, also a PDF located on the companion website page, lists the completed tables to check yourself. You can also just refer to the tables as printed in the book.

- **Exercises:** One or more sample exercises at the end of each chapter list a series of tasks for you to practice, which apply the lessons from the chapter in a real-world setting.
- **Command Reference to Check Your Memory:** Chapters 3, 4, and 5 each include a command table that lists commonly used tools and their corresponding commands and descriptions.
- **Review Questions:** Each chapter includes review questions to help you confirm that you understand the content you just covered. The answers are provided in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Companion Website

This book's companion website gives you access to the Pearson Test Prep software (both online and Windows desktop versions) with two full practice exams, a PDF of the Glossary, and PDFs of Appendixes A, B, and C. To access the companion website, simply follow these steps:

1. Register your book by going to http://www.pearsonitcertification.com/register and entering the ISBN: **9780789756916**.
2. Respond to the challenge questions.
3. Go to your account page and click the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.

Pearson Test Prep Practice Test Software

This book comes complete with the Pearson Test Prep practice test software containing two full exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

1. Go to http://www.pearsontestprep.com.
2. Select **Pearson IT Certification** as your product group.
3. Enter your email/password for your account. If you don't have a Pearson IT Certification account, you will need to establish one by going to http://www.pearsonitcertification.com/join.
4. In the **My Products** tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product.
6. The product will now be listed in your My Products page. Click the **Exams** button to launch the exam settings screen and start your exam.

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website, or you can just enter this link in your browser:

http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip

To access the book's companion website and the software, simply follow these steps:

1. Register your book by going to: http://www.pearsonitcertification.com/register and entering the ISBN: **9780789756916**.
2. Respond to the challenge questions.
3. Go to your account page and click the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. After the software finishes downloading, unzip all the files on your computer.
7. Double-click the application file to start the installation, and follow the on-screen instructions to complete the registration.
8. When the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.

9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.
11. Click **Next** and then click **Finish** to download the exam data to your application.
12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will synch together, so saved exams and grade results recorded on one version will be available to you on the other as well.

Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study Mode
- Practice Exam Mode
- Flash Card Mode

Study Mode allows you to fully customize your exams and review the answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps. Practice Exam Mode locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card Mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode will not provide the detailed score reports that the other two modes will, so it should not be used if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you as well as two additional exams of unique

questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes that were made since the last time you used the software. This requires that you are connected to the Internet at the time you launch the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This will ensure you are running the latest version of the software engine.

Premium Edition eBook and Practice Tests

This book includes an exclusive offer for 70 percent off the Premium Edition eBook and Practice Tests edition of this title. See the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

End-of-Chapter Review Tools

Chapters 1 through 12 each have several features in the "Exam Preparation Tasks" and "Review Questions" sections at the end of the chapter. You might have already worked through these in each chapter. However, you might also find it helpful to use these tools again as you make your final preparations for the exam.

Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the CEH exam. In fact, if the primary objective of this book was different, the book's title would be misleading; however, the methods used in this book to help you pass the CEH exam are designed to also make you much more knowledgeable about how penetration testers do their job. While this book and the practice tests together have more than enough questions to help you prepare for the actual exam, the method in which they are used is not to simply make you memorize as many questions and answers as you possibly can.

One key methodology used in this book is to help you discover the exam topics and tools that you need to review in more depth. Remember that the CEH exam will expect you to understand not only hacking concepts but also common tools. So, this book does not try to help you pass by memorization, but helps you truly learn and understand the topics and when specific tools should be used. This book will help you pass the CEH exam by using the following methods:

- Helping you discover which test topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions in the practice tests

Who Should Read This Book?

This book is not designed to be a general security book or one that teaches network defenses. This book looks specifically at how attackers target networks, what tools attackers use, and how these techniques can be used by ethical hackers. Overall, this book is written with one goal in mind: to help you pass the exam.

So, why should you want to pass the CEH exam? Because it's one of the leading entry-level hacking certifications. It is also featured as part of DoD Directive 8140, and having the certification might mean a raise, a promotion, or other recognition. It's also a chance to enhance your résumé and to demonstrate that you are serious about continuing the learning process and that you're not content to rest on your laurels. Or one of many other reasons.

Strategies for Exam Preparation

Although this book is designed to prepare you to take and pass the CEH certification exam, there are no guarantees. Read this book, work through the questions and exercises, and when you feel confident, take the practice exams and additional exams provided in the test software. Your results should tell you whether you are ready for the real thing.

When taking the actual certification exam, make sure that you answer all the questions before your time limit expires. Do not spend too much time on any one question. If you are unsure about the answer to a question, answer it as best as you can, and then mark it for review.

Remember that the primary objective is not to pass the exam but to understand the material. When you understand the material, passing the exam should be simple. Knowledge is a pyramid; to build upward, you need a solid foundation. This book and the CEH certification are designed to ensure that you have that solid foundation.

Regardless of the strategy you use or the background you have, the book is designed to help you get to the point where you can pass the exam with the least amount of time required. For instance, there is no need for you to practice or read about scanning and Nmap if you fully understand the tool already. However, many people like to make sure that they truly know a topic and therefore read over material that they already know. Several book features will help you gain the confidence that you need to be convinced that you know some material already, and to help you know what topics you need to study more.

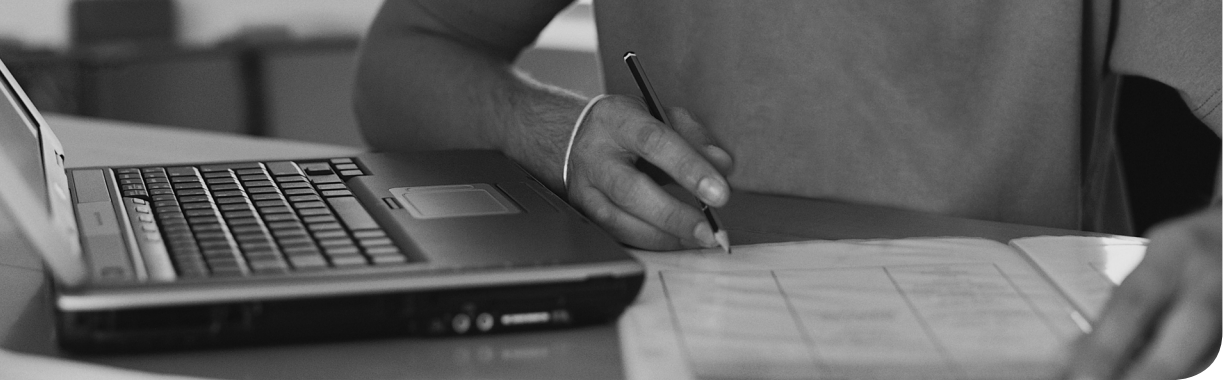
How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. Chapter 1 provides an overview of ethical hacking and reviews some basics. Chapters 2 through 12 are the core chapters. If you do intend to read them all, the order in the book is an excellent sequence to use.

The core chapters, Chapters 2 through 12, cover the following topics:

- **Chapter 2, "The Technical Foundations of Hacking"**—This chapter discusses basic techniques that every security professional should know. This chapter reviews TCP/IP and essential network knowledge.
- **Chapter 3, "Footprinting and Scanning"**—This chapter discusses the basic ideas behind target selection and footprinting. The chapter reviews what type of information should be researched during footprinting and how passive and active footprinting and scanning tools should be used.

- **Chapter 4, "Enumeration and System Hacking"**—This chapter covers enumeration, a final chance to uncover more detailed information about a target before system hacking. System hacking introduces the first step at which the hacker is actually exploiting a vulnerability in systems.
- **Chapter 5, "Malware Threats"**—This chapter examines all types of malware, including Trojans, worms, and viruses, and examines how malware is analyzed. This can include both static and dynamic analysis of malicious code.
- **Chapter 6, "Sniffers, Session Hijacking, and Denial of Service"**—This chapter covers sniffing tools such as Wireshark. The chapter examines the difference in passive and active sniffing. It also reviews session hijacking and DoS, DDoS, and botnet techniques.
- **Chapter 7, "Web Server Hacking, Web Applications, and Database Attacks"**—This chapter covers the basics of web hacking, application attacks, and how SQL injection works.
- **Chapter 8, "Wireless Technologies, Mobile Security, and Attacks"**—This chapter examines the underlying technology of wireless technologies, mobile devices, Android, iOS, and Bluetooth.
- **Chapter 9, "IDS, Firewalls, and Honeypots"**—This chapter discusses how attackers bypass intrusion detection systems and firewalls. This chapter also reviews honeypots and honeynets and how they are used to jail attackers.
- **Chapter 10, "Physical Security and Social Engineering"**—This chapter covers the fundamentals of social engineering attacks and introduces the concept that not all attacks are technical in nature. Attacks can be technical, social, or even physical. Finally, this chapter reviews important concepts of penetration testing.
- **Chapter 11, "Cryptographic Attacks and Defenses"**—This chapter covers the fundamentals of attacking cryptographic systems and how tools such as encryption can be used to protect critical assets.
- **Chapter 12, "Cloud Computing and Botnets"**—This chapter covers the fundamentals of cloud computing and reviews common cloud modeling types. The chapter reviews common cloud security issues and examines penetration testing concerns. The chapter also examines botnets and examines how they are used, detected, and dealt with.



This chapter covers the following topics:

- **Security Fundamentals:** You need to understand the security triad—confidentiality, integrity, and availability—because they form the basis on which all security is built.
- **Security Testing:** It is important to realize that ethical hackers differ from hackers in that ethical hackers perform activities only after obtaining written permission from the client that different types of tests can be performed.
- **Hacker and Cracker Descriptions:** Hackers can be known by many names. You should know these and what motivates various types of hacking attacks.
- **Ethical Hackers:** Ethical hackers perform security tests to strengthen the organization for which they work. You need to know the standards by which they work to perform their jobs ethically and effectively.
- **Test Plans—Keeping It Legal:** Test plans and deliverables usually include reports and data that detail the types of vulnerabilities discovered.
- **Ethics and Legality:** Knowledge of the legal environment is critical because you must ensure and maintain proper legal standing. In the United States, federal laws 18 U.S. Code Sections 1029 and 1030 are two such laws.

This chapter introduces you to the world of ethical hacking. Ethical hacking is a form of legal hacking done with the permission of an organization to help increase its security. This chapter discusses many of the business aspects of penetration (pen) testing. How should a pen test be performed, what types can be performed, what the legal requirements are, and what type of report should be delivered are all basic items that you need to know before you perform any type of security testing. However, first, you need to review some security basics. That's right, as my mom always said, "You must walk before you can run!" This chapter starts with a discussion of confidentiality, integrity, and availability. Next, it moves on to the subject of risk analysis, and it finishes up with the history of hacking and a discussion of some of the pertinent laws.

An Introduction to Ethical Hacking

CAUTION Nothing contained in this book is intended to teach or encourage the use of security tools or methodologies for illegal or unethical purposes. Always act in a responsible manner. Make sure you have written permission from the proper individuals before you use any of the tools or techniques described in this book. Always obtain permission before installing any security tools on a network.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 1-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Table 1-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Security Fundamentals	1
Security Testing	8–10
Hacker and Cracker Descriptions	3, 4, 7
Ethical Hackers	5
Test Plans—Keeping It Legal	6
Ethics and Legality	2

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you incorrectly guess skews your self-assessment results and might provide you with a false sense of security.

1. What are the three main tenants of security?
   a. Confidentiality, integrity, and availability
   b. Authorization, authentication, and accountability
   c. Deter, delay, and detect
   d. Acquire, authenticate, and analyze

2. Which of the following laws pertains to accountability for public companies relating to financial information?
   a. FISMA
   b. SOX
   c. 18 U.S.C. 1029
   d. 18 U.S.C. 1030

3. Which type of testing occurs when individuals know the entire layout of the network?
   a. Black box
   b. Gray box
   c. White box
   d. Blind testing

4. Which type of testing occurs when you have no knowledge of the network?
   a. Black box
   b. Gray box
   c. White box
   d. Blind testing

5. Which form of testing occurs when insiders are not informed of the pending test?
   a. Black box
   b. Gray box
   c. White box
   d. Blind testing

6. How is ethical hacking different from simple hacking?
   a. Ethical hackers never launch exploits.
   b. Ethical hackers have written permission.
   c. Ethical hackers act with malice.
   d. Ethical hackers have permission.

7. Which type of hacker is considered a good guy?
   a. White hat
   b. Gray hat
   c. Black hat
   d. Suicide hacker

8. Which type of hacker is considered unethical?
   a. White hat
   b. Gray hat
   c. Black hat
   d. Brown hat

9. Which type of hacker will carry out an attack even if the result could be a very long prison term?
   a. White hat
   b. Gray hat
   c. Black hat
   d. Suicide hacker

10. Which type of hacker performs both ethical and unethical activities?
    a. White hat
    b. Gray hat
    c. Black hat
    d. Suicide hacker

Foundation Topics

Security Fundamentals

Security is about finding a balance, as all systems have limits. No one person or company has unlimited funds to secure everything, and we cannot always take the most secure approach. One way to secure a system from network attack is to unplug it and make it a standalone system. Although this system would be relatively secure from Internet-based attackers, its usability would be substantially reduced. The opposite approach of plugging it in directly to the Internet without any firewall, antivirus, or security patches would make it extremely vulnerable, yet highly accessible. So, here again, you see that the job of security professionals is to find a balance somewhere between security and usability. Figure 1-1 demonstrates this concept. What makes this so tough is that companies face many more different challenges today than in the past. Whereas many businesses used to be bricks and mortar, they are now bricks and clicks. Modern businesses face many challenges, such as the increased sophistication of cyber criminals and the evolution of advanced persistent threats.

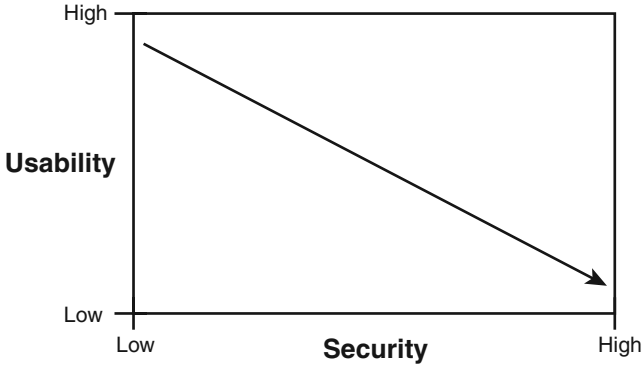


Figure 1-1 Security Versus Usability

To find this balance and meet today's challenges, you need to know what the goals of the organization are, what security is, and how to measure the threats to security. The next section discusses the goals of security.

Key Topic

Goals of Security

There are many ways in which security can be achieved, but it's universally agreed that the security triad of confidentiality, integrity, and availability (CIA) form the basic building blocks of any good security initiative.

Confidentiality addresses the secrecy and privacy of information. Physical examples of confidentiality include locked doors, armed guards, and fences. In the logical world, confidentiality must protect data in storage and in transit. For a real-life example of the failure of confidentiality, look no further than the recent news reports that have exposed how several large-scale breaches in confidentiality were the fault of corporations, such as Yahoo's loss of a billion passwords that occurred in the 2012 and 2013 timeframe and was reported in 2016 or the August 2016 revelation that more than 68 million Dropbox users had their usernames and passwords compromised in 2012. The graphic shown in Figure 1-2 from www.informationisbeautiful.net shows the scope of security breaches over the past several years. It offers a few examples of the scope of personally identifiable information (PII) that has been exposed.

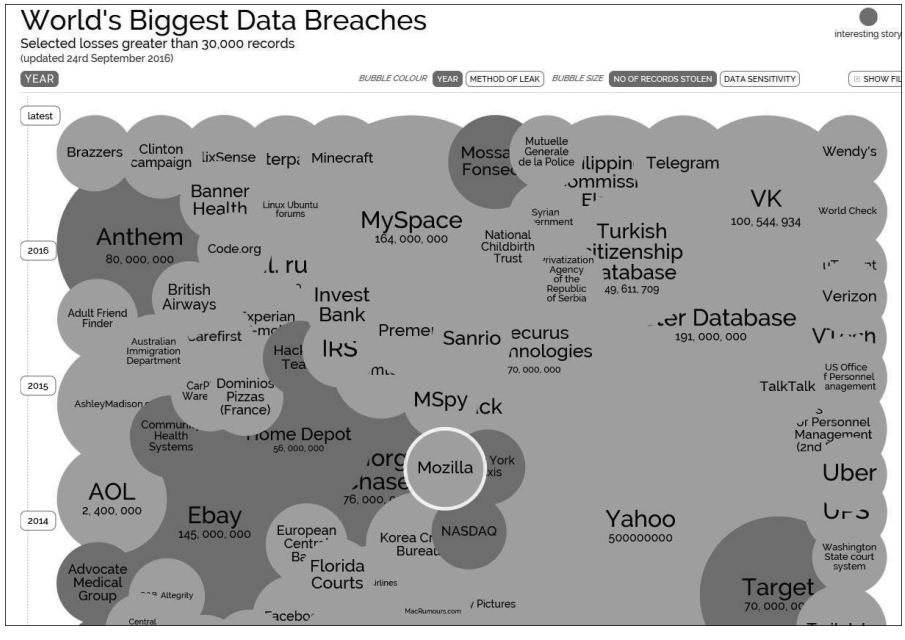


Figure 1-2 World's Biggest Data Breaches as of September 2016

Integrity is the second piece of the CIA security triad. Integrity provides for the correctness of information. It allows users of information to have confidence in its correctness. Correctness doesn't mean that the data is accurate, just that it hasn't been modified in storage or transit. Integrity can apply to paper or electronic documents. It is much easier to verify the integrity of a paper document than an electronic one. Integrity in electronic documents and data is much more difficult to protect than in paper ones. Integrity must be protected in two modes: storage and transit.

Information in storage can be protected if you use access and audit controls. Cryptography can also protect information in storage through the use of hashing algorithms. Real-life examples of this technology can be seen in programs such as Tripwire, MD5Sum, and Windows Resource Protection (WRP). Integrity in transit can be ensured primarily by the protocols used to transport the data. These security controls include hashing and cryptography.

Availability is the third leg of the CIA triad. Availability simply means that when a legitimate user needs the information, it should be available. As an example, access to a backup facility 24×7 does not help if there are no updated backups from which to restore. Similarly, cloud storage is of no use if the cloud provider is down. Service-level agreements (SLA) are one way availability can be ensured, and backups are another. Backups provide a copy of critical information should files and data be destroyed or equipment fail. Failover equipment is another way to ensure availability. Systems such as redundant array of inexpensive disks (RAID) and services such as redundant sites (hot, cold, and warm) are two other examples. Disaster recovery is tied closely to availability, as it's all about getting critical systems up and running quickly. Denial of service (DoS) is an attack against availability. Figure 1-3 shows an example of the CIA triad.

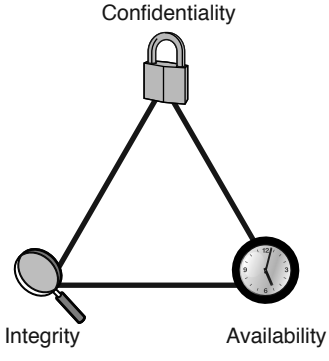


Figure 1-3 The CIA Triad

Risk, Assets, Threats, and Vulnerabilities

As with any new technology topic, to better understand the security field, you must learn the terminology that is used. To be a security professional, you need to understand the relationship between risk, threats, assets, and vulnerabilities.

Risk is the probability or likelihood of the occurrence or realization of a threat. There are three basic elements of risk: assets, threats, and vulnerabilities. To deal with risk, the U.S. federal government has adopted a risk management framework (RMF). The RMF process is based on the key concepts of mission- and risk-based, cost-effective,

and enterprise information system security. NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," transforms the traditional Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF). Let's look at the various components that are associated with risk, which include assets, threats, and vulnerabilities.

An asset is any item of economic value owned by an individual or corporation. Assets can be real—such as routers, servers, hard drives, and laptops—or assets can be virtual, such as formulas, databases, spreadsheets, trade secrets, and processing time. Regardless of the type of asset discussed, if the asset is lost, damaged, or compromised, there can be an economic cost to the organization.

NOTE No organization can ever be 100 percent secure. There will always be some risk left over. This is known as residual risk, the amount of risk left after safeguards and controls have been put in place to protect the asset.

A threat sets the stage for risk and is any agent, condition, or circumstance that could potentially cause harm, loss, or damage, or compromise an IT asset or data asset. From a security professional's perspective, threats can be categorized as events that can affect the confidentiality, integrity, or availability of the organization's assets. These threats can result in destruction, disclosure, modification, corruption of data, or denial of service. Examples of the types of threats an organization can face include the following:

- **Natural disasters, weather, and catastrophic damage:** Hurricanes, such as Matthew (which hit Florida and the U.S. East Coast in 2016), storms, weather outages, fire, flood, earthquakes, and other natural events compose an ongoing threat.
- **Hacker attacks:** An insider or outsider who is unauthorized and purposely attacks an organization's components, systems, or data.
- **Cyberattack:** Attackers who target critical national infrastructures such as water plants, electric plants, gas plants, oil refineries, gasoline refineries, nuclear power plants, waste management plants, and so on. Stuxnet is an example of one such tool designed for just such a purpose.
- **Viruses and malware:** An entire category of software tools that are malicious and are designed to damage or destroy a system or data. Cryptowall and Sality are two example of malware.
- **Disclosure of confidential information:** Anytime a disclosure of confidential information occurs, it can be a critical threat to an organization if that disclosure causes loss of revenue, causes potential liabilities, or provides a competitive advantage to an adversary.

- **Denial of service (DoS) or distributed DoS (DDoS) attacks:** An attack against availability that is designed to bring the network or access to a particular TCP/IP host/server to its knees by flooding it with useless traffic. Today, most DoS attacks are launched via botnets, whereas in the past tools such as the Ping of Death or Teardrop may have been used. Like malware, hackers constantly develop new tools so that Storm and Mariposa are replaced with other more current threats.

NOTE If the organization is vulnerable to any of these threats, there is an increased risk of successful attack.

A vulnerability is a weakness in the system design, implementation, software, or code, or the lack of a mechanism. A specific vulnerability might manifest as anything from a weakness in system design to the implementation of an operational procedure. Vulnerabilities might be eliminated or reduced by the correct implementation of safeguards and security countermeasures.

Vulnerabilities and weaknesses are common mainly because there isn't any perfect software or code in existence. Vulnerabilities can be found in each of the following:

- **Applications:** Software and applications come with tons of functionality. Applications may be configured for usability rather than for security. Applications may be in need of a patch or update that may or may not be available. Attackers targeting applications have a target-rich environment to examine. Just think of all the applications running on your home or work computer.
- **Operating systems:** This operating system software is loaded in workstations and servers. Attacks can search for vulnerabilities in operating systems that have not been patched or updated.
- **Misconfiguration:** The configuration file and configuration setup for the device or software may be misconfigured or may be deployed in an unsecure state. This might be open ports, vulnerable services, or misconfigured network devices. Just consider wireless networking. Can you detect any wireless devices in your neighborhood that have encryption turned off?
- **Shrinkwrap software:** The application or executable file that is run on a workstation or server. When installed on a device, it can have tons of functionality or sample scripts or code available.

Vulnerabilities are not the only concern the ethical hacker will have. Ethical hackers must also understand how to protect data. One way to protect data is through backup.

Backing Up Data to Reduce Risk

One way to reduce risk is by backing up data. While backups won't prevent problems such as ransomware, they can help mitigate the threat. The method your organization chooses depends on several factors:

- How often should backups occur?
- How much data must be backed up?
- How will backups be stored and transported offsite?
- How much time do you have to perform the backup each day?

The following are the three types of backup methods. Each backup method has benefits and drawbacks. Full backups take the longest time to create, whereas incremental backups take the least.

- **Full backups:** During a full backup, all data is backed up, and no files are skipped or bypassed; you simply designate which server to back up. A full backup takes the longest to perform and the least time to restore when compared to differential or incremental backups because only one set of tapes is required.
- **Differential backups:** Using differential backup, a full backup is typically done once a week and a daily differential backup is completed that copies all files that have changed since the last full backup. If you need to restore, you need the last full backup and the most recent differential backup.
- **Incremental backups:** This backup method works by means of a full backup scheduled for once a week, and only files that have changed since the previous full backup or previous incremental backup are backed up each day. This is the fastest backup option, but it takes the longest to restore. Incremental backups are unlike differential backups. When files are copied, the archive bit is reset; therefore, incremental backups back up only changes made since the last incremental backup.

Defining an Exploit

An *exploit* refers to a piece of software, a tool, a technique, or a process that takes advantage of a vulnerability that leads to access, privilege escalation, loss of integrity, or denial of service on a computer system. Exploits are dangerous because all software has vulnerabilities; hackers and perpetrators know that there are vulnerabilities and seek to take advantage of them. Although most organizations attempt to find and fix vulnerabilities, some organizations lack sufficient funds for securing their networks. Sometimes you may not even know the vulnerability exists, and that is

known as zero day exploit. Even when you do know there is a problem, you are burdened with the fact that a window exists between when a vulnerability is discovered and when a patch is available to prevent the exploit. The more critical the server, the slower it is usually patched. Management might be afraid of interrupting the server or afraid that the patch might affect stability or performance. Finally, the time required to deploy and install the software patch on production servers and workstations exposes an organization's IT infrastructure to an additional period of risk.

NOTE If you are looking for a good example of exploit code, consider the Mirai botnet. This exploit allowed hackers to take control of Internet of Things (IoT) devices with default usernames and passwords. While not the biggest botnet, it was able to exploit over 500,000 IoT devices in a very short period of time. Read more about it at http://www.computerweekly.com/news/450400311/Mirai-IoT-botnet-code-release-raises-fears-of-surge-in-DDoS-attacks.

Risk Assessment

A risk assessment is a process to identify potential security hazards and evaluate what would happen if a hazard or unwanted event were to occur. There are two approaches to risk assessment: qualitative and quantitative. Qualitative risk assessment methods use scenarios to drive a prioritized list of critical concerns and do not focus on dollar amounts. Example impacts might be identified as critical, high, medium, or low. Quantitative risk assessment assigns a monetary value to the asset. It then uses the anticipated exposure to calculate a dollar cost. These steps are as follows:

Step 1. **Determine the single loss expectancy (SLE):** This step involves determining the single amount of loss you could incur on an asset if a threat becomes realized or the amount of loss you expect to incur if the asset is exposed to the threat one time. SLE is calculated as follows: SLE = asset value × exposure factor. The exposure factor (EF) is the subjective, potential portion of the loss to a specific asset if a specific threat were to occur.

Step 2. **Evaluate the annual rate of occurrence (ARO):** The purpose of evaluating the ARO is to determine how often an unwanted event is likely to occur on an annualized basis.

Step 3. **Calculate the annual loss expectancy (ALE):** This final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE), which is calculated as follows: ALE = SLE × ARO.

CEH exam questions might ask you to use the SLE and ALE risk formulas. As an example, a question might ask, "If you have data worth $500 that has an exposure

factor of 50 percent due to lack of countermeasures such as antivirus, what would the SLE be?" You would use the following formula to calculate the answer:

SLE × EF = SLE, or $500 × .50 = $250

As part of a follow-up test question, could you calculate the annualized loss expectance (ALE) if you knew that this type of event typically happened four times a year? Yes, as this would mean the ARO is 4. Therefore:

ALE = SLE × ARO or $250 × 4 = $1,000

This means that, on average, the loss is $1,000 per year.

Because the organization cannot provide complete protection for all of its assets, a system must be developed to rank risk and vulnerabilities. Organizations must seek to identify high-risk and high-impact events for protective mechanisms. Part of the job of an ethical hacker is to identify potential vulnerabilities to these critical assets, determine potential impact, and test systems to see whether they are vulnerable to exploits while working within the boundaries of laws and regulations.

TIP Although it's important to know the steps involved in hacking, it's just as important to know the formulas used for risk assessment. These include: SLE = AV × EF and ALE = SLE × ARO.

Key Topic

Security Testing

Security testing is the primary job of ethical hackers. These tests might be configured in such way that the ethical hackers have no knowledge, full knowledge, or partial knowledge of the target of evaluation (TOE).

NOTE The term *target of evaluation* is widely used to identify an IT product or system that is the subject of an evaluation. The EC-Council and some security guidelines and standards use the term to describe systems that are being tested to measure their CIA.

The goal of the security test (regardless of type) is for the ethical hacker to test the TOE's security controls and evaluate and measure its potential vulnerabilities.

No-Knowledge Tests (Black Box)

No-knowledge testing is also known as black box testing. Simply stated, the security team has no knowledge of the target network or its systems. Black box testing simulates an outsider attack, as outsiders usually don't know anything about the network or systems they are probing. The attacker must gather all types of information about

the target to begin to profile its strengths and weaknesses. The advantages of black box testing include the following:

- The test is unbiased because the designer and the tester are independent of each other.
- The tester has no prior knowledge of the network or target being examined. Therefore, there are no preconceptions about the function of the network.
- A wide range of reconnaissance work is usually done to footprint the organization, which can help identify information leakage.
- The test examines the target in much the same way as an external attacker.

The disadvantages of black box testing include the following:

- Performing the security tests can take more time than partial- or full-knowledge testing.
- It is usually more expensive because it takes more time to perform.
- It focuses only on what external attackers see, whereas in reality many attacks are launched by insiders.

Full-Knowledge Testing (White Box)

White box testing takes the opposite approach of black box testing. This form of security test takes the premise that the security tester has full knowledge of the network, systems, and infrastructure. This information allows the security tester to follow a more structured approach and not only review the information that has been provided but also verify its accuracy. So, although black box testing will usually spend more time gathering information, white box testing will spend that time probing for vulnerabilities.

Partial-Knowledge Testing (Gray Box)

In the world of software testing, gray box testing is described as a partial-knowledge test. EC-Council literature describes gray box testing as a form of internal test. Therefore, the goal is to determine what insiders can access. This form of test might also prove useful to the organization because so many attacks are launched by insiders.

Types of Security Tests

Several different types of security tests can be performed. These can range from those that merely examine policy to those that attempt to hack in from the Internet

and mimic the activities of true hackers. These security tests are also known by many names, including the following:

- Vulnerability testing
- Network evaluations
- Red-team exercises
- Penetration testing
- Host vulnerability assessment
- Vulnerability assessment
- Ethical hacking

No matter what the security test is called, it is carried out to make a systematic examination of an organization's network, policies, and security controls. Its purpose is to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of potential security measures, and confirm the adequacy of such measures after implementation. Security tests can be defined as one of three types:

NOTE Although the CEH exam focuses on one type of security test, you should be aware of the different types so that you are fully able to meet any challenge presented to you.

- **High-level assessment/audit:** Also called a level I assessment, it is a top-down look at the organization's policies, procedures, and guidelines. This type of vulnerability assessment or audit does not include any hands-on testing. The purpose of a top-down assessment is to answer three questions:
  - Do the applicable policies, procedures, and guidelines exist?
  - Are they being followed?
  - Is their content sufficient to guard against potential risk?
- **Network evaluation:** Also called a level II assessment, it has all the elements specified in a level I assessment, and it includes hands-on activities. These hands-on activities include information gathering, scanning, vulnerability-assessment scanning, and other hands-on activities. Throughout this book, tools and techniques used to perform this type of assessment are discussed.
- **Penetration test:** Unlike assessments and evaluations, penetration tests are adversarial in nature. Penetration tests are also referred to as level III

assessments. These events usually take on an adversarial role and look to see what the outsider can access and control. Penetration tests are less concerned with policies and procedures and are more focused on finding low-hanging fruit and seeing what a hacker can accomplish on this network. This book offers many examples of the tools and techniques used in penetration tests.

Just remember that penetration tests are not fully effective if an organization does not have the policies and procedures in place to control security. Without adequate policies and procedures, it's almost impossible to implement real security. Documented controls are required. If none are present, you should evaluate existing practices.

Security policies are the foundation of the security infrastructure. There can be many different types of polices, such as access control, password, user account, email, acceptable use, and incident response. As an example, an incident response plan consists of actions to be performed in responding to and recovering from incidents. There are several slightly different approaches to incident response. The EC-Council approach to incident response follows the steps shown in Figure 1-4.

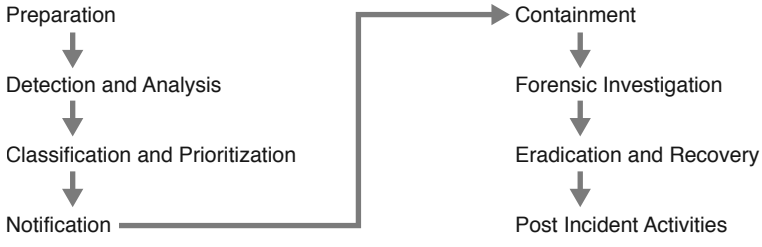


Figure 1-4 The Incident Response Process

You might be tasked with building security policies based on existing activities and known best practices. Good and free resources for accomplishing such a task are the SANS policy templates, available at http://www.sans.org/security-resources/policies/. How do ethical hackers play a role in these tests? That's the topic of the next section.

Hacker and Cracker Descriptions

To understand your role as an ethical hacker, it is important to know the players. Originally, the term *hacker* was used for a computer enthusiast. A hacker was a person who enjoyed understanding the internal workings of a system, computer, and computer network. Over time, the popular press began to describe hackers as individuals who broke into computers with malicious intent. The industry responded by

developing the word *cracker*, which is short for criminal hacker. The term cracker was developed to describe individuals who seek to compromise the security of a system without permission from an authorized party. With all this confusion over how to distinguish the good guys from the bad guys, the term *ethical hacker* was coined. An ethical hacker is an individual who performs security tests and other vulnerability-assessment activities to help organizations secure their infrastructures. Sometimes ethical hackers are referred to as white hat hackers.

Hacker motives and intentions vary. Some hackers are strictly legitimate, whereas others routinely break the law. Let's look at some common categories:

Key Topic

- **White hat hackers:** These individuals perform ethical hacking to help secure companies and organizations. Their belief is that you must examine your network in the same manner as a criminal hacker to better understand its vulnerabilities.
- **Black hat hackers:** These individuals perform illegal activities.
- **Gray hat hackers:** These individuals usually follow the law but sometimes venture over to the darker side of black hat hacking. It would be unethical to employ these individuals to perform security duties for your organization because you are never quite clear where they stand. Think of them as the character of Luke in *Star Wars*. While wanting to use the force of good, he is also drawn to the dark side.
- **Suicide hackers:** These are individuals that may carry out an attack even if they know there is a high chance that they will get caught and serve a long prison term.

NOTE Sometimes security professionals have crossed the line between ethical and unethical and not even known it. For example, in 2012, Andrew Auernheimer, who believed he was acting as an ethical hacker, exposed security flaws at AT&T and was charged with one count under the Computer Fraud and Abuse Act (CFAA). While he was convicted and sentenced to 41 months in prison, he argued on appeal that the techniques used were the same as those of ethical hackers. In April 2014, the U.S. Court of Appeals for the Third Circuit issued an opinion vacating Auernheimer's conviction, and while the judges did not address the substantive question on the legality of the site access, they were skeptical of the original conviction, noting that no circumvention of passwords had occurred and that only publicly accessible information was obtained. You can read more at http://www.techworm.net/2014/04/notorious-at-hacker-andrew-weev.html.

Hackers usually follow a fixed methodology that includes the following steps:

1. **Reconnaissance and footprinting:** Can be both passive and active.
2. **Scanning and enumeration:** Can include the use of port scanning tools and network mappers.
3. **Gaining access:** The entry point into the network, application, or system.
4. **Maintaining access:** Techniques used to maintain control, such as escalation of privilege.
5. **Covering tracks:** Planting rootkits, backdoors, and clearing logs are activities normally performed at this step.

Now let's turn our attention to who these attackers are and what security professionals are up against.

TIP Although it's important to know the steps involved in hacking, it is just as important to know what tools are used at a specific step. Questions on the CEH exam may ask you what tools are used at a specific step.

Who Attackers Are

Ethical hackers are up against several types of individuals in the battle to secure the network. The following list presents some of the more commonly used terms for these attackers:

- **Phreakers:** The original hackers. These individuals hacked telecommunication and PBX systems to explore the capabilities and make free phone calls. Their activities include physical theft, stolen calling cards, access to telecommunication services, reprogramming of telecommunications equipment, and compromising user IDs and passwords to gain unauthorized use of facilities, such as phone systems and voicemail.
- **Script kiddies:** A term used to describe often younger attackers who use widely available freeware vulnerability-assessment tools and hacking tools that are designed for attacking purposes only. These attackers usually do not have programming or hacking skills and, given the techniques used by most of these tools, can be defended against with the proper security controls and risk-mitigation strategies.
- **Disgruntled employees:** Employees who have lost respect and integrity for the employer. These individuals might or might not have more skills than the script kiddie. Many times, their rage and anger blind them. They rank as a

potentially high risk because they have insider status, especially if access rights and privileges were provided or managed by the individual.

- **Software crackers/hackers:** Individuals who have skills in reverse engineering software programs and, in particular, licensing registration keys used by software vendors when installing software onto workstations or servers. Although many individuals are eager to partake of their services, anyone who downloads programs with cracked registration keys is breaking the law and can be a greater potential risk and subject to malicious code and malicious software threats that might have been injected into the code.
- **Cyberterrorists/cybercriminals:** An increasing category of threat that can be used to describe individuals or groups of individuals who are usually funded to conduct clandestine or espionage activities on governments, corporations, and individuals in an unlawful manner. These individuals are typically engaged in sponsored acts of defacement: DoS/DDoS attacks, identity theft, financial theft, or worse, compromising critical infrastructures in countries, such as nuclear power plants, electric plants, water plants, and so on. These attacks may take months or years and are described as advanced persistent threats (APT).
- **System crackers/hackers:** Elite hackers who have specific expertise in attacking vulnerabilities of systems and networks by targeting operating systems. These individuals get the most attention and media coverage because of the globally affected malware, botnets, and Trojans that are created by system crackers/hackers. System crackers/hackers perform interactive probing activities to exploit security defects and security flaws in network operating systems and protocols.

Now that you have an idea who the adversary is, let's briefly discuss ethical hackers.

Ethical Hackers

Ethical hackers perform penetration tests. They perform the same activities a hacker would but without malicious intent. They must work closely with the host organization to understand what the organization is trying to protect, who they are trying to protect these assets from, and how much money and resources the organization is willing to expend to protect the assets.

By following a methodology similar to that of an attacker, ethical hackers seek to see what type of public information is available about the organization. Information leakage can reveal critical details about an organization, such as its structure, assets, and defensive mechanisms. After the ethical hacker gathers this information, it is evaluated to determine whether it poses any potential risk. The ethical hacker further probes the network at this point to test for any unseen weaknesses.

Penetration tests are sometimes performed in a double-blind environment. This means that the internal security team has not been informed of the penetration test. This serves an important purpose, allowing management to gauge the security team's responses to the ethical hacker's probing and scanning. Did they notice the probes, or have the attempted attacks gone unnoticed?

Now that the activities performed by ethical hackers have been described, let's spend some time discussing the skills that ethical hackers need, the different types of security tests that ethical hackers perform, and the ethical hacker rules of engagement.

Key Topic

Required Skills of an Ethical Hacker

Ethical hackers need hands-on security skills. Although you do not have to be an expert in everything, you should have an area of expertise. Security tests are usually performed by teams of individuals, where each individual has a core area of expertise. These skills include the following:

- **Routers:** Knowledge of routers, routing protocols, and access control lists (ACLs). Certifications such as Cisco Certified Network Associate (CCNA) and Cisco Certified Internetworking Expert (CCIE) can be helpful.
- **Microsoft:** Skills in the operation, configuration, and management of Microsoft-based systems. These can run the gamut from Windows 7 to Windows Server 2012. These individuals might be Microsoft Certified Solutions Associate (MCSA) or Microsoft Certified Solutions Expert (MCSE) certified.
- **Linux:** A good understanding of the Linux/UNIX OS. This includes security setting, configuration, and services such as Apache. These individuals may be Fedora or Linux+ certified.
- **Firewalls:** Knowledge of firewall configuration and the operation of intrusion detection systems (IDS) and intrusion prevention systems (IPS) can be helpful when performing a security test. Individuals with these skills may be certified as a Cisco Certified Network Associate Security Professional (CCNA) or Check Point Certified Security Administrator (CCSA).
- **Programming:** Knowledge of programming, including SQL, programming languages such as C++, Ruby, C#, and C, and scripting languages such as PHP and Java.
- **Mainframes:** Although mainframes do not hold the position of dominance they once had in business, they still are widely used. If the organization being assessed has mainframes, the security teams would benefit from having someone with that skill set on the team.

- **Network protocols:** Most modern networks are Transmission Control Protocol/Internet Protocol (TCP/IP). Someone with good knowledge of networking protocols, as well as how these protocols function and can be manipulated, can play a key role in the team. These individuals may possess certifications in other operating systems or hardware or may even possess a CompTIA Network+, Security+, or Advanced Security Practitioner (CASP) certification.
- **Project management:** Someone will have to lead the security test team, and if you are chosen to be that person, you will need a variety of the skills and knowledge types listed previously. It can also be helpful to have good project management skills. The parameters of a project are typically time, scope, and cost. After all, you will be defining the project scope when leading a pen test team. Individuals in this role may benefit from having Project Management Professional (PMP) certification.

On top of all this, ethical hackers need to have good report writing skills and must always try to stay abreast of current exploits, vulnerabilities, and emerging threats, as their goal is to stay a step ahead of malicious hackers.

Modes of Ethical Hacking

With all this talk of the skills that an ethical hacker must have, you might be wondering how the ethical hacker can put these skills to use. An organization's IT infrastructure can be probed, analyzed, and attacked in a variety of ways. Some of the most common modes of ethical hacking are described here:

- **Information gathering:** This testing technique seeks to see what type of information is leaked by the company and how an attack might leverage this information.
- **External penetration testing:** This ethical hack seeks to simulate the types of attacks that could be launched across the Internet. It could target Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), Structured Query Language (SQL), or any other available service.
- **Internal penetration testing:** This ethical hack simulates the types of attacks and activities that could be carried out by an authorized individual with a legitimate connection to the organization's network.
- **Network gear testing:** Firewall, IDS, router, and switches.
- **DoS testing:** This testing technique can be used to stress test systems or to verify their ability to withstand a DoS attack.

- **Wireless network testing:** This testing technique looks at wireless systems. This might include wireless networking systems, RFID, ZigBee, Bluetooth, or any wireless device.
- **Application testing:** Application testing is designed to examine input controls and how data is processed. All areas of the application may be examined.
- **Social engineering:** Social engineering attacks target the organization's employees and seek to manipulate them to gain privileged information. Employee training, proper controls, policies, and procedures can go a long way in defeating this form of attack.
- **Physical security testing:** This simulation seeks to test the organization's physical controls. Systems such as doors, gates, locks, guards, closed circuit television (CCTV), and alarms are tested to see whether they can be bypassed.
- **Authentication system testing:** This simulated attack is tasked with assessing authentication controls. If the controls can be bypassed, the ethical hacker might probe to see what level of system control can be obtained.
- **Database testing:** This testing technique is targeted toward SQL servers.
- **Communication system testing:** This testing technique examines communications such as PBX, Voice over IP (VoIP), modems, and voice communication systems.
- **Stolen equipment attack:** This simulation is closely related to a physical attack because it targets the organization's equipment. It could seek to target the CEO's laptop or the organization's backup tapes. No matter what the target, the goal is the same: extract critical information, usernames, and passwords.

Every ethical hacker must abide by the following rules when performing the tests described previously. If not, bad things can happen to you, which might include loss of job, civil penalty, or even jail time:

- **Never exceed the limits of your authorization:** Every assignment will have rules of engagement. This document includes not only what you are authorized to target but also the extent that you are authorized to control such system. If you are only authorized to obtain a prompt on the target system, downloading passwords and starting a crack on these passwords would be in excess of what you have been authorized to do.
- **Protect yourself by setting up damage limitations:** There has to be a nondisclosure agreement (NDA) between the client and the tester to protect them both. You should also consider liability insurance and an errors and omissions policy. Items such as the NDA, rules of engagement, project scope, and

resumes of individuals on the penetration testing team may all be bundled together for the client into one package.

- **Be ethical:** That's right; the big difference between a hacker and an ethical hacker is the word *ethics*. Ethics is a set of moral principles about what is correct or the right thing to do. Ethical standards sometimes differ from legal standards in that laws define what we must do or not do, whereas ethics define what we should do or not do.

In the Field: The OSSTMM—An Open Methodology

In January 2001, the Institute for Security and Open Methodologies (ISECOM) released the Open Source Security Testing Methodology Manual (OSSTMM). Hundreds of people contributed knowledge, experience, and peer review to the project. Eventually, as the only publicly available methodology that tested security from the bottom of operations and up (as opposed to from the policy on down), it received the attention of businesses, government agencies, and militaries around the world. It also scored success with little security start-ups and independent ethical hackers who wanted a public source for client assurance of their security testing services.

The primary purpose of the OSSTMM is to provide a scientific methodology for the accurate characterization of security through examination and correlation in a consistent and reliable way. Great effort has been put into the OSSTMM to ensure reliable cross-reference to current security management methodologies, tools, and resources. This manual is adaptable to penetration tests, ethical hacking, security assessments, vulnerability assessments, red-teaming, blue-teaming, posture assessments, and security audits. Your primary purpose for using it should be to guarantee facts and factual responses, which in turn ensures your integrity as a tester and the organization you are working for, if any. The end result is a strong, focused security test with clear and concise reporting. The main site for the nonprofit organization, ISECOM, that maintains the OSSTMM and many other projects is http://www.isecom.org.

This In the Field note was contributed by Pete Herzog, managing director, ISECOM.

- **Maintain confidentiality:** During security evaluations, you will likely be exposed to many types of confidential information. You have both a legal and a moral duty to treat this information with the utmost privacy. You should not share this information with third parties and should not use it for any unapproved purposes. There is an obligation to protect the information sent between the tester and the client. This has to be specified in an NDA.

- **Do no harm:** It's of utmost importance that you do no harm to the systems you test. Again, a major difference between a hacker and an ethical hacker is that an ethical hacker should do no harm. Misused security tools can lock out critical accounts, cause denial of service, and crash critical servers or applications. Take care to prevent these events unless that is the goal of the test.

Test Plans—Keeping It Legal

Most of us make plans before we take a big trip or vacation. We think about what we want to see, how we plan to spend our time, what activities are available, and how much money we can spend and not regret it when the next credit card bill arrives. Ethical hacking is much the same minus the credit card bill. Many details need to be worked out before a single test is performed. If you or your boss is tasked with managing this project, some basic questions need to be answered, such as what's the scope of the assessment, what are the driving events, what are the goals of the assessment, what will it take to get approval, and what's needed in the final report.

Before an ethical hacking test can begin, the scope of the engagement must be determined. Defining the scope of the assessment is one of the most important parts of the ethical hacking process. At some point, you will be meeting with management to start the discussions of the how and why of the ethical hack. Before this meeting ever begins, you will probably have some idea what management expects this security test to accomplish. Companies that decide to perform ethical hacking activities don't do so in a vacuum. You need to understand the business reasons behind this event. Companies can decide to perform these tests for various reasons. The most common reasons include the following:

- **A breach in security:** One or more events have occurred that highlight a lapse in security. It could be that an insider was able to access data that should have been unavailable, or it could be that an outsider was able to hack the organization's web server.
- **Compliance with state, federal, regulatory, or other law or mandate:** Compliance with state or federal laws is another event that might be driving the assessment. Companies can face huge fines and executives can face potential jail time if they fail to comply with state and federal laws. The Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), and Health Insurance Portability and Accountability Act (HIPAA) are three such laws. SOX requires accountability for public companies relating to financial information. HIPAA requires organizations to perform a vulnerability assessment. Your organization might decide to include ethical hacking into this test regime. One such standard that the organization might be attempting to comply with is ISO/IEC 27002. This information security standard was first published in

December 2000 by the International Organization for Standardization and the International Electrotechnical Commission. This code of practice for information security management is considered a security standard benchmark and includes the following 14 main elements:

- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and environmental security
- Operation security
- Communication security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

- **Due diligence:** Due diligence is another reason a company might decide to perform a pen test. The new CEO might want to know how good the organization's security systems really are, or it could be that the company is scheduled to go through a merger or is acquiring a new firm. If so, the pen test might occur before the purchase or after the event. These assessments are usually going to be held to a strict timeline. There is only a limited amount of time before the purchase, and if performed afterward, the organization will probably be in a hurry to integrate the two networks as soon as possible.

Test Phases

Security assessments in which ethical hacking activities will take place are composed of three phases: scoping the project, in which goals and guidelines are established, performing the assessment, and performing post-assessment activities, including the report and remediation activities. Figure 1-5 shows the three phases of the assessment and their typical times.

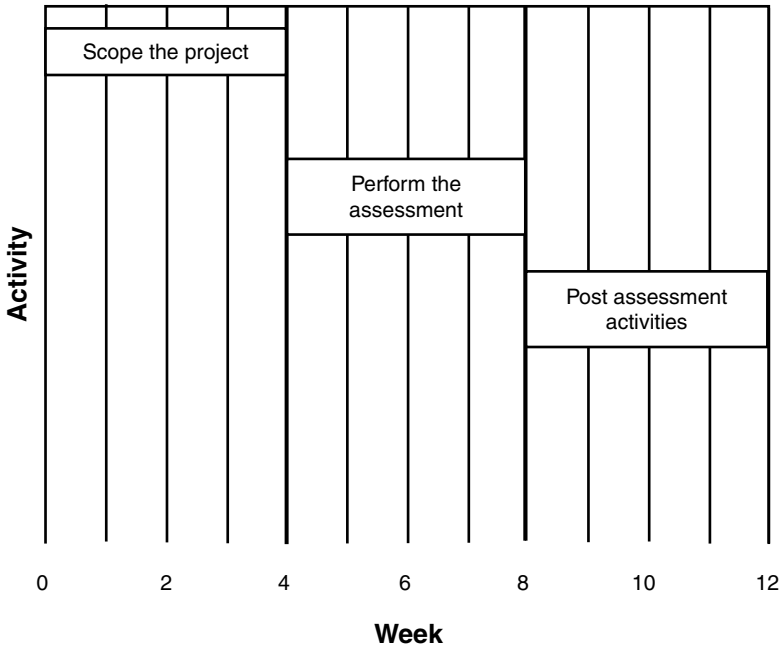


Figure 1-5 Ethical hacking phases and times.

Establishing Goals

The need to establish goals is critical. Although you might be ready to jump in and begin hacking, a good plan will detail the goals and objectives of the test. Common goals include system certification and accreditation, verification of policy compliance, and proof that the IT infrastructure has the capability to defend against technical attacks.

Are the goals to certify and accredit the systems being tested? Certification is a technical evaluation of the system that can be carried out by independent security teams or by the existing staff. Its goal is to uncover any vulnerabilities or weaknesses in the implementation. Your goal will be to test these systems to make sure that they are configured and operating as expected, that they are connected to and communicate with other systems in a secure and controlled manner, and that they handle data in a secure and approved manner.

If the goals of the penetration test are to determine whether current policies are being followed, the test methods and goals might be somewhat different. The security team will be looking at the controls implemented to protect information being stored, being transmitted, or being processed. This type of security test might not

have as much hands-on hacking but might use more social engineering techniques and testing of physical controls. You might even direct one of the team members to perform a little dumpster diving.

The goal of a technical attack might be to see what an insider or outsider can access. Your goal might be to gather information as an outsider and then use that data to launch an attack against a web server or externally accessible system.

Regardless of what type of test you are asked to perform, you can ask some basic questions to help establish the goals and objectives of the tests, including the following:

- What is the organization's mission?
- What specific outcomes does the organization expect?
- What is the budget?
- When will tests be performed: during work hours, after hours, on weekends?
- How much time will the organization commit to completing the security evaluation?
- Will insiders be notified?
- Will customers be notified?
- How far will the test proceed? Root the box, gain a prompt, or attempt to retrieve another prize, such as the CEO's password?
- Whom do you contact should something go wrong?
- What are the deliverables?
- What outcome is management seeking from these tests?

Key Topic

Getting Approval

Getting approval is a critical event in the testing process. Before any testing actually begins, you need to make sure that you have a plan that has been approved in writing. If this is not done, you and your team might face unpleasant consequences, which might include being fired or even facing criminal charges.

NOTE Written approval is the most critical step of the testing process. *Never* perform tests without written approval.

If you are an independent consultant, you might also get insurance before starting any type of test. Umbrella policies and those that cover errors and omissions are

commonly used in the field. These types of liability policies can help protect you should anything go wrong.

To help make sure that the approval process goes smoothly, ensure that someone is the champion of this project. This champion or project sponsor is the lead contact to upper management and your contact person. Project sponsors can be instrumental in helping you gain permission to begin testing and to provide you with the funding and materials needed to make this a success.

NOTE Management support is critical if a security test is to be successful.

Key Topic

Ethical Hacking Report

Although you have not actually begun testing, you do need to start thinking about the final report. Throughout the entire process, you should be in close contact with management to keep them abreast of your findings. There shouldn't be any big surprises when you submit the report. While you might have found some serious problems, they should be discussed with management before the report is written and submitted. The goal is to keep management in the loop and advised of the status of the assessment. If you find items that present a critical vulnerability, stop all tests and immediately inform management. Your priority should always be the health and welfare of the organization.

The report itself should detail the results of what was found. Vulnerabilities should be discussed, as should the potential risk they pose. Although people aren't fired for being poor report writers, don't expect to be promoted or praised for your technical findings if the report doesn't communicate your findings clearly. The report should present the results of the assessment in an easily understandable and fully traceable way. The report should be comprehensive and self-contained. Most reports contain the following sections:

- Introduction
- Statement of work performed
- Results and conclusions
- Recommendations

Because most companies are not made of money and cannot secure everything, rank your recommendations so that the ones with the highest risk/highest probability appear at the top of the list.

The report needs to be adequately secured while in electronic storage. Use encryption. The printed copy of the report should be marked *Confidential*, and while it is in

its printed form, take care to protect the report from unauthorized individuals. You have an ongoing responsibility to ensure the safety of the report and all information gathered. Most consultants destroy reports and all test information after a contractually obligated period of time.

NOTE The report is a piece of highly sensitive material and should be protected in storage and when in printed form.

Vulnerability Research—Keeping Up with Changes

If you are moving into the IT security field or are already working in IT security, you probably already know how quickly things change in this industry. That pace of change requires the security professional to keep abreast of new/developing tools, techniques, and emerging vulnerabilities. Although someone involved in security in the 1990s might know about Code Red or Nimda, that will do little good to combat ransomware or a Java watering hole attack. Because tools become obsolete and exploits become outdated, you want to build up a list of websites that you can use to keep up with current vulnerabilities. The sites listed here are but a few you should review:

- **National Vulnerability Database:** http://nvd.nist.gov/
- **Security Tracker:** http://securitytracker.com/
- **HackerWatch:** http://www.hackerwatch.org/
- **Dark Reading:** http://www.darkreading.com/
- **Exploit Database:** http://www.exploit-db.com/
- **HackerStorm:** http://hackerstorm.co.uk/
- **SANS Reading Room:** http://www.sans.org/reading_room/
- **SecurityFocus:** http://www.securityfocus.com/

NOTE At the end of each chapter is a more complete list of websites and URLs you should review.

Ethics and Legality

The word *ethics* is derived from the Greek word *ethos* (character) and from the Latin word *mores* (customs). Laws and ethics are much different in that ethics cover the gray areas that laws do not always address. Most professions, including EC-Council,

have highly detailed and enforceable codes of ethics for their members. Some examples of IT organizations that have codes of ethics include

- **EC-Council:** https://www.eccouncil.org/code-of-ethics
- **(ISC)^2:** https://www.isc2.org/ethics/default.aspx
- **ISACA:** http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx

To become a CEH, you must have a good understanding of ethical standards because you might be presented with many ethical dilemmas during your career. You can also expect to see several questions relating to ethics on the CEH exam.

Recent FBI reports on computer crime indicate that unauthorized computer use has continued to climb. A simple review of the news on any single day usually indicates reports of a variety of cybercrime and network attacks. Hackers use computers as a tool to commit a crime or to plan, track, and control a crime against other computers or networks. Your job as an ethical hacker is to find vulnerabilities before the attackers do and help prevent the attackers from carrying out malicious activities. Tracking and prosecuting hackers can be a difficult job because international law is often ill-suited to deal with the problem. Unlike conventional crimes that occur in one location, hacking crimes might originate in India, use a system based in Singapore, and target a computer network located in Canada. Each country has conflicting views on what constitutes cybercrime. Even if hackers can be punished, attempting to prosecute them can be a legal nightmare. It is hard to apply national borders to a medium such as the Internet that is essentially borderless.

TIP Some individuals approach computing and hacking from the social perspective and believe that hacking can promote change. These individuals are known as hactivists ("hacker activists") and use computers and technology for hi-tech campaigning and social change. They believe that defacing websites and hacking servers is acceptable as long as it promotes their goals. Regardless of their ethics and motives, hacking remains illegal, and hackers are subject to the same computer crime laws as any other criminal.

Overview of U.S. Federal Laws

Although some hackers might have the benefit of bouncing around the globe from system to system, your work will likely occur within the confines of the host nation. The United States and some other countries have instigated strict laws to deal with hackers and hacking. During the past 10 to 15 years, the U.S. federal government has taken a much more active role in dealing with computer crime, Internet activity,

privacy, corporate threats, vulnerabilities, and exploits. These are laws you should be aware of and not become entangled in. Hacking is covered under the U.S. Code Title 18: Crimes and Criminal Procedure: Part 1: Crimes: Chapter 47: Fraud and False Statements: Sections 1029 and 1030. Each section is described here:

- **Section 1029, Fraud and related activity with access devices:** This law gives the U.S. federal government the power to prosecute hackers who knowingly and with intent to defraud produce, use, or traffic in one or more counterfeit access devices. Access devices can be an application or hardware that is created specifically to generate any type of access credentials, including passwords, credit card numbers, long-distance telephone service access codes, PINs, and so on for the purpose of unauthorized access.
- **Section 1030, Fraud and related activity in connection with computers:** The law covers just about any computer or device connected to a network or Internet. It mandates penalties for anyone who accesses a computer in an unauthorized manner or exceeds one's access rights. This is a powerful law because companies can use it to prosecute employees when they use the capability and access that companies have given them to carry out fraudulent activities.

The Evolution of Hacking Laws

In 1985, hacking was still in its infancy in England. Because of the lack of hacking laws, some British hackers believed that there was no way they could be prosecuted. Triludan the Warrior was one of these individuals. Besides breaking into the British Telecom system, he also broke an admin password for Prestel. Prestel was a dialup service that provided online services, shopping, email, sports, and weather reports. One user of Prestel was His Royal Highness, Prince Phillip. Triludan broke into the prince's mailbox, along with various other activities, such as leaving the Prestel system admin messages and taunts.

Triludan the Warrior was caught on April 10, 1985, and was charged with five counts of forgery, as no hacking laws existed. After several years and a $3.5 million legal battle, Triludan was eventually acquitted. Others were not so lucky because in 1990, parliament passed the Computer Misuse Act, which made hacking attempts punishable by up to 5 years in jail. Today, the United Kingdom, along with most of the Western world, has extensive laws against hacking.

TIP 18 U.S. Code Sections 1029 and 1030 are the main statutes that address computer crime in U.S. federal law. You want to understand their basic coverage and penalties.

The punishment described in Sections 1029 and 1030 for hacking into computers ranges from a fine or imprisonment for no more than 1 year up to a fine and imprisonment for no more than 20 years. This wide range of punishment depends on the seriousness of the criminal activity and what damage the hacker has done and whether you are a repeat offender. Other federal laws that address hacking include the following:

- **Electronic Communication Privacy Act:** Mandates provisions for access, use, disclosure, interception, and privacy protections of electronic communications. The law encompasses U.S. Code Sections 2510 and 2701. According to the U.S. Code, *electronic communications* "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, or photo optical system that affects interstate or foreign commerce." This law makes it illegal for individuals to capture communication in transit or in storage. Although these laws were originally developed to secure voice communications, they now cover email and electronic communication.
- **Computer Fraud and Abuse Act of 1984:** The Computer Fraud and Abuse Act (CFAA) of 1984 protects certain types of information that the government maintains as sensitive. The Act defines the term *classified computer*, and imposes punishment for unauthorized or misused access into one of these protected computers or systems. The Act also mandates fines and jail time for those who commit specific computer-related actions, such as trafficking in passwords or extortion by threatening a computer. In 1992, Congress amended the CFAA to include malicious code, which was not included in the original Act.
- **The Cyber Security Enhancement Act of 2002:** This Act mandates that hackers who carry out certain computer crimes might now get life sentences in prison if the crime could result in another's bodily harm or possible death. This means that if hackers disrupt a 911 system, they could spend the rest of their days in prison.
- **The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001:** Originally passed because of the World Trade Center attack on September 11, 2001, it strengthens computer crime laws and has been the subject of some controversy. This Act gives the U.S. government extreme latitude in pursuing criminals. The Act permits the U.S. government to monitor hackers without a warrant and perform sneak-and-peek searches.
- **The Federal Information Security Management Act (FISMA):** This was signed into law in 2002 as part of the E-Government Act of 2002, replacing the Government Information Security Reform Act (GISRA). FISMA was

enacted to address the information security requirements for government agencies other than those involved in national security. FISMA provides a statutory framework for securing government-owned and -operated IT infrastructures and assets.

- **Federal Sentencing Guidelines of 1991:** Provides guidelines to judges so that sentences are handed down in a more uniform manner.
- **Economic Espionage Act of 1996:** Defines strict penalties for those accused of espionage.

NOTE Ethical hackers need to know that U.S. laws are not the only legal guidelines. Most nations have cybercrime laws on the books that address using a computer or network in the commission of a crime or the targeting of another computer or network.

Compliance Regulations

Although it's good to know what laws your company or client must abide by, ethical hackers should have some understanding of compliance regulations, too. In the United States, laws are passed by Congress. Regulations can be created by executive department and administrative agencies. The first step is to understand what regulations your company or client needs to comply with. Common ones include those shown in Table 1-2.

Table 1-2 Compliance Regulations and Frameworks

Name of Law/ Framework	Areas Addressed or Regulated	Responsible Agency or Entity
Sarbanes-Oxley (SOX) Act	Corporate financial information	Securities and Exchange Commission (SEC)
Gramm-Leach-Bliley Act (GLBA)	Consumer financial information	Federal Trade Commission (FTC)
Health Insurance Portability and Accountability Act (HIPAA)	Established privacy and security regulations for the healthcare industry	Department of Health and Human Services (HHS)
ISO/IEC 27001:2013	Operates as a risk management standard and provides requirements for establishing, implementing, and maintaining an information security management system	International Organization for Standardization (ISO)

Name of Law/ Framework	Areas Addressed or Regulated	Responsible Agency or Entity
Children's Internet Protection Act (CIPA)	Controls Internet access to pornography in schools and libraries	Federal Trade Commission (FTC)
Payment Card Industry Data Security Standard (PCI-DSS)	Controls on credit card processors	Payment Card Industry (PCI)

Typically, you will want to use a structured approach such as the following to evaluate new regulations that may lead to compliance issues:

Step 1. Interpret the law or regulation and the way it applies to the organization.

Step 2. Identify the gaps in the compliance and determine where the organization stands regarding the mandate, law, or requirement.

Step 3. Devise a plan to close the gaps identified.

Step 4. Execute the plan to bring the organization into compliance.

Let's look at one specific industry standard that CEH candidates should be aware of because it is global in nature and is a testable topic.

Payment Card Industry Data Security Standard (PCI-DSS)

PCI-DSS is a standard that most security professionals must understand because it applies in many different countries and to industries around the world. It is a proprietary information security standard that addresses credit card security. It applies to all entities that handle credit card data, such as merchants, processors, acquirers, and any other party that stores, processes, or transmits credit card data. PCI-DSS mandates a set of 12 high-level requirements that prescribe operational and technical controls to protect cardholder data. The requirements follow security best practices and are aligned across six goals:

- Build and maintain a secure network that is PCI compliant
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

For companies that are found to be in noncompliance, the fines can range from $5,000 to $500,000 and are levied by banks and credit card institutions.

Summary

This chapter established that security is based on the CIA triad of confidentiality, integrity, and availability. The principles of the CIA triad must be applied to IT networks and their data. The data must be protected in storage and in transit.

Because the organization cannot provide complete protection for all of its assets, a system must be developed to rank risk and vulnerabilities. Organizations must seek to identify high-risk and high-impact events for protective mechanisms. Part of the job of an ethical hacker is to identify potential threats to these critical assets and test systems to see whether they are vulnerable to exploits.

The activities described are security tests. Ethical hackers can perform security tests from an unknown perspective (black box testing) or with all documentation and knowledge (white box testing). The type of approach to testing that is taken will depend on the time, funds, and objective of the security test. Organizations can have many aspects of their protective systems tested, such as physical security, phone systems, wireless access, insider access, and external hacking.

To perform these tests, ethical hackers need a variety of skills. They not only must be adept in the technical aspects of networks but also must understand policy and procedure. No single ethical hacker will understand all operating systems, networking protocols, or application software. That's okay, though, because security tests typically are performed by teams of individuals, with each person bringing a unique skill or set of skills to the table.

So, even though god-like knowledge isn't required, an ethical hacker does need to understand laws pertaining to hackers and hacking and understand that the most important part of the pretest activities is to obtain written authorization. No test should be performed without the written permission of the network or service. Following this simple rule will help you stay focused on the legitimate test objectives and avoid any activities or actions that might be seen as unethical/unlawful.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 13, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 1-3 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 1-3 Key Topics for Chapter 1

Key Topic Element	Description	Page Number
Section	Goals of security	6
Section	Security testing	13
List	Categories of hackers	17
Section	Required skills of an ethical hacker	20
Section	Getting approval	27
Section	Ethical hacking report	28
Section	Ethics and legality	29

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

asset, availability, black box testing, confidentiality, denial of service (DoS), exploit, gray box testing, integrity, RAID, risk, target of engagement (TOE), threat, vulnerability, and white box testing

Hands-On Labs

As an ethical hacker, it is important to not only be able to test security systems but also understand that a good policy structure drives effective security. While this chapter discusses policy, laws, and rules of engagement, now is a good time to review the SANS Information Security Policy Templates page. These templates should be useful when you are helping an organization promote the change to a more secure setting.

Equipment Needed

A computer and Internet connection

Estimated Time: 15 minutes

Lab 1-1 Examining Security Policies

Step 1. Go to the SANS Information Security Policy Templates page located at https://www.sans.org/security-resources/policies.

Step 2. Click the **Network Security** category, and then click the **Acquisition Assessment Policy** hyperlink.

Step 3. Click the **PDF** hyperlink and review the Acquisition Assessment Policy. It defines responsibilities regarding corporate acquisitions and the minimum requirements of an acquisition assessment to be completed by the information security group.

Step 4. Return to the main Policy Templates page, click the **Old/Retired** category, click the **Risk Assessment Policy** hyperlink, click **PDF**, and review the template. This policy template defines the requirements and provides the authority for the information security team to identify, assess, and remediate risks to the organization's information infrastructure associated with conducting business.

Step 5. Return to the main Policy Templates page, click the **General** category, click the **Ethics Policy** hyperlink, click **PDF**, and review the template. This template discusses ethics and defines the means to establish a culture of openness, trust, and integrity in the organization.

Review Questions

1. You have been asked to perform a penetration test for a local company. You have had several meetings with the client and are now almost ready to begin the assessment. Which of the following is the document that would contain verbiage which describes what type of testing is allowed and when you will perform testing and limits your liabilities as a penetration tester?
   a. Nondisclosure agreement
   b. Rules of engagement
   c. Service-level agreement
   d. Project scope

2. Which of the following addresses the secrecy and privacy of information?
   a. Integrity
   b. Confidentially
   c. Availability
   d. Authentication

3. You are part of a pen testing team that has been asked to assess the risk of an online service. Management is concerned as to what the cost would be if there was an outage and how frequent these outages might be. Your objective is to determine whether there should be additional countermeasures. Given the following variables, which of the following amounts is the resulting annualized loss expectancy (ALE)?

   Single loss expectancy = $2,500

   Exposure factor = .9

   Annual rate of occurrence = .4

   Residual risk = $300

   a. $960
   b. $120
   c. $1,000
   d. $270

4. Who are the individuals who perform legal security tests while sometimes performing questionable activities?

   a. Gray hat hackers
   b. Ethical hackers
   c. Crackers
   d. White hat hackers

5. Which of the following is the most important step for the ethical hacker to perform during the pre-assessment?

   a. Hack the web server.
   b. Obtain written permission to hack.
   c. Gather information about the target.
   d. Obtain permission to hack.

6. Which of the following is one primary difference between a malicious hacker and an ethical hacker?
   a. Malicious hackers use different tools and techniques than ethical hackers use.
   b. Malicious hackers are more advanced than ethical hackers because they can use any technique to attack a system or network.
   c. Ethical hackers obtain permission before bringing down servers or stealing credit card databases.
   d. Ethical hackers use the same methods but strive to do no harm.

7. This type of security test might seek to target the CEO's laptop or the organization's backup tapes to extract critical information, usernames, and passwords.
   a. Insider attack
   b. Physical entry
   c. Stolen equipment
   d. Outsider attack

8. Which of the following best describes an attack that altered the contents of two critical files?
   a. Integrity
   b. Confidentially
   c. Availability
   d. Authentication

9. Which individuals believe that hacking and defacing websites can promote social change?
   a. Ethical hackers
   b. Gray hat hackers
   c. Black hat hackers
   d. Hactivists

10. After the completion of the pen test, you have provided the client with a list of controls to implement to reduce the identified risk. What term best describes the risk that remains after the controls have been implemented?
    a. Gap analysis
    b. Total risk
    c. Inherent risk
    d. Residual risk

11. This type of security test usually takes on an adversarial role and looks to see what an outsider can access and control.
    a. Penetration test
    b. High-level evaluation
    c. Network evaluation
    d. Policy assessment

12. Assume you performed a full backup on Monday and then an incremental backup on Tuesday and Wednesday. If there was on outage on Thursday, what would you need to restore operations?
    a. The full backup from Monday
    b. Both incremental backups from Tuesday and Wednesday
    c. The full backup from Monday and Wednesday's incremental backup
    d. The full backup from Monday and both incremental backups from Tuesday and Wednesday

13. During a security review you have discovered that there are no documented security policies for the area you are assessing. Which of the following would be the most appropriate course of action?
    a. Identify and evaluate current practices
    b. Create policies while testing
    c. Increase the level of testing
    d. Stop the audit

14. Your company performs PCI-DSS audits and penetration testing for third-party clients. During an approved pen test you have discovered a folder on an employee's computer that appears to have hundreds of credit card numbers and other forms of personally identifiable information (PII). Which of the following is the best course of action?
    a. Contact the employee and ask why they have the data.
    b. Make a copy of the data and store it on your local machine.
    c. Stop the pen test immediately and contact management.
    d. Continue the pen test and include this information in your report.

15. During which step of the incident response process would you be tasked with building the team, identifying roles, and testing the communication system?
    a. Containment
    b. Recovery
    c. Preparation
    d. Notification

16. Clark is a talented coder and as such has found a vulnerability in a well-known application. Unconcerned about the ethics of the situation, he has developed an exploit that can leverage this unknown vulnerability. Based on this information, which of the following is most correct?
    a. Clark is a suicide hacker.
    b. Clark has violated U.S. Code Section 1027.
    c. Clark has developed a zero day.
    d. Clark is a white hat hacker.

17. Your ethical hacking firm has been hired to conduct a penetration test. Which of the following documents limits what you can discuss publicly?
    a. Nondisclosure agreement
    b. PCI-DSS
    c. Memorandum of understanding
    d. Terms of engagement

18. Which of the following is a common framework applied by business management and other personnel to identify potential events that may affect the enterprise, manage the associated risks and opportunities, and provide reasonable assurance that objectives will be achieved?
    a. NIST SP 800-37
    b. Qualitative risk assessment
    c. PC-DSS
    d. Risk management framework

19. Your ethical hacking firm has been hired to conduct a penetration test. Which of the following documents limits the scope of your activities?
    a. Nondisclosure agreement
    b. PCI-DSS
    c. Memorandum of understanding
    d. Terms of engagement

20. Which of the following is a proprietary information security standard that requires organizations to follow security best practices and use 12 high-level requirements, aligned across six goals?
    a. SOX
    b. FISMA
    c. PCI-DSS
    d. Risk Management Framework

Suggested Reading and Resources

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh: EC-Council CEH certification details

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/: Top IT security breaches

http://searchnetworking.techtarget.com/tutorial/Network-penetration-testing-guide: Guide to penetration testing

https://www.rapid7.com/resources/how-to-respond-to-an-incident/: Incident response methodologies

http://securityaffairs.co/wordpress/49624/hacking/cyber-red-team-blue-team.html: Description of hacking teams including pen testers, blue teams, and red teams

http://www.hackerlaw.org/?page_id=55: U.S. hacker laws

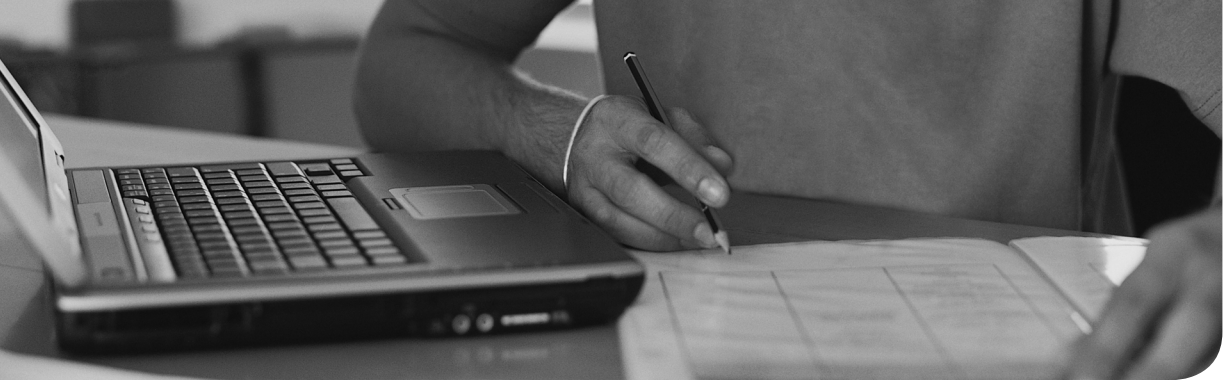
https://tools.ietf.org/html/rfc1087: Ethics and the Internet

https://www.owasp.org/index.php/Main_Page: The Open Web Application Security Project

https://www.owasp.org/index.php/Penetration_testing_methodologies: Various pen testing methodologies

http://blogs.getcertifiedgetahead.com/quantitative-risk-assessment/: Quantitative risk assessment

https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf: A guide to PCI-DSS



Index

Symbols

+.htr exploit, 315-316

Numbers

007 Shell
application layer tunneling, 222
Internet layer tunneling, 220
1G cell phones, 360-363
2G cell phones, 361
2.5G cell phones, 361
3DES (3Data Encryption Standard), symmetric encryption, 488, 491
3G cell phones, 361-362
4G cell phones, 361-362
18 USC 1028 (U.S. federal law), 361
18 USC 1029 (U.S. federal law), 361
802.11 standard and WLAN, 372

A

Abel password-extraction tool, 176
Absinthe, 345, 367
access
attacker's process
gaining access, 50
maintaining access, 51
cloud computing, 530
ethical hacker's process, 52
gaining, 18, 50
maintaining, 18, 51
physical access and Trojans, 209
ace locks, physical security, 452
ACK storms, 270
ACK values (active fingerprinting), 131
AckCmd, application layer tunneling, 222
active fingerprinting
ACK values, 131
bogus flag probe, 130
FIN probe, 130
fragmentation handling, 131
IPID sampling, 130
ISN sampling, 130
Nmap, 131-132
Queso, 131
TCP initial window, 130
TCP option, 131
type of service, 131
Winfingerprint, 132
Xprobe2, 132
active machines, identifying, 115
active sniffing, 252-253
ARP, 254
DAI, 266
poisoning, 255-257
spoofing, 255-257
DHCP
redirect attacks, 259
snooping, 259-260, 266
DNS, 261

MAC
flooding, *258-259*
spoofing, *260*
activity blockers, 232
activity profiling, DoS/DDoS attacks, 287
Acunetix Web Vulnerability Scanner, web server security, 320
AD (Active Directory), 155
Adleman, Leonard, 493
ADMutate, IDS evasion, 411
ADS (Alternate Data Streams), file hiding, 184
advertising, spyware and, 227
AES (Advanced Encryption Standard), symmetric encryption, 490-492
Agobot, 212. *See also* Phatbot
Aircrack-ng Suite, WLAN and, 383
AirSnare, 389
Airsnarf, WLAN and, 383
AirSnort, WEP cracking, 384
AirTraf, 384
Aitel, Dave, 317
alarms (delay), physical security, 451
ALE (Annual Loss Expectancy), risk assessment, 12-13
algorithms (encryption), 486-487
Allied Haxor Elite, Trojans and, 210
Amazon, memes, 200
Amitis Trojan, 212
amplification attacks (DNS), web server hacking, 310-311
analyzing
malware
dynamic analysis, *237-239*
static analysis, *234-236*
Microsoft Baseline Security Analyzer, web server security, 319
signatures (pattern-matching IDS) via Snort, 406
wireless traffic, WLAN and, 383
Anderson, James, 400
Android mobile device platform, 364-366
AndroRAT, 366
anomaly detection, IDS, 403
antennas, 377
antidetection routines (viruses), 200
antimalware
analyzing malware
dynamic analysis, *237-239*
static analysis, *234-236*
detecting malware, 228-231, 234
Registry, scanning for changes, 228
system file verification, 228
Tripwire, 228
antispyware, 227
antivirus programs
activity blockers, 232
EICAR and, 232
heuristic scanning programs, 232
integrity checking, 232
Jotti's malware scanning service, 232
online virus/malware scanning sites, 233
signature-scanning programs, 231
virus prevention plans, 230-231
AP (Access Points)
rogue AP, WLAN, 379
scanning, 116-117
Hping, *128*
idle scanning, *119*
IPID scanning, *120*
Nmap, *123-126*
SuperScan, *127*
TCP scanning, *118-119*
THC-Amap, *127*
UDP scanning, *122*
war driving, *129*
spoofing, WLAN, 379
unauthorized AP, WLAN, 379
API (Application Programming Interface), malware detection, 230

AppDetectivePRO, web application security, 339
appenders, viruses, 200
Apple
iOS mobile device platform, 366-367
Trojans and, 213
application layer
firewalls, 416, 422
tunneling and covert communication, 221-222
application layer (OSI model), 55
application layer (TCP model), session hijacking
client-side attacks, 272-274
man-in-the-browser attacks, 272
man-in-the-middle attacks, 272, 277
predicting session token ID, 271
session fixation attacks, 274
session replay attacks, 274
session sniffing, 271
application layer (TCP/IP model), 59
common ports/protocols table, 60-61
DHCP, 61
DNS, 62
FTP, 61
HTTP, 63
SMTP, 62
SNMP, 63
Telnet, 61
TFTP, 63
application-level attacks, 282-283
applications
mobile devices, sandbox issues, 363
rootkits, 182-183
testing (ethical hacking), 22
web applications, 298, 320
authentication attacks, 328-329
brute-force attacks, 329
buffer overflows, 326-327
CSRF, 323-324
dictionary attacks, 329
Direct OS commands, 327
DoS attacks, 327
Hex encoding, 328
hidden field attacks, 325-326
hybrid attacks, 329
injection flaws, 322
parameter/form tampering, 321-322
password cracking, 329-334
path traversal, 328
scanning tools, 338
securing, 337-339
session fixation, 327
SOAP injection, 327
Unicode encoding, 328
unvalidated input, 321
URL encoding, 328
URL obfuscation, 334-335
WAF, 335
web traffic interception, 335-337
XSS, 323
approval, getting (test plans), 27
Aramco (Saudi Arabian Oil Co.), permanent DoS attacks, 283
archived web pages, viewing, 92
Arduino microcontrollers, picking electronic locks, 454
area controls (physical security), 456, 459
Argo, 448
ARO (Annual Rate of Occurrence), risk assessment, 12-13
ARP (Address Resolution Protocol), 57
active sniffing, 254
Arpwatch, 266
DAI, 266
DNS and, 254
MAC addresses and, 254
poisoning, 255-257
Proxy ARP, 76
replies, 255

requests, 255
spoofing, 255-257
Arpwatch, 266
assessments
ethical hacker's process, 52
organizational security process, 52
risk, 12-13
assets, defined, 9
asymmetric encryption, 484, 487-488, 492
Diffie-Hellman, 494
ECC, 494-495
ElGamal, 494
RSA, 493
trapdoor functions, 493
AT&T, 17
ATBASH and the history of cryptography, 485
attachments (email)
social engineering and, 465
Trojans and, 209
attack surfaces (networks), mapping
automated mapping, 136-137
manual mapping, 135
attacker's process
access
gaining, 50
maintaining, 51
backdoors, 51
covering tracks, 51
enumeration, 49
escalation of privileges, 51
footprinting, 48
reconnaissance, 48
scanning, 49
auditing
cloud computing, 530
Elcomsoft Wireless Security Auditor, 384
organizational security process, 53
RATS, web application security, 338
web server security, 319
Auditpol, 181
Auernheimer, Andrew, 17
AUP (Acceptable Usage Policies), 469
Aurora exploits, 172
authentication
authentication attacks
cloud computing, 532
flood attacks, 381
biometric authentication
acceptance of, 167
CER, 166
FAR, 166
FRR, 166
strength of, 166
certificate-based authentication, 329
cryptography and, 485
de-authentication flood attacks, 381
EAP, WLAN and, 388
forms-based authentication, 329
Kerberos authentication, 168
Linux authentication, 177-180
message digest authentication, 328
OSA, WLAN, 378
passwords, 166
physical security, 462-463
SKA, 378
system testing (ethical hacking), 22
VPN, 485
weak authentication, 485
web application hacking
certificate-based authentication, 329
forms-based authentication, 329
message digest authentication, 328
web servers, password cracking, 314
Windows authentication, 168, 173-174
WordPress, 330
authenticity, 485
authority (social engineering), 464
authorization
ethical hacking, legality of, 22
third-party authorization attacks, 465

automated exploit tools, web server hacking, 316-317
automated password guessing, 167
availability (CIA triad), 8
Avatar rootkit, 182
Azazel rootkit, 183

B

backdoors, 207
attacker's process, 51
ICMP backdoors
application layer tunneling, 222
Internet layer tunneling, 220
undocumented firewalls, 423
backups, 8
differential backups, 11
documentation security
continuous backups, 449
differential backups, 448
full backups, 448
incremental backups, 449
full backups, 11
incremental backups, 11
bad passwords list, 331
bandwidth attacks, 280
Chargen, 281
DoS/DDoS attacks, 287
Fraggle, 281
BangleDoS, DDoS attacks, 286
banking systems, cryptography, 513
Banking Trojans, 535
banner grabbing, 420-421
HTTPrint, 134
Netcat, 134
Telnet, 133
web server hacking, 303-309
Base64, weak encryption, 512
Bash, 109
bastion hosts, 428
BCP (Business Continuity Plans), cloud computing, 531
Beast Trojan, 212
BeEF (Browser Exploitation Framework), web server hacking, 317
BER (Basic Encoding Rules), LDAP enumeration, 156
Berners-Lee, Tim, 302
best practices/standards, ethical hacker's process
NIST SP 800-15, 53
OCTAVE, 53
OSSTMM, 54
Big Brother, status monitoring, 98
binary numbers, converting IP addresses to, 424
BinText static malware analysis, 234
biometric access control (physical security, authentication), 462-463
biometric authentication
acceptance of, 167
CER, 166
FAR, 166
FRR, 166
strength of, 166
BitLocker, 509
black box (no-knowledge) testing, 13-14, 339
black hat hackers, defined, 17
black hole filtering, DoS/DDoS attacks, 287
BlackBerry mobile device platform, 367
BlackHole RAT (Remote-Access Trojans), 211
blackouts, 446
BlackWidow, web server hacking, 308
blind SQL injection attacks, 342
block ciphers (DES), 490
Blowfish, symmetric encryption, 488
BlueBug, 370
BlueScanner, 370
Bluesniff, 369

Bluetooth technology, 199, 368-369
bogons, NAT, 413
bogus flag probe (active fingerprinting), 130
bollards (physical security, facility controls), 460
bot herders, defined, 533
botnets, 524
Citadel botnets, 535
countermeasures
egress filtering, 538
IDS, 537
IPID analysis, 538
ISP and legitimate traffic, 538
mitigation, 538
TCP window size, 538
tracebacks, 538
TTL inspection, 538
crimeware kits, 535
DDoS attacks, 537
defined, 533
fast-flux botnets, 534
financial-based attacks, 536
form grabbers, 535
HTML injection, 535
installing, 536
IoT and, 537
IRC servers, 534
Mirai botnet, 12
money mules, 536
Silentbanker botnets, 535
SYN flood attacks, 538
TAN grabbers, 535
box, owning the, 172
Brain, history of viruses, 201
breaches (security), cloud computing, 531
British law, hacking and, 31
broadcast MAC addresses, 76
brownouts, 446
browsers (web)
application layer (TCP) hijacking, 272
browser bugs, Trojans and, 209
man-in-the-browser attacks, 272
brute-force attacks, 176, 329, 495, 512
Brutus encryption-cracking tool, 330, 514
Bryant, Darla, 425
BSQL Hacker, 344
BTCrack, 369
buffer overflows, 170-171
buffers, defined, 326
heap-based overflows, 326
SQL2.exe, 345
vulnerable C functions, 326-327
web application hacking, 326-327
Bugs and Kisses, 368
bump attacks, mobile devices, 363
bump keys, 452
Burger, Ralf, 201
BurnEye wrappers, 214
Burp Proxy
web application hacking, 321
web server hacking, 317
web traffic interception, 335
Burp Suite
cookies, 333
session hijacking, 276
web application hacking, 330
BYOD policies (mobile devices), 364

C

CA (Certificate Authority), PKI framework, 503
Caesar's cipher (ROT3) and the history of cryptography, 485
Caffrey, Aaron, 210
Cain and Abel, 257, 384
Cain password-extraction tool, 176
Camillagate, 360
cantennas, 377

Canvas automated exploit tool, 317
Capsa Network Analyzer, dynamic malware analysis, 237
Capt. Midnight, HBO hack, 359
capture filters, 264
capture-the-flag websites, 545
carriers (steganography), 498
CartoReso, mapping network attack surfaces, 136
catastrophic damage (natural disasters), 9
CBC (Cipher Block Chaining) mode (DES), 490
CCTV (Closed-Circuit TV) and area controls (physical security), 456, 459
CEH (Certified Ethical Hacker) exam preparation
hands-on activities, 545
suggested study plans, 545-546
cell phones
1G, 360-363
2G, 361
2.5G, 361
3G, 361-362
4G, 361-362
Cellebrite forensic tool, 363
cloning, 360
concerns
application sandbox issues, 363
bump attacks, 363
BYOD policies, 364
data confidentiality, 364
data disposal, 364
data exfiltration, 362
data leakage, 364
device support, 364
geolocation/location-based services, 362
jailbreaking, 363, 366-367
malware, 362
mixing personal/private data, 364
spoofing cell towers, 363
eavesdropping, 360
geotagging/location data, 456
managing, 368
platforms
Android, 364-366
BlackBerry, 367
iOS, 366-367
Windows Phone, 367
securing, 368
spread spectrum technologies, 361
subscription fraud, 360
triangulation/GPS tracking, 457-458
tumbling attacks, 360
Cellebrite mobile device forensic tool, 363
CER (Crossover Error Rates), biometric authentication, 166
certificate servers, PKI framework, 504
certificates
certificate-based authentication, web application hacking, 329
digital certificates, 502-503
signed certificates, PKI, 506
CFAA (Computer Fraud and Abuse Act), 17
CFB (Cipher Feedback) mode (DES), 491
Chaos Computer Club, history of viruses, 201
Chappell, Laura, 277
Chargen bandwidth attacks, 281
Charles, Prince, 360
chats, IRC and Trojans, 209
Chkrootkit, 184
chosen cipher-text attacks, 510
chosen plain-text attacks, 510
CIA triad
availability, 8
confidentiality, 7
integrity, 7

Cialdini, Robert, 464
CIPA (Children's Internet Protection Act), 34
cipher locks (programmable), physical security, 451
cipher text (encryption), 486, 510
circuit-level gateways, 416
Citadel botnets, 535
classifying data
cloud computing, 530
commercial data classification and social engineering, 471
government data classification and social engineering, 470-471
clickjacking, 316
client-side attacks
application layer (TCP) hijacking, 272-274
CSRF, 272
JavaScript and, 272-274
XSS, 272
cloning cell phones, 360
cloud computing, 524
authentication attacks, 532
concerns
access, 530
auditing, 530
data classification, 530
dedicated servers, 531
DR/BCP, 531
employee training, 530
encryption, 531
provider viability, 531
regulatory requirements, 530
security breaches, 531
shared servers, 531
SLA, 531
DBaaS model, 529
DDoS attacks, 532
deployment models, 528
DNS attacks, 532
hybrid clouds, 528
IaaS model, 528
MaaS model, 529
man-in-the-middle attacks, 532
PaaS model, 529
SaaS model, 529
security control layers, 533
session hijacking, 532
session riding, 532
side-channel attacks, 532
social engineering, 532
SQL injection, 532
wrapping attacks, 532
XSS, 532
clusters, 198
Code Red worm, 202
cognitive passwords, 469
Cohen, Fred, 201
collisions (hashing), 496
combination locks, physical security, 451
command injection, web application hacking, 322
commercial data classification and social engineering, 471
communication system testing (ethical hacking), 22
community clouds, 528
company directories, footprinting/scanning information-gathering process, 92
compliance regulations, 33-34
Computer Fraud and Abuse Act of 1984, 32
Computer Management Console (Microsoft), malware detection, 229
computer-based social engineering, 465
phishing, 466-467
SMiShing, 466
spear phishing, 466-467
whaling, 466

Conficker worm, 203
confidentiality, 470
CIA triad, 7
data
disclosure of, 9
mobile devices, 364
defined, 484
ethical hacking, legality of, 23
consistency (social engineering), 464
continuous backups, documentation security, 449
Control Point, 223
converting IP addresses to binary numbers, 424
cookies
Burp Suite, 333
Cookie Cadger, session hijacking, 276
CookieSpy, 333
password cracking, web application hacking, 333-334
cordless phones, 359
Core Impact automated exploit tool, 318
covering tracks, 18
attacker's process, 51
ethical hacker's process, 52
file hiding, 184-185
logs
clearing log files, 181
disabling, 181
rootkits, 182-184
covert communication, 194-195
covert channels, 115, 217
Pirate Bay, The, 223
storage channel attacks, 217
TCSEC and, 217
timing attacks, 217
tunneling
application layer, 221-222
Internet layer, 218-220
port redirection, 223-225
transport layer, 220-221
Cowden, Jim, 223
coWPAtty, 384
cracking
defined, 17
encryption
brute-force attacks, 512
Brutus tool, 514
chosen cipher-text attacks, 510
chosen plain-text attacks, 510
cipher-text only attacks, 510
CryptoTool, 514
Hashcat tool, 514
inference attacks, 509
John the Ripper, 514
known plain-text attacks, 510
man-in-the-middle attacks, 510
Poodlebleed, 511
replay attacks, 510
rubber hose attacks, 510
side-channel attacks, 510
THC-Hydra tool, 514
weak encryption, 512-513
passwords
Brutus tool, 514
cookies, 333-334
CryptoTool, 514
Hashcat tool, 514
John the Ripper, 514
Linux passwords, 180-181
preteen style, 332
SQLbf, 344
THC-Hydra tool, 514
web application hacking, 329-334
web server hacking, 314
Windows passwords, 175-177
software crackers, defined, 19
system crackers, defined, 19
Wi-Fi networks, 384
WPA encryption, 384

crimeware kits, 535
CRL (Certificate Revocation Lists), PKI framework, 503
crosscut shredders, documentation security, 448
cross-frame scripting, 316
Cryptcat, 221
crypters, Trojans and, 215-216
cryptography, 8, 481
authentication, 485
authenticity, 485
BitLocker, 509
brute-force attacks, 512
chosen cipher-text attacks, 510
chosen plain-text attacks, 510
cipher-text only attacks, 510
cloud computing, 532
defined, 484
EFS, 509
encryption
algorithms, 486-487
asymmetric encryption, 484, 487-488, 492-495
banking systems and, 513
brute-force attacks, 512
Brutus tool, 514
chosen cipher-text attacks, 510
chosen plain-text attacks, 510
cipher text, 486
cipher-text only attacks, 510
confidentiality, 484
cryptographic keys, 486
CryptoTool, 514
defined, 484, 487
EFS, 509
Hashcat tool, 514
history of, 487
inference attacks, 509
John the Ripper, 514
known plain-text attacks, 510
man-in-the-middle attacks, 510
plain text, 486
Poodlebleed, 511
public key encryption. See *asymmetric encryption*
replay attacks, 510
rubber hose attacks, 510
side-channel attacks, 510
SSLv3, 511
substitution ciphers, 486
symmetric encryption, 484-492
THC-Hydra tool, 514
weak encryption, 512-513
hashing
collisions, 496
digital certificates, 502-503
digital signatures, 496
hash values, 495
integrity, 485
MD5, 496
SHA-1, 496
steganography, 497-502
history of, 485-487
inference attacks, 509
integrity, defined, 485
IPsec, 508
known plain-text attacks, 510
LAN Turtles, 507
man-in-the-middle attacks, 510, 532
nonrepudiation, 485
PGP, 507
PKI
CA, 503
certificate servers, 504
CRL, 503
RA, 504
trust models, 504-506
X.509 standard, 504
PPTP, 509
replay attacks, 510
rubber hose attacks, 510

side-channel attacks, 510
S/MIME, 507
SSH, 507
SSL, 508
CryptoTool encryption-cracking tool, 514
CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), WLAN, 372
CSMA/CD Ethernet, WLAN, 372
CSRF (Cross-Site Request Forgery), 272, 323-324
CurrPorts, malware detection, 229
Cyber Security Enhancement Act of 2002, 32
cyberattacks, 9
cybercriminals, defined, 19
cyberterrorists, defined, 19
Cydia, 367
CypherX Crypter, 216

D

Daemen, Joan, 492
DAI (Dynamic ARP Inspection), 266
data
classifying
cloud computing, 530
commercial data and social engineering, 471
government data and social engineering, 470-471
confidentiality, mobile devices, 364
disposal, mobile devices, 364
exfiltration, mobile devices, 362
hiding, 206
leakage, mobile devices, 364
data link layer (Layer 2), OSI model, 56
databases
hacking, 298, 339
SQL injection attacks, 341-344
SQL server identification, 340-341
hierarchical database management system, 340
network database management system, 340
object-oriented database management system, 340
popular applications, 340-341
relational database management system, 340
testing (ethical hacking), 22
Datapipe, port redirection, 224
DBaaS (Database as a Service) cloud computing model, 529
DDoS (Distributed Denial of Service) attacks, 248, 284-285
botnets, 537
cloud computing, 532
countermeasures
activity profiling, 287
black hole filtering, 287
DoS prevention services, 287
egress filtering, 288-289
load balancing, 287
maximizing bandwidth, 287
mitigation, 289
throttling, 287
tracking attack sources, 289
tools
BangleDoS, 286
Dereil, 286
DoS HTTP, 286
HOIC, 286
LOIC, 286
Pandora, 286
TFN, 285
Trinoo, 286
web server hacking, 310
DDoS (Distributed DoS) attacks, 10
dedicated servers, cloud computing, 531
defacing websites, web server hacking, 313

Defense in Depth (physical security), 384-386, 463
delay alarms, physical security, 451
deleting data from mobile devices, 364
Dendroid, 366
deny all, 50
Der Spiegel, 183
Dereil, DDoS attacks, 286
DES (Data Encryption Standard), 489
block ciphers, 490
CBC mode, 490
CFB mode, 491
ECB mode, 490
OFB mode, 491
rounds, 490
stream ciphers, 490
symmetric encryption, 488
destruction of physical assets and physical security, 445
device locks, physical security, 452
DHCP (Dynamic Host Configuration Protocol), 61
redirect attacks, 259
snooping, 259-260, 266
dictionary attacks, 175
SQLDict, 344
web application hacking, 329
differential backups, 11, 448
Diffie, Dr. W
asymmetric encryption, 492-494
Diffie-Hellman encryption, 494
Dig, 111-112
digital certificates, 502-503
digital signatures, 496
digital watermarks, 502
Direct OS commands, web application hacking, 327
directories (company), footprinting/scanning information-gathering process, 92
directory (path) traversal, web server hacking, 311-313
DIRECTV, 358-359
disaster recovery, 8, 531
disasters (natural), 9
disclosure of confidential information, 9
disgruntled employees as hackers, 18
DISH Network, 358-359
display filters, 264
DLL injection, 169, 175
DMZ (Demilitarized Zones), 136, 416-417, 428
DNS (Domain Name Service), 62
application layer tunneling, 221
ARP and, 254
attacks
amplification attacks, 310-311
cloud computing, 532
server hijacking, 310-311
cache poisoning, 261
DNSSEC, 266
enumeration, 107-111, 163
IPv4 DNS records/types, 108-109
queries, 105
reverse DNS lookups, 267
spoofing, 261
web server hacking, 310-311
zone transfers, 163
dnscat, 221
DNSChanger, 213
DNSSEC (DNS Security Extensions), DNS spoofing, 266
"do no harm," legality of ethical hacking, 24
documentation
footprinting information-gathering process, 91
scanning information-gathering process, 91
security
backups, 448-449
shredders, 448

dogs (physical security, facility controls), 460
domain proxies, 107
doors (physical security, area controls), 456
DoS
IDS and, 410
testing (ethical hacking), 21
DoS (Denial of Service) attacks, 8, 206, 248
application-level attacks, 283
authentication flood attacks, 381
bandwidth attacks, 280-281
booter sites, 279
countermeasures, 288
activity profiling, 287
black hole filtering, 287
DoS prevention services, 287
egress filtering, 289
load balancing, 287
maximizing bandwidth, 287
mitigation, 289
throttling, 287
tracking attack sources, 289
DDoS attacks, 10, 284
botnets, 537
cloud computing, 532
countermeasures, 287-289
tools, 285-286
web server hacking, 310
de-authentication flood attacks, 381
equipment destruction attacks, 381
hacktivism and, 280
ICMP attacks, 282
methodology of, 278
network-jamming attacks, 381
peer-to-peer attacks, 282
permanent DoS attacks (phlashing attacks), 283-284
program-level attacks, 282-283
Smurf attacks, 282
SYN flood attacks, 281
web application hacking, 327
web server hacking, 310
WLAN, 380-381
DoS HTTP, DDoS attacks, 286
double decode directory (path) traversal, 312
Double DES (3Data Encryption Standard), symmetric encryption, 491
DR/BCP (Disaster Recovery/Business Continuity Plans), cloud computing, 531
DroidSheep, 366
Dropbox, 7
droppers, 227
Dsniff, 265
DSSS (Direct-Sequence Spread Spectrum), 373
dual-homed host firewalls, 417
DumpSec, LDAP enumeration, 158
dumpster diving, 48, 164, 448
Dupuis, Clement, 387
dynamic malware analysis, 237

E

E-banking, 206
EAP (Extensible Authentication Protocol), WLAN and, 388
earthquakes and physical security, 445
eavesdropping
1G cell phones, 360
WLAN, 378
eBLASTER, 226
ECB (Electronic Code Book) mode (DES), 490
ECC (Elliptic Curve Cryptography), 494-495
echo replies, 115
echo requests, 115
Economic Espionage Act of 1996, 33
EDGAR database, footprinting/scanning information-gathering process, 97

EFS (Encrypting File System), 509
egress filtering
botnets and, 538
DoS/DDoS attacks, 289
EICAR (European Institute of Computer Antivirus Research), 232
Elcomsoft Wireless Security Auditor, 384
Electronic Communications Privacy Act, 32, 470
electronic locks, 454
ElGamal encryption, 494
email
attachments
social engineering and, 465
Trojans and, 209
phishing attacks, 467
SMTP, 60
employees
cloud computing training, 530
disgruntled employees, as hackers, 18
hiring/termination policies and social engineering, 469
ID badges, 469
NDA, 469
physical security, 447
searches, footprinting/scanning information-gathering process, 94-97
encapsulation, TCP/IP model, 58
encryption
algorithms, 486-487
asymmetric encryption, 484, 487-488, 492
Diffie-Hellman, 494
ECC, 494-495
ElGamal, 494
RSA, 493
trapdoor functions, 493
banking systems and, 513
cipher text, 486
cloud computing, 531
confidentiality, defined, 484
cracking
brute-force attacks, 512
Brutus tool, 514
chosen cipher-text attacks, 510
chosen plain-text attacks, 510
cipher-text only attacks, 510
CryptoTool, 514
Hashcat tool, 514
inference attacks, 509
John the Ripper, 514
known plain-text attacks, 510
man-in-the-middle attacks, 510
Poodlebleed, 511
replay attacks, 510
rubber hose attacks, 510
side-channel attacks, 510
THC-Hydra tool, 514
weak encryption, 512-513
cryptographic keys, 486
defined, 484, 487
EFS, 509
history of, 487
plain text, 486
public key encryption. *See* asymmetric encryption
session hijacking, 277
sniffers and, 263
SSLv3, breaking via Poodlebleed, 511
substitution ciphers, 486
symmetric encryption, 484-486
3DES, 488, 491
AES, 490-492
Blowfish, 488
DES, 488-491
Double DES, 491
key distribution, 489
RC, 492
RC4, 488, 492
RC5, 488, 492
RC6, 488
Rijndael, 488, 492
SAFER, 488

Videocipher II satellite encryption, 358
weak encryption
Base64, *512*
Uuencode, *513*
XOR, *512*
web server hacking, 316
web server security, 319
WPA encryption, cracking, 384
Enigma, history of cryptography, 487
enrollment periods (biometric access control), 463
enum4linux command, Linux enumeration, 162
enumeration, 18
attacker's process, 49
defined, 148, 152
DNS
enumeration, *163*
footprinting/scanning information-gathering process, *107-111*
LDAP enumeration, 155-160
Linux enumeration, 161-162
NTP enumeration, 162-163
SMTP enumeration, 163
SNMP enumeration
Network Performance Monitor, *161*
snmpwalk, *160*
SNScan, *161*
UNIX enumeration, 161-162
web server hacking, 303-309
Windows enumeration, 152-155
equipment
destruction attacks, 381
failure and physical security, 445
equipment controls (physical security), 445
delay alarms, *451*
fax machines, *454-455*
locks, *449-454*
visibility shields, *451*
error-based SQL injection attacks, 342
escalation of privilege
attacker's process, 51
DLL injection, 169
horizontal escalation, 172
vertical escalation, 172
EtherFlood, MAC flooding, 258
Ethernet, WLAN, 372
ethical hacking
application testing, 22
assessments, 52
authentication system testing, 22
communication system testing, 22
covering tracks, 52
database testing, 22
defined, 17-19
"do no harm," 24
DoS testing, 21
external penetration testing, 21
gaining access, 52
information gathering, 21
internal penetration testing, 21
legality of
authorization, *22*
confidentiality, *23*
defining ethics, *23*
NDA, *22*
maintaining access, 52
modes of, 21-22
network gear testing, 21
NIST SP 800-15, 53
OCTAVE, 53
OSSTMM, 54
permissions, 52
physical security testing, 22
reconnaissance, 52
reports, 28-29, 52
scanning, 52
security testing, 53-54
skill requirements, 20-21

standards/practices, 53-54
stolen equipment attacks, 22
wireless network testing, 22
ethics, 23, 29-30
Ettercap
ARP spoofing, 257
session hijacking, 274-277
European Union Privacy Law, 470
evil-twin attacks, 379. *See also* man-in-the-middle attacks
exam preparation
hands-on activities, 545
suggested study plans, 545-546
ExploitDB website, identifying web server vulnerabilities, 309
exploiting vulnerabilities, 169
buffer overflow, 170-171
StickyKeys, 170
exploits
+.htr exploit, 315-316
automated exploit tools, web server hacking, 316-317
defined, 11-12
exploit database website, 50
Unicode Web Traversal, 203
web resources, 50
external penetration testing (ethical hacking), 21
eye-recognition systems (biometric access control), 463

F

Facebook, dangers of, 97
FaceNiff, 366
facial scans (biometric access control), 462
facility controls (physical security)
bollards, 460
dogs, 460
fences, 458-459
guards, 459
lighting, 459
mantraps, 460
turnstiles, 460
failover equipment, 8
failure (equipment) and physical security, 445
FakeToken, 366
false positives, IDS and, 409
Family Education Rights and Privacy Act, 470
FAR (False Acceptance Rates)
biometric access control, 463
biometric authentication, 166
fast infections, 199
fast-flux botnets, 534
faults (power anomalies), 446
fax machines, physical security, 454-455
Federal Sentencing Guidelines of 1991, 33
fences (physical security, facility controls), 458-459
FGdump password-extraction tool, 175
FHSS (Frequency-Hopping Spread Spectrum), 373
files
hiding, 184-185
infections, 198
injection, web application hacking, 322
system files, verifying, 228
filetype (Google search term), 99
FIN probe (active fingerprinting), 130
financial-based botnet attacks, 536
finger command, Linux enumeration, 162
finger-printing layer, BurnEye wrappers, 214
fingerprinting
active fingerprinting
ACK values, 131
bogus flag probe, 130
FIN probe, 130

fragmentation handling, *131*
IPID sampling, *130*
ISN sampling, *130*
Nmap, *131-132*
Queso, *131*
TCP initial window, *130*
TCP options, *131*
type of service, *131*
Winfingerprint, *132*
Xprobe2, *132*
biometric access control, 462
default ports/services, 133
open services, 133-135
passive fingerprinting, 129
fire
physical security, 444
prevention/detection/suppression (physical security), 461
Firesheep, session hijacking, 276
firewalking, 412, 419
firewalls, 396, 412
application layer firewalls, 416
bypassing
application layer, *422*
HTTP, *422*
HTTPS, *422*
ICMP, *422*
inside attacks, *423*, *427*
internal hacking, *423*, *427*
Internet layer, *421*
misconfigured firewalls, *423*
physical security, *423*
poor policies, *423*
proxy servers, *423*
secondary connections, *423*
social engineering, *423*
syslog services, *424*
TFTP, *425*
transport layer, *422*
tunneling, *423*
UDP, *422*
undocumented firewalls, *423*
circuit-level gateways, 416
connecting, 424
DMZ, 416-417
dual-homed host firewalls, 417
ethical hacker skill requirements, 20
identifying
banner grabbing, *420-421*
firewalking, *419*
port scanning, *417-418*
NAT, 413
packet filters, 414-417
screened host firewalls, 417
stateful inspection firewalls, 416-417
WAF, 335
FISMA (Federal Information Security Management Act), 32
Flame virus, 199
Flappy Bird, 468
Flawfinder, web application security, 338
Flexilis, BlueSniper rifle, 369
flood attacks
authentication flood attacks, 381
de-authentication flood attacks, 381
IDS and, 408
MAC flooding, 258-259
floods (natural disasters) and physical security, 444
FOCA, 101
footprinting, 18
active machines, identifying, 115
AP scanning, 116-117
Hping, *128*
idle scanning, *119*
IPID scanning, *120*
Nmap, *123-126*
SuperScan, *127*
TCP scanning, *118-119*
THC-Amap, *127*

UDP scanning, *122*
war driving, *129*
attacker's process, 48
fingerprints
active fingerprinting, *130-132*
default ports/services, *133*
open services, *133-135*
passive fingerprinting, *129*
information-gathering process, 90
DNS enumeration, *107-111*
documentation, *91*
EDGAR database, *97*
employee/people searches, *94-97*
Google hacking, *98-103*
job boards, *93-94*
organization websites, *91-93*
registrar queries, *104-107*
Usenet, *103-104*
mapping attack surfaces
automated mapping, *136-137*
manual mapping, *135*
network ranges, determining, 112-114
port scanning, 116-117
Hping, *128*
idle scanning, *119*
IPID scanning, *120*
Nmap, *123-126*
port knocking, *128*
SuperScan, *127*
TCP scanning, *118-119*
THC-Amap, *127*
UDP scanning, *122*
war driving, *129*
forensics
Cellebrite mobile device forensic tool, 363
man-in-the-middle attacks, 276
forms
authentication, 329
form grabbers, botnets, 535
form/parameter tampering, 321-322
web application hacking, 321-322
Fournier, Rodney, 93
FPipe, port redirection, 225
FQDN (Fully Qualified Domain Names), 62
Fraggle bandwidth attacks, 281
fragmentation
active fingerprinting, 131
IP, 68-70
overlapping fragmentation attacks, 70
fraud, U.S. federal laws, 31-32
free speech and the Internet, 93
freeware, Trojans and, 209
FRR (False Rejection Rates)
biometric access control, 463
biometric authentication, 166
FTP (File Transfer Protocol), 61, 425
FTP Trojans, 206
full backups, 11, 448
full-knowledge (white box) testing, 14
fuzzing, 339

G

gaining access, 18
Galbraith, Bryce, 234
geolocation/location-based services, mobile devices, 362
geotagging/location data (physical security), 456
GFI LanGuard, web server security, 318-320
Gh0st RAT (Remote-Access Trojans), 212, 467
GHDB (Google Hacking Database), 101
Ghost Keylogger, 226
GhostNet spear phishing attack, 467
GID (Group ID), 154
Gilmore, John, 511
Gingrich, Newt, 360
GLBA (Gramm-Leach-Bliley Act), 33

goals, test plans, 26-27
Gonzalez, Albert, 339
Google
Android mobile device platform, 364-366
Google Groups, 103
hacking, 98-103
search terms, 99
government data classification and social engineering, 470-471
GPS (Global Positioning System)
mapping and WLAN, 383
tracking/smartphone triangulation, 457-458
grabbing banners, 303-309, 420-421
gray box (partial-knowledge) testing, 14
gray hat hackers, defined, 17
Green, Julian, 210
guards (physical security, facility controls), 459
guessing passwords, 165-167

H

hackers, defined, 16
black hat hackers, 17
cybercriminals, 19
cyberterrorists, 19
disgruntled employees, 18
ethical hackers, 17-21
gray hat hackers, 17
phreakers, 18
script kiddies, 18
software hackers, 19
suicide hackers, 17
system hackers, 19
white hat hackers, 17
hacking laws, evolution of, 31
hacktivism, DoS attacks, 280
hacktivists, 30
Hamster, session hijacking, 276
hand geometry (biometric access control), 462
hardware keyloggers, 225-226
Hashcat encryption-cracking tool, 514
hashing, 167
collisions, 496
digital certificates, 502-503
digital signatures, 496
hash values, 495
integrity, defined, 485
MD5, 496
SHA-1, 496
steganography
carriers, 498
defined, 497
digital watermarks, 502
laser printers, 501
operation of, 498-499
tools, 499-502
Have I Been Pwned? website, 165
Havij, SQL injection, 345
HBO, 359
headers
ICMP, 218
IPv4, 67
IPv6, 67
TCP headers, 117-118
heap spraying, 172
heap-based buffer overflows, 326
Heartbleed, 508
Hell Raiser, 213
Hellman, Dr. M.E.
asymmetric encryption, 492-494
Diffie-Hellman encryption, 494
help desk procedures and social engineering, 469
Hennard, George, 460
heuristic scanning antivirus programs, 232
Hex encoding, web application hacking, 328
hidden field attacks, web application hacking, 325-326

hiding
data, 206
files, 184-185
HIDS (Host-based IDS), 400
hierarchical database management system, 340
hierarchical trust model (PKI), 505
high-level assessments/audits (Level I assessments), security testing, 15
hijacking
DNS servers, 310-311
sessions, 56, 248, 267
application layer (TCP) hijacking, 271-277
cloud computing, 532
encryption, 277
preventing, 277
transport layer (TCP) hijacking, 267-270
HIPAA (Health Insurance Portability and Accountability Act), 33, 470
hiring/termination policies and social engineering, 469
Hitprint, web server hacking, 308-309
hoax viruses, 199
HOIC (High Orbit Ion Cannon), DDoS attacks, 286
honeynets, 428
honeypots, 428
defined, 396
detecting, 430-431
types of, 429-430
hopcount ramping (firewalking), 419
horizontal privilege escalation, 172
host routing, WLAN, 380
Hping
AP scanning, 128
firewalls, port scanning, 418
port scanning, 128
HTML (Hypertext Markup Language)
HTML injection, botnets, 535
web servers, 302
HTTP (Hypertext Transfer Protocol), 63
application layer tunneling, 221
DoS HTTP, DDoS attacks, 286
firewalls, bypassing, 422
GET requests, session hijacking, 276
response splitting, web server hacking, 314
tunneling, 223, 411
web servers, 302
HTTPrint, banner grabbing, 134
HTTPS (HTTP over SSL)
application layer tunneling, 221
firewalls, bypassing, 422
Hunt, session hijacking, 276
hurricanes (tropical storms) and physical security, 444
hybrid attacks
password attacks, 175
web application hacking, 329
Hyena GUI tool, LDAP enumeration, 158

I

IaaS (Infrastructure as a Service) cloud computing model, 528
IANA (Internet Assigned Numbers Authority), 104, 117
IBM Internet Scanner, web server security, 320
ICANN (Internet Corporation for Assigned Names and Numbers), 104
IceSword, malware detection, 229
ICMP (Internet Control Message Protocol), 70-71
backdoors
application layer tunneling, 222
Internet layer tunneling, 220

firewalls, bypassing, 422
headers, 218
ICMPSend
application layer tunneling, 222
Internet layer tunneling, 220
ping command and, 218
Smurf attacks, 282
traceroute, 72-74
IDA Pro static malware analysis, 234
identifying
active machines, 115
firewalls
banner grabbing, 420-421
firewalking, 419
port scanning, 417-418
phishing attacks, 467
SQL servers, database hacking, 340-341
web server vulnerabilities, 309
identity, Windows security, 154, 158
idle scanning, 119-121
IDP (Intrusion Detection Prevention), 412
IDS (Intrusion Detection Systems), 396
anomaly detection, 403
botnets and, 537
components of, 400
evasion
ADMutate, 411
DoS, 410
false positives, 409
flooding, 408
HTTP tunneling, 411
insertion attacks, 408
invalid RST, 410
Mendax, 411
Nessus, 411
NIDSbench, 411
obfuscation, 410
post-connection SYN, 410
pre-connection SYN, 410
session splicing, 408-409
shellcode attacks, 409
tools, 411-412
HIDS, 400
NIDS, 400
pattern-matching IDS (signatures), 403-406, 410
port scans, 49
protocol-decoding IDS, 403
Snort, 410
components of, 404
keywords, 405
rules, 405-406
signature analysis, 406
true/false matrix, 401
tuning, 401-402
WLAN and, 389
IFrame attacks, 274
IIS (Internet Information Services)
IIS Lockdown, 319
vulnerabilities, 315-316
web servers
hacking, 315-316
security, 319
WebDAV, 315
Iliad, The, 205
IM (Instant Messaging), Trojans and, 209
ImageHide stenographic tool, 500
implementation, organizational security process, 52
important user attacks, 464
in person attacks, 465
incident response process, 16
incremental backups, 11, 449
infection routines (viruses), 200
inference attacks, 509

information-gathering
ethical hacking, 21
footprinting/scanning, 90
DNS enumeration, *107-111*
documentation, *91*
EDGAR database, *97*
employee/people searches, *94-97*
Google hacking, *98-103*
job boards, *93-94*
organization websites, *91-93*
registrar queries, *104-107*
Usenet, *103-104*
injection attacks (SQL), 339-344
injection flaws, web application hacking, 322
inrushes (power anomalies), 446
insertion attacks, IDS and, 408
insider attacks, bypassing firewalls, 423, 427
inSSIDer, Wi-Fi network discovery, 382
integrity
checking, 232
CIA triad, 7
defined, 485
intercepting web traffic, web application hacking, 335-337
internal hacking, bypassing firewalls, 423, 427
internal penetration testing (ethical hacking), 21
Internet, free speech and, 93
Internet layer
firewalls, bypassing, 421
tunneling, covert communication and, 218-220
Internet layer (TCP/IP model), 66
ICMP, 70-74
IP
fragmentation, *68-70*
source routing, *72*
IPv4
addressing, *67-68*
headers, *67*
IPv6 headers, 67
traceroute, 72-74
intitle (Google search term), 99
inurl (Google search term), 99
invalid RST, IDS and, 410
iOS mobile device platform, 366-367
IoT (Internet of Things)
botnets and, 537
physical security and, 447
Shodan website, 447
IP (Internet Protocol)
addresses, converting to binary numbers, 424
fragmentation, 68-70
IPv4
addressing, *67-68*
DNS records/types, *108-109*
headers, *67*
IPv6 headers, 67
overlapping fragmentation attacks, 70
source routing, 72
IPC$ share, 156
IPID (Internet Protocol ID)
ACK scans, 122
botnets and, 538
FTP Bounce scans, 122
open port, 120
port closed, 121
RPC scans, 122
sampling (active fingerprinting), 130
Window scans, 122
IPIP, 56
IPsec (IP Security), 508
IRC (Internet Relay Chats)
servers, botnets, 534
Trojans and, 209

iris recognition (biometric access control), 463
ISAPI DLL buffer-overflow attacks, 315
ISN (Initial Sequence Number) sampling (active fingerprinting), 130
ISO/IEC 27001:2013, 33
ISP (Internet Service Providers), botnets and legitimate traffic, 538

J

JAD (Java Application Descriptor) files, BlackBerry exploits, 367
jailbreaking mobile devices, 363, 366-367
jammers, network-jamming attacks, 381
Jaschan, Sven, 203
Java watering-hole attacks, 172
JavaScript, client-side attacks, 272-274
job boards, footprinting/scanning information-gathering process, 93-94
John the Ripper
encryption-cracking, 514
password-extraction, 176, 180-181
Jotti's malware scanning service, 232
Jumper RAT (Remote-Access Trojans), 212

K

Kali Linux, 137, 545-546
Kalman, Steve, 290
KerbCrack, 168
Kerberos
authentication, 168
Windows authentication, 173-174
kernel rootkits, 182-183
KeyGhost keylogger, 169, 226
keyloggers, 194
eBLASTER, 226
Ghost Keylogger, 226
hardware keyloggers, 225-226
KeyGhost, 168, 226
KeyStrokeSpy, 169
software keyloggers, 226
Spy PC Keylogger, 226
Veriato Investigator, 226
web server security, 319
keys
cryptographic keys (encryption), 486
public key encryption. *See* asymmetric encryption
symmetric encryption key distribution, 489
KeyStrokeSpy, keylogger, 169
Kismet, 384, 389
Kmart, free speech and the Internet, 93
known plain-text attacks, 510
Kocher, Paul, 511

L

L0phtCrack password-extraction tool, 175-176
LAN (Local Area Networks)
LAN Turtles, 507
WLAN, 370
802.11 standard, 372
ad hoc mode, 371
AP spoofing, 379
cantennas, 377
cracking/compromising Wi-Fi networks, 384
CSMA/CA, 372
CSMA/CD Ethernet, 372
defense in depth concept, 384-386
DoS attacks, 380-381
EAP, 388
eavesdropping, 378
evil-twin attacks, 379
frequencies, 372
GPS mapping, 383
host routing, 380
IDS, 389
infrastructure mode, 371

launching wireless attacks, *383*
misuse detection, *389*
OSA, *378*
rogue/unauthorized AP, *379*
security, *373-375*, *384-389*
site surveys, *386-387*
spread spectrum technology, *372*
SSID, *371*, *385*
threats, *376-381*
war chalking, *376*
war driving, *377*
war flying, *377*
WEP, *373-375*
Wi-Fi network discovery, *381-382*
wireless traffic analysis, *383*
WPA, *375*
WPA2, *375*
Land attacks, 283
laser printers and steganography, 501
LCP password-extraction tool, 176
LDAP (Lightweight Directory Access Protocol)
AD, 155
enumeration, 155-160
LDAP injection, web application hacking, 322
Ldp, LDAP enumeration, 159
Leaked Source website, 165
leaking data, mobile devices, 364
least privilege, principle of, 61
legality
British law, 31
compliance regulations, 33-34
ethics, 29-30
hacking laws, evolution of, 31
ISO/IEC 27001:2013, 33
PCI-DSS, 34
Trojans and, 210
U.S. federal laws, 30
CIPA, *34*
Computer Fraud and Abuse Act of 1984, *32*
Cyber Security Enhancement Act of 2002, *32*
Economic Espionage Act of 1996, *33*
Electronic Communication Privacy Act, *32*
Federal Sentencing Guidelines of 1991, *33*
FISMA, *32*
GLBA, *33*
HIPAA, *33*
SOX Act, *33*
U.S. Code Title 18, *31*
USA PATRIOT Act of 2001, *32*
Let Me Rule RAT (Remote-Access Trojans), 212
lighting (physical security, facility controls), 459
liking (social engineering), 464
link (Google search term), 99
LINNT, 173
Linux
authentication, 177-180
enumeration, 161-162
ethical hacker skill requirements, 20
Kali Linux, 137
passwords, 177-181
ping capture, 219
LKM (Loadable Kernel Module), rootkits and, 182
LLC (Logical Link Control) layer, data link layer (OSI model), 57
LM, Windows authentication, 173-174
load balancing, DoS/DDoS attacks, 287
Locard's exchange principle, 181
location data/geotagging (physical security), 456
location-based services/geolocation, mobile devices, 362
locks, physical security, 449
ace locks, 452

bypassing locks
bump keys, 452
lock picking, 452-454
scrubbing locks, 452
combination locks, 451
device locks, 452
electronic locks, 454
grades of locks, 451
master key locks, 452
picking locks, 452-454
programmable cipher locks, 451
tumbler locks, 450
warded locks, 450
logs
clearing log files, 181
disabling, 181
LOIC, DDoS attacks, 286
Loki, application layer tunneling, 222
LoriotPro, 114
LSASS (Local Security Authority Server Service), 155, 167

M

MaaS (Monitoring as a Service) cloud computing model, 529
MAC (Media Access Control) layer, data link layer (OSI model), 57
MAC addresses, 75
ARP and, 254
broadcast MAC addresses, 76
flooding, 258-259
malware prevention, 237
multicast MAC addresses, 76
spoofing, 260
unicast MAC addresses, 76
MAC filtering, WLAN and, 386
MacDougall, John R., 359
Macof, MAC flooding, 259
macro infections, 198
magnetic strip cards, authentication (physical security), 462
mainframes, ethical hacker skill requirements, 20
maintaining access, 18
malware, 9
analyzing
dynamic analysis, 237-239
static analysis, 234-236
antimalware, 234-239
detecting malware, 228-231, 234
Registry, scanning for changes, 228
system file verification, 228
Tripwire, 228
covert communication, 194-195
application layer tunneling, 221-222
covert channels, 217
Internet layer tunneling, 218-220
Pirate Bay, The, 223
port redirection, 223-225
storage channel attacks, 217
TCSEC and, 217
timing attacks, 217
transport layer tunneling, 220-221
detecting, 228-231, 234
keyloggers, 194, 225-226
mobile devices, 362
ransomware, 203
spyware, 198, 227
Trojans, 194
Apple products and, 213
backdoors, 207
browser bugs, 209
communication methods, 206-208
crypters, 215-216
data hiding, 206
delivery mechanisms, 208-210
distributing, 213-216
DoS attacks, 206
E-banking, 206
effects of, 210
email attachments, 209

freeware, *209*
FTP, *206*
goals of, *208*
IM, *209*
infection mechanisms, *208-210*
IRC, *209*
legal issues, *210*
P2P networks, *209*
packers, *214-216*
physical access as delivery method, *209*
poison apple attacks, *207*
ports, *206-208*
proxies, *206*
RAT, *206*, *211*
security software disablers, *206*
social engineering and, *213*
Tini, *211*
tools, *210-213*
types of, *205-206*
Visual Basic Trojans, *212*
watering holes, *209*
wrappers, *213-216*
viruses, 194, 197
antidetection routines, *200*
antivirus programs, *230-233*
appenders, *200*
Brain, *201*
clusters, *198*
components of, *200*
fast infections, *199*
file infections, *198*
Flame, *199*
history of, *201*
hoaxes, *199*
infection routines, *200*
macro infections, *198*
master boot record infections, *198*
Melissa, *202*
memes, *199-200*
multipartite viruses, *199*
payloads, *200*
polymorphic viruses, *199*
prependers, *200*
prevention plans, *230-231*
ransomware, *203*
search routines, *200*
sparse infections, *199*
tools, *204-205*
transmission methods, *198-199*
trigger routines, *200*
types of, *198-200*
well-known viruses, *202-203*
worms, 194, 197, 202-203
man-in-the-browser attacks, application layer (TCP) hijacking, 272
man-in-the-middle attacks, 510. *See also* evil-twin attacks
application layer (TCP) hijacking, 272, 277
cloud computing, 532
POODLE attacks, 316
web server hacking, 313
man-made threats to physical security, 445
managing
cell phones (smartphones), 368
databases, 340
mobile devices, 368
projects, ethical hacker skill requirements, 21
risk, backups, 11
mantraps (physical security, facility controls), 460
mapping
networks
attack surfaces, *135-137*
subnets and, *112*
SolarWinds Network Topology Mapper, 136
Marathon Tool, SQL injection testing, 345

masquerading attacks, 465
master boot record infections, 198
master key locks, physical security, 452
Matlego, 101
Matrix, The, 123
maximizing bandwidth, DoS/DDoS attacks, 287
Mays, George, 377
McAfee Rootkit Detective, 184
MD5 hashing algorithm, 496
Melissa virus, 202
memes, virus transmission, 199-200
memory tables, 546
Mendax, IDS evasion, 411
Merdinger, Shawn, 103
message digest authentication, web application hacking, 328
Metasploit, 316
methodologies
attacker's methodologies
backdoors, 51
covering tracks, 51
enumeration, 49
escalation of privileges, 51
footprinting, 48
gaining access, 50
maintaining access, 51
reconnaissance, 48
scanning, 49
ethical hacker's methodologies
assessments, 52
covering tracks, 52
gaining access, 52
maintaining access, 52
NIST SP 800-15, 53
OCTAVE, 53
OSSTMM, 54
permissions, 52
reconnaissance, 52
reporting, 52
scanning, 52
security testing, 53-54
standards/practices, 53-54
organizational security
assessments, 52
auditing, 53
implementation, 52
policy development, 52
training, 52
OSSTMM, 23
MIC (Message Integrity Check), 375
Microsoft /GS, web application security, 338
Microsoft Baseline Security Analyzer, web server security, 319
Microsoft Computer Management Console, malware detection, 229
Mimikatz, 167
Mirai botnet, 12
mirroring, 252
misconfigured firewalls, bypassing, 423
misconfiguring web servers, web server hacking, 313
mitigation
botnets and, 538
DoS/DDoS attacks, 289
Mitnick, Kevin, 92
mobile devices
1G, 360-363
2G, 361
2.5G, 361
3G, 361-362
4G, 361-362
Cellebrite forensic tool, 363
cloning, 360
concerns
application sandbox issues, 363
bump attacks, 363
BYOD policies, 364
data confidentiality, 364
data disposal, 364

data exfiltration, *362*
data leakage, *364*
device support, *364*
geolocation/location-based services, *362*
jailbreaking, *363*, *366-367*
malware, *362*
mixing personal/private data, *364*
spoofing cell towers, *363*
eavesdropping, 360
geotagging/location data, 456
managing, 368
platforms
Android, *364-366*
BlackBerry, *367*
iOS, *366-367*
Windows Phone, *367*
securing, 368
spread spectrum technologies, 361
subscription fraud, 360
triangulation/GPS tracking, 457-458
tumbling attacks, 360
Mognet, Wi-Fi network discovery, 382
money mules, botnets and, 536
monitoring status, Big Brother, 98
Moore's Law, 490
Morphine packers/crypters, 216
Morris Jr., Robert T, 202
MoSucker Trojan, 212
Movie Channel, The, 359
MP3Stego stenographic tool, 499
MTBF (Mean Time Between Failure), 445
MTTR (Mean Time To Repair), 445
multicast MAC addresses, 76
multipartite viruses, 199
MyDoom worm, 203

N

N-Stalker, web application security, 339
NAT (Network Address Translation), 413
natural disasters, 9
natural threats to physical security, 444-445
Navajo language, history of cryptography, 487
NDA (Nondisclosure Agreements), 22, 469
Necurs rootkit, 183
Nessus
IDS evasion, 411
web server security, 320
NetBIOS, LDAP enumeration, 155-157, 160
DumpSec, 158
Hyena GUI tool, 158
Ldp, 159
NetBIOS Enumerator, 159
SuperScan, 159
NetBus, 211
Netcat
+.htr exploit, 315-316
banner grabbing, 134
firewalls, bypassing, 427
port redirection, 223-224
web server enumeration, 305
Netcraft, 91, 304
NetResident, dynamic malware analysis, 237
Netsparker, web server security, 320
Netstat, malware detection, 229
NetStumbler, 377, 382
network access layer (TCP/IP model)
ARP, 76
MAC addresses, 75-76
network layer (Layer 3), OSI model, 56
Network Performance Monitor, SNMP enumeration, 161
network protocols, ethical hacker skill requirements, 21
Network Security Test Lab: A Step-by-Step Guide, The, 545

networks
database management system, 340
evaluations (Level II assessments), security testing, 15
forensics, man-in-the-middle attacks, 276
gear testing (ethical hacking), 21
jamming attacks, 381
mapping
attack surfaces, *135-137*
subnets and, *112*
P2P networks
Pirate Bay, The, *223*
Trojans and, *209*
PAN, 369
ranges, determining, 112-114
VPN, 485
Wi-Fi networks
cracking/compromising, *384*
discovery, *WLAN and*, *381-382*
WLAN, 370
802.11 standard, *372*
ad hoc mode, *371*
AP spoofing, *379*
cantennas, *377*
cracking/compromising Wi-Fi networks, *384*
CSMA/CA, *372*
CSMA/CD Ethernet, *372*
defense in depth concept, *384-386*
DoS attacks, *380-381*
EAP, *388*
eavesdropping, *378*
evil-twin attacks, *379*
frequencies, *372*
GPS mapping, *383*
host routing, *380*
IDS, *389*
infrastructure mode, *371*
launching wireless attacks, *383*
misuse detection, *389*
OSA, *378*
rogue/unauthorized AP, *379*
security, *373-375*, *384-389*
site surveys, *386-387*
spread spectrum technology, *372*
SSID, *371*, *385*
threats, *376-381*
war chalking, *376*
war driving, *377*
war flying, *377*
WEP, *373-375*
Wi-Fi network discovery, *381-382*
wireless traffic analysis, *383*
WPA, *375*
WPA2, *375*
NIC (Network Interface Cards)
promiscuous mode, 252-254, 378
wireless NIC, 378
NIDS (Network-based IDS), 400
NIDSbench, IDS evasion, 411
Nikto, web application security, 339
Nimda worm, 203, 312-313
NIST SP 800-15, ethical hacker's process, 53
NLog, mapping network attack surfaces, 136
Nmap
active fingerprinting, 131-132
AP scanning, 123-126
NSE, 124, 306
port scanning, 123-126
Zenmap, 126
no-knowledge (black box) testing, 13-14
noise (power anomalies), 446
nonrepudiation, 485
nontechnical password attacks, 164
NSA, web server security, 319
NSE (Nmap Scripting Engine), 124, 306
Nslookup, 108, 112
NT ERD (Emergency Repair Disk), 173

NTFSDOS, 173
NTLM (NT LAN Manager), Windows authentication, 173-174
NTLM v2 (NT LAN Manager version 2), Windows authentication, 173-174
NTP (Network Time Protocol), enumeration, 162-163
null sessions, 156

O

Obad, 366
obfuscation
attacks, 404
IDS and, 410
obfuscation layer, BurnEye wrappers, 214
object-oriented database management system, 340
obscurity, security by, 512
OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), ethical hacker's process, 53
Oechslin, Philippe, 177
OFB (Output Feedback) mode (DES), 491
OFDM (Orthogonal Frequency-Division Multiplexing), 373
OllyDbg static malware analysis, 235
Omnipeek
sniffing, 265
Wi-Fi network discovery, 382
online resources
exploit database, 50
GHDB, 101
vulnerability research websites, 29
open AP scanning, 116-117
Hping, 128
idle scanning, 119
IPID scanning, 120
Nmap, 123-126
SuperScan, 127
TCP scanning, 118-119
THC-Amap, 127
UDP scanning, 122
war driving, 129
open port scanning, 116-117
Hping, 128
idle scanning, 119
IPID scanning, 120
Nmap, 123-126
port knocking, 128
SuperScan, 127
TCP scanning, 118-119
THC-Amap, 127
UDP scanning, 122
war driving, 129
Open VMS passwords, 177
OpenPuff stenographic tool, 500
OpenSSL, Heartbleed, 508
Operation Payback, 310
Ophcrack password-extraction tool, 177
organization websites
footprinting information-gathering process, 91-93
scanning information-gathering process, 91-93
organizational security process
assessments, 52
auditing, 53
implementation, 52
policy development, 52
training, 52
OS fingerprinting
active fingerprinting
ACK values, 131
bogus flag probe, 130
FIN probe, 130
fragmentation handling, 131
IPID sampling, 130
ISN sampling, 130
Nmap, 131-132

Queso, *131*
TCP initial window, *130*
TCP options, *131*
type of service, *131*
Winfingerprint, *132*
Xprobe2, *132*
default ports/services, 133
open services, 133-135
passive fingerprinting, 129
OSA (Open System Authentication), WLAN, 378
Osborn, Mark, 402
OSI (Open Systems Interconnection) model
application layer (Layer 7), 55
data link layer (Layer 2), 56
network layer (Layer 3), 56
physical layer (Layer 1), 57
presentation layer (Layer 6), 55
session layer (Layer 5), 56
transport layer (Layer 4), 56
OSSTMM (Open Source Security Testing Methodology Manual), 23, 54
overlapping fragmentation attacks, 70
OWASP ZAP (Zed Application Proxy)
web application hacking, 321
web server hacking, 317
web traffic interception, 335-337
owning the box, 172

P

P2P (Peer-to-Peer)
DoS attacks, 282
networks
Pirate Bay, The, *223*
Trojans and, *209*
PaaS (Platform as a Service) cloud computing model, 529
packers, Trojans and, 214, 216
packets
filtering, 414-417
SYN packets, transport layer tunneling, 220
TCP ACK packets, transport layer tunneling, 221
palm scans (biometric access control), 462
PAN (Personal-Area Networks), 369
Pandora, DDoS attacks, 286
parameter/form tampering, web application hacking, 321-322
Parker Bowles, Camilla, 360
Paros Proxy, web traffic interception, 335
partial-knowledge (gray box) testing, 14
passing the hash, 167
passive fingerprinting, 129
passive sniffing, 252-253
password layer, BurnEye wrappers, 214
passwords
authentication, 166, 462, 485
automated password guessing, 167
bad passwords list, 331
brute-force attacks, 176
change policies, 469
cognitive passwords, 469
cracking
Brutus tool, *514*
cookies, *333-334*
CryptoTool, *514*
Hashcat tool, *514*
John the Ripper, *514*
Linux passwords, *180-181*
preteen style, *332*
SQLbf, *344*
THC-Hydra tool, *514*
web application hacking, *329-334*
web server hacking, *314*
Windows passwords, *175-177*
dictionary attacks, 175
guessing, 165-167
hybrid password attacks, 175

keylogging (keystroke loggers), 168-169
Linux passwords, 177-181
nontechnical password attacks, 164
Open VMS passwords, 177
resetting with StickyKeys, 170
sniffing, 167-168
technical password attacks, 164
automated password guessing, 167
keylogging (keystroke loggers), 168-169
password guessing, 165-167
password sniffing, 167-168
web application hacking, 329-334
web server password cracking, 314
Windows passwords, cracking, 175-177
path (directory) traversal
web application hacking, 328
web server hacking, 311-313
pattern-matching IDS (signatures), 403, 410
components of, 404
keywords, 405
rules, 405-406
signature analysis, 406
PC Activity Monitor, keylogging (keystroke loggers), 169
PC Magazine, 468
PCI-DSS (Payment Card Industry Data Security Standard), 34
Pearson Test Prep software, 546
peer-to-peer attacks, 282
penetration testing, 20, 440
external penetration testing, 21
internal penetration testing, 21
Level III assessments, security testing, 15
web application hacking, 331
web server enumeration, 306
people/employee searches, footprinting/scanning information-gathering process, 94-97
permanent DoS attacks (phlashing attacks), 283-284
permissions, ethical hacker's process, 52
person-to-person social engineering, 464-465
personal safety controls (physical security), 461
PGMP (Pretty Good Malware Protection), 216
PGP (Pretty Good Privacy), 506-507
Phatbot, 212. *See also* Agobot
phishing
identifying, 467
SMiShing, 466
spear phishing, 466-467
whaling, 466
phlashing attacks (permanent DoS attacks), 283-284
phones
cell phones (smartphones)
1G, 360-363
2G, 361
2.5G, 361
3G, 361-362
4G, 361-362
Android platform, 364-366
application sandbox issues, 363
BlackBerry platform, 367
bump attacks, 363
BYOD policies, 364
Cellebrite forensic tool, 363
cloning, 360
data confidentiality, 364
data disposal, 364
data exfiltration, 362
data leakage, 364
device support, 364
eavesdropping, 360
geolocation/location-based services, 362
iOS platform, 366-367
jailbreaking, 363, 366-367
malware, 362
managing, 368

mixing personal/private data, *364*
securing, *368*
spoofing cell towers, *363*
spread spectrum technologies, *361*
subscription fraud, *360*
tumbling attacks, *360*
Windows Phone platform, *367*
cordless phones, 359
PhoneSnoop, 368
Phrak magazine, 222
phreakers, defined, 18
physical access controls (physical security)
authentication, 462-463
Trojans and, 209
physical layer (Layer 1), OSI model, 57
physical security
area controls, 456, 459
Defense in Depth, 463
documentation
backups, *448-449*
shredders, *448*
employee training, 447
equipment controls
delay alarms, *451*
fax machines, *454-455*
locks, *449-454*
visibility shields, *451*
facility controls
bollards, *460*
dogs, *460*
fences, *458-459*
guards, *459*
lighting, *459*
mantraps, *460*
turnstiles, *460*
firewalls, bypassing, 423
IoT and, 447
location data/geotagging, 456
penetration testing, 440
personal safety controls, 461
physical access controls, authentication
biometric access control, *462-463*
magnetic strip cards, *462*
passwords, *462*
PIN, *462*
smart cards, *462*
tokens, *462*
policies, 447
SCADA, 446
shoulder surfing, 451
smartphone triangulation/GPS tracking, 457-458
testing, 22
threats
dumpster diving, *448*
man-made threats, *445*
natural threats, *444-445*
power anomalies, *446*
picking locks, 452-454
picks (lock), 452
piggybacking and mantraps, 460
PIN (Personal Identification Numbers), authentication (physical security), 462
PIN-cracking, Bluetooth, 369
ping command, 114
active machines, identifying, 115
Hping, 128
ICMP and, 218
Linux ping capture, 219
sweeps, 116
Ping of Death, 283
Pipkin, Donald L., 332
Pirate Bay, The, 223
PKI (Public Key Infrastructure)
CA, 503
certificate servers, 504
CRL, 503
RA, 504
trust models, 504

hierarchical trust model, 505
signed certificates, 506
single-authority trust model, 505
web of trust model, 506
X.509 standard, 504
plain text
chosen plain-text attacks, 510
encryption, 486
known plain-text attacks, 510
planning tests
business reasons for testing, 24-25
establishing goals, 26-27
ethical hacking reports, 28-29
getting approval, 27
phases of testing, 25
researching vulnerabilities, 29
scope of assessment, 24
poison apple attacks, 207
Poison Ivy, 211
poisoning attacks
ARP poisoning, 255-257
DNS cache poisoning, 261
policies
development, organizational security process, 52
firewalls, bypassing, 423
physical security, 447
security policies, 16
polymorphic viruses, 199
POODLE (Padding Oracle On Downgraded Legacy Encryption)
man-in-the-middle attacks, 316
Poodlebleed, 511
pop-up windows, social engineering and, 465
ports
common ports/protocols table, 60-61, 116
DHCP redirect attacks, 259
fingerprinting, 133
idle scanning, 119-121
IPID
open port, 120
port closed, 121
knocking, 128
principle of least privilege, 61
redirecting, 223-225
scanning, 49, 116-117, 303
firewalls, 417-418
Hping, 128
idle scanning, 119
IPID scanning, 120
legality of, 122
Nmap, 123-126
port knocking, 128
SuperScan, 127
TCP scanning, 118-119
THC-Amap, 127
UDP scanning, 122
war driving, 129
spanning, 252
Trojan ports, 206-208
post-connection SYN, IDS and, 410
power anomalies and physical security, 446
PPTP (Point-to-Point Tunneling Protocol), 509
practices/standards, ethical hacker's process
NIST SP 800-15, 53
OCTAVE, 53
OSSTMM, 54
pre-connection SYN, IDS and, 410
PremiumSMS, 366
preparing for exams
hands-on activities, 545
suggested study plans, 545-546
prependers, viruses, 200
presentation layer (Layer 6), OSI model, 55
Prestel, 31
principle of least privilege, 61

printers (laser) and steganography, 501
privacy
PGP, 506-507
policies, 470
private clouds, 528
privileges
escalating, 51
DLL injection, 169
horizontal escalation, 172
vertical escalation, 172
principle of least privilege, 61
Process Explorer, dynamic malware analysis, 237
Process Monitor, malware detection, 229
Process Viewer, malware detection, 229
processes
attacker's process
backdoors, 51
covering tracks, 51
enumeration, 49
escalation of privileges, 51
footprinting, 48
gaining access, 50
maintaining access, 51
reconnaissance, 48
scanning, 49
ethical hacker's process
assessments, 52
covering tracks, 52
gaining access, 52
maintaining access, 52
NIST SP 800-15, 53
OCTAVE, 53
OSSTMM, 54
permissions, 52
reconnaissance, 52
reporting, 52
scanning, 52
security testing, 53-54
standards/practices, 53-54
organizational security
assessments, 52
auditing, 53
implementation, 52
policy development, 52
training, 52
OSSTMM, 23
program-level attacks, 282-283
programmable cipher locks, physical security, 451
programming, ethical hacker skill requirements, 20
project management, ethical hacker skill requirements, 21
promiscuous mode, 252-254, 267, 378
protocol analyzers, man-in the-middle attacks, 276
protocol-decoding IDS, 403
provider viability, cloud computing concerns, 531
proxies, 206
proxy ARP (Address Resolution Protocol), 76
proxy servers, bypassing firewalls, 423
Ps command, malware detection, 229
public clouds, 528
public key encryption. *See* asymmetric encryption
Purple Machine, history of cryptography, 487
PWdump password-extraction tool, 175
PwnageTool, 367
pwned accounts, 165

Q - R

queries (DNS), 105
Queso, active fingerprinting, 131

RA (Registration Authority), PKI framework, 504
RAID (Redundant Array of Inexpensive Disks), 8

RainbowCrack password-extraction tool, 177
ranges (network), determining, 112-114
ransomware, 203
RAT (Remote-Access Trojans), 206
BlackHole RAT, 211
Gh0st RAT, 212
Jumper RAT, 212
Let Me Rule RAT, 212
NetBus, 211
Poison Ivy, 211
Shady Rat, 211
RATS (Rough Auditing Tool for Security), web application security, 338
RC2 (Rivest Cipher 2), symmetric encryption, 492
RC4 (Rivest Cipher 4), symmetric encryption, 488, 492
RC5 (Rivest Cipher 5), symmetric encryption, 488, 492
RC6 (Rivest Cipher 6), symmetric encryption, 488, 492
reciprocation (social engineering), 464
reconnaissance, 18
attacker's process, 48
ethical hacker's process, 52
redirect attacks (DHCP), 259
redirecting ports, 223-225
Redsn0w, 367
registrars, queries and footprinting/scanning information-gathering process, 104-107
registries
Registry, scanning for changes, 228
RIR, 104
Regshot, malware detection, 229
regulatory requirements, cloud computing, 530
relational database management system, 340
RemoteSpy, keylogging (keystroke loggers), 169
replay attacks, 510
reports, ethical hacking reports, 28-29, 52
researching vulnerabilities (test plans), 29
resetting passwords, StickyKeys, 170
resource exhaustion attacks, SYN flood attacks and botnets, 538
resources (web), vulnerability research websites, 29
Restorator, 216
Retina CS, web server security, 319-320
retina patterns (biometric access control), 463
reverse social engineering, 468
reverse WWW tunneling shell, application layer tunneling, 222
review/study plans, 545-546
RID (Relative Identifiers), 154, 158
Rijmen, Vincent, 492
Rijndael, symmetric encryption, 488, 492
RIR (Regional Internet Registries), 104
risk
assessing, 12-13
defined, 8
managing, backups, 11
RMF, 8
Rivest, Ron
RC (Rivest Cipher), 492
RSA encryption, 493
RMF (Risk Management Framework), 8
rogue AP (Access Points), WLAN, 379
rooting Android devices, 366
rootkits
application rootkits, 182-183
Avatar, 182
Azazel, 183
Chkrootkit, 184
covering tracks, 182-184
defined, 51

kernel rootkits, 182-183
McAfee Rootkit Detective, 184
Necurs, 183
RootkitBuster, 184
RootKitRevealer, 184
Zeroaccess, 183
ROT3 (Caesar's cipher) and the history of cryptography, 485
rounds (DES), 490
routers/routing
ethical hacker skill requirements, 20
host routing, WLAN, 380
source routing, 72
RPC (Remote Procedure Call) services, 162
rpcclient command, Linux enumeration, 162
rpinfo command, Linux enumeration, 162
RSA encryption, 493
RSA NetWitness, sniffing, 265
RTM worm, 202
rubber hose attacks, 510
Rusers, 162
Rwho, 162
Ryan, Thomas, 97

S

S-Tools stenographic tool, 500-501
S/MIME (Secure/Multipurpose Internet Mail Extensions), 507
SaaS (Software as a Service) cloud computing model, 529
SAFER (Secure and Fast Encryption Routine), symmetric encryption, 488
Sage, Robin, 97
sags (power anomalies), 446
Sality security software disabler, 206
SAM (Security Account Manager)
database, 155
stealing, 172
sandboxes
application sandbox issues and mobile devices, 363
defined, 235, 363
Sasser worm, 203
satellite TV, 358-359
Saudi Arabian Oil Co. (Aramco), permanent DoS attacks, 283
SCADA (Supervisory Control and Data Acquisition), 101
buffer overflows, 327
physical security, 446
scanning, 18
active machines, identifying, 115
AP scanning, 116-117
Hping, 128
idle scanning, 119
IPID scanning, 120
Nmap, 123-126
SuperScan, 127
TCP scanning, 118-119
THC-Amap, 127
UDP scanning, 122
war driving, 129
attacker's process, 49
ethical hacker's process, 52
facial scans (biometric access control), 462
fingerprinting (OS)
active fingerprinting, 130-132
default ports/services, 133
open services, 133-135
passive fingerprinting, 129
heuristic scanning antivirus programs, 232
information-gathering process, 90
DNS enumeration, 107-111
documentation, 91
EDGAR database, 97
employee/people searches, 94-97
Google hacking, 98-103
job boards, 93-94
organization websites, 91-93

registrar queries, *104-107*
Usenet, *103-104*
Jotti's malware scanning service, 232
mapping attack surfaces
automated mapping, *136-137*
manual mapping, *135*
network ranges, determining, 112-114
online virus/malware scanning sites, 233
palm scans (biometric access control), 462
port scanning, 116-117, 303
firewalls, *417-418*
Hping, *128*
idle scanning, *119*
IPID scanning, *120*
Nmap, *123-126*
port knocking, *128*
SuperScan, *127*
TCP scanning, *118-119*
THC-Amap, *127*
UDP scanning, *122*
war driving, *129*
Registry for changes, 228
signature-scanning antivirus programs, 231
UDP, 122
vulnerabilities, 303
Acunetix Web Vulnerability Scanner, *320*
disadvantages, *50*
IBM Internet Scanner, *320*
Retina C S, *320*
web server security, *319-320*
web application scanners, 338
web servers, 304
scarcity (social engineering), 464
Schiffman, Michael, 113
Schneider, Sondra, 514
***Science and Practice of Persuasion, The*, 464**
scope of assessment (test plans), 24
screened host firewalls, 417
script kiddies
defined, 18
virus toolkits, 204
scripting, XSS and cloud computing, 532
scrubbing locks, 452
Scytale and the history of cryptography, 485
Sealand, 136
search routines (viruses), 200
searches
employee/people searches, footprinting/scanning information-gathering process, 94-97
Google search terms, 99
secondary connections, bypassing firewalls, 423
security
breaches, cloud computing, 531
goals of, 7-8
obscurity, security by, 512
physical security testing, 22
policies, 16
software, disabling, 206
testing
ethical hacker's process, *53-54*
full-knowledge (white box) testing, *14*
goal of, *13*
high-level assessments/audits (Level I assessments), *15*
network evaluation (Level II assessments), *15*
NIST SP 800-15, *53*
no-knowledge (black box) testing, *13-14*
OCTAVE, *53*
OSSTMM, *54*
partial-knowledge (gray box) testing, *14*
penetration tests (Level III assessments), *15*
TOE, *13*
types of tests, *15*
usability versus, 6

servers
certificate servers, PKI framework, 504
dedicated servers, cloud computing, 531
DNS servers, 310-311
IRC servers, botnets, 534
shared servers, cloud computing, 531
SQL servers, 340-341
servers (web)
authentication, password cracking, 314
hacking, 298
automated exploit tools, 316-317
banner grabbing, 303-309
DDoS attacks, 310
directory (path) traversal, 311-313
DNS amplification attacks, 310-311
DNS server hijacking, 310-311
DoS attacks, 310
encryption, 316
enumeration, 303-309
HTTP response splitting, 314
IIS vulnerabilities, 315-316
man-in-the-middle attacks, 313
password cracking, 314
port scanning, 303
securing servers, 318
vulnerability identification, 309
vulnerability scanning, 303
web server misconfiguration, 313
web server scanning, 304
website defacement, 313
HTML, 302
HTTP, 302
misconfiguring, web server hacking, 313
password cracking, web server hacking, 314
scanning, 304
securing, 318
vulnerabilities, identifying, 309
services
fingerprinting, 131-135
location-based services/geolocation, mobile devices, 362
syslog services, bypassing firewalls, 424
session layer (Layer 5), OSI model, 56
Session Thief, session hijacking, 276
sessions
fixation attacks, 274, 327
hijacking, 56, 248
application layer (TCP) hijacking, 271-274, 277
cloud computing, 532
encryption, 277
HTTP GET requests, 276
preventing, 277
tools, 274-277
transport layer (TCP) hijacking, 267-270
replay attacks, application layer (TCP) hijacking, 274
riding, cloud computing, 532
splicing, IDS and, 408-409
SHA-1 (Secret Hash Algorithm-1), 496
Shady Rat, 211
Shamir, Adi, 493
Shamoon permanent DoS attacks, 284
shared servers, cloud computing, 531
shellcode attacks, IDS and, 409
shields (visibility), physical security, 451
shims (locks), 453
Shodan, 101-102, 447
shoulder surfing, 164, 451
showmount command, Linux enumeration, 162
Showtime, 359
shredders and documentation security, 448
shrinkwrap software, 10
SID (Security Identifiers), 154, 158
side-channel attacks, 510, 532
signatures
digital signatures, 496

pattern-matching IDS, Snort and, 403-406, 410
signature-scanning antivirus programs, 231
signed certificates, PKI, 506
Silentbanker botnets, 535
simple SQL injection attacks, 342
single-authority trust model (PKI), 505
site surveys, WLAN and, 386-387
SKA (Shared Key Authentication), 378
SLA (Service Level Agreements), 8, 531
Slammer worm, 203
SLE (Single-Loss Expectancy), risk assessment, 12-13
SMAC (Social, Mobile, Analytics, Cloud), MAC spoofing, 260
smart cards, authentication (physical security), 462
smartphones
1G, 360-363
2G, 361
2.5G, 361
3G, 361-362
4G, 361-362
Cellebrite forensic tool, 363
cloning, 360
concerns
application sandbox issues, 363
bump attacks, 363
BYOD policies, 364
data confidentiality, 364
data disposal, 364
data exfiltration, 362
data leakage, 364
device support, 364
geolocation/location-based services, 362
jailbreaking, 363, 366-367
malware, 362
mixing personal/private data, 364
spoofing cell towers, 363
eavesdropping, 360
geotagging/location data, 456
managing, 368
platforms
Android, 364-366
BlackBerry, 367
iOS, 366-367
Windows Phone, 367
securing, 368
spread spectrum technologies, 361
subscription fraud, 360
triangulation/GPS tracking, 457-458
tumbling attacks, 360
SmartWhois, 105
SMB (Server Message Blocks), LDAP enumeration, 155-156
SMiShing, 367, 466
Smith, David, 202
SMTP (Simple Mail Transfer Protocol), 60-62, 163
Smurf attacks, 282
Sn0wbreeze, 367
sniffers, 51, 57, 248
active sniffing, 252-253
ARP, 254
ARP, DAI, 266
ARP poisoning, 255-257
ARP spoofing, 255-257
DHCP redirect attacks, 259
DHCP snooping, 259-260, 266
DNS cache poisoning, 261
DNS spoofing, 261
MAC flooding, 258-259
MAC spoofing, 260
application layer (TCP) hijacking, session sniffing, 271
countermeasures, 266-267
defined, 252
encryption and, 263
NIC, promiscuous mode, 252-254

passive sniffing, 252-253
passwords, 167-168
spanning ports, 252
tools for sniffing
Dsniff, 265
OmniPeek, 265
RSA NetWitness, 265
TCPdump, 265
WinDump, 265
Wireshark, 262-265
web traffic interception, 335
SNMP (Simple Network Management Protocol)
defined, 63
enumeration
Network Performance Monitor, 161
snmpwalk, 160
SNScan, 161
snmpwalk, SNMP enumeration, 160
snooping (DHCP), 259-260, 266
Snort, 410
components of, 404
keywords, 405
rules, 405-406
signature analysis, 406
Snow stenographic tool, 499
SNScan, SNMP enumeration, 161
SOAP injection, web application hacking, 327
SoapUI, web server security, 319
social engineering, 22, 49, 164, 440
cloud computing, 532
computer-based social engineering, 465
phishing, 466-467
SMiShing, 466
spear phishing, 466-467
whaling, 466
defined, 463
firewalls, bypassing, 423
person-to-person social engineering, 464-465
policies/procedures
AUP, 469
commercial data classification, 471
employee ID badges, 469
government data classification, 470-471
help desk procedures, 469
hiring/termination policies, 469
NDA, 469
password change policies, 469
privacy policies, 470
user awareness, 471-472
reverse social engineering, 468
social networking and, 465-467
social validation, 464
Trojans and, 213
types of, 464
social networking
dangers of, 97
social engineering and, 465-467
social validation (social engineering), 464
software
crackers/hackers, defined, 19
keyloggers, 226
shrinkwrap software, 10
SolarWinds Network Topology Mapper, 136
Sony Pictures, permanent DoS attacks, 283
source routing, 72
source-disclosure attacks, 315
SOX (Sarbanes-Oxley) Act, 33
Spam Mimic, 500
spanning ports, 252
sparse infections, 199
spear phishing, 466-467
spikes (power anomalies), 446
splicing sessions, IDS and, 408-409
spoofing, 277
AP, WLAN, 379
ARP spoofing, 255-257

cell phone towers, 363
countermeasures
Arpwatch, *266*
DAI, *266*
DNSSEC, *266*
promiscuous mode, *267*
DNS spoofing, 261, 266
MAC spoofing, 260
spread spectrum technology
DSSS, 373
FHSS, 373
mobile devices, 361
OFDM, 373
WLAN, 372
Spy PC Keylogger, 226
spyware, 198, 227
SQL (Structured Query Language)
injection
attacks, *339-344*
cloud computing, *532*
hacking tools, *344-345*
web application hacking, *322*
server identification, database hacking, 340-341
SQL Power Injector, 345
SQL2.exe, 345
SQLbf, 344
SQLDict, 344
SQLExec, 344
SSH (Secure Shell), LAN Turtles, 507
SSID (Service Set ID), WLAN and, 371, 385
SSL (Secure Sockets Layer), OpenSSL and Heartbleed, 508
SSLstrip, session hijacking, 276
SSLv3 (Secure Sockets Layer version 3), breaking via Poodlebleed, 511
stack security
OSI model
application layer (Layer 7), *55*
data link layer (Layer 2), *56*
network layer (Layer 3), *56*
physical layer (Layer 1), *57*
presentation layer (Layer 6), *55*
session layer (Layer 5), *56*
transport layer (Layer 4), *56*
TCP/IP model, 57
application layer, *59-63*
encapsulation, *58*
Internet layer, *66-74*
network access layer, *75-76*
transport layer, *63-66*
StackGuard, web application security, 338
standards/practices, ethical hacker's process
NIST SP 800-15, 53
OCTAVE, 53
OSSTMM, 54
Star Wars, 17
stateful inspection firewalls, 416-417
static malware analysis, 234-236
status monitoring, Big Brother, 98
stealing SAM (Security Account Manager), 172
steganography
carriers, 498
defined, 497
digital watermarks, 502
laser printers, 501
operation of, 498-499
tools
ImageHide stenographic tool, *500*
MP3Stego stenographic tool, *499*
OpenPuff stenographic tool, *500*
S-Tools stenographic tool, *500-501*
Snow stenographic tool, *499*
Spam Mimic, *500*
steganalysis, *502*
Steganography Studio, *500*
Steghide stenographic tool, *499*

Steghide stenographic tool, 499
StickyKeys, 170
stolen equipment attacks, 22
storage channel attacks, 217
Storm worm, 203
stream ciphers (DES), 490
strip-cut shredders, documentation security, 448
study plans (suggested), 545-546
subnets, mapping networks, 112
subscription fraud, cell phones, 360
substitution ciphers (encryption), 486
suggested study plans, 545-546
suicide hackers, defined, 17
Super Bluetooth Hack, 369
SuperScan
AP scanning, 127
LDAP enumeration, 159
port scanning, 127
surges (power anomalies), 446
surveillance, spyware and, 227
symmetric encryption, 484-486
3DES, 488, 491
AES, 490-492
Blowfish, 488
DES, 488-489
block ciphers, 490
CBC mode, 490
CFB mode, 491
ECB mode, 490
OFB mode, 491
rounds, 490
stream ciphers, 490
Double DES, 491
key distribution, 489
RC2, 492
RC4, 488, 492
RC5, 488, 492
RC6, 488, 492
Rijndael, 488, 492
SAFER, 488
SYN
flood attacks, 64, 281, 538
packets, transport layer tunneling, 220
post-connection SYN, IDS and, 410
pre-connection SYN, IDS and, 410
synchronize sequence number flags, 117
SYSKEY, 173
syslog services, bypassing firewalls, 424
system files, verifying, 228
system hacking
crackers/hackers, defined, 19
cracking
Linux passwords, 180-181
Windows passwords, 175-177
defined, 148, 164
exploiting vulnerabilities, 169
buffer overflow, 171
buffer overflows, 170
privilege escalation, 172
StickyKeys, 170
goal of, 164
Linux
authentication, 177-180
passwords, 177-181
nontechnical password attacks, 164
owning the box, 172
privilege escalation, 169
stealing SAM, 172
technical password attacks, 164
automated password guessing, 167
keylogging (keystroke loggers), 168-169
password guessing, 165-167
password sniffing, 167-168
Windows authentication, 173-174

T

tables (memory), 546
Tamper IE, session hijacking, 276
TAN grabbers, botnets, 535
Task Manager, malware detection, 229

Taylor, Allen, 455
TCSEC (Trusted Computer System Evaluation Criteria), covert communication and, 217
TCP (Transmission Control Protocol), 63-65
application layer session hijacking
client-side attacks, 272-274
man-in-the-browser attacks, 272
man-in-the-middle attacks, 272, 277
predicting session token ID, 271
session fixation attacks, 274
session replay attacks, 274
session sniffing, 271
flag types, 117-118
headers, 117-118
initial window (active fingerprinting), 130
scanning
ACK scans, 119
FIN scans, 118
full connect scans, 118
NULL scans, 119
SYN scans, 118
XMAS scans, 119
TCP options (active fingerprinting), 131
transport layer session hijacking, 267
controlling sessions, 270
identifying/finding active sessions, 268
predicting sequence numbers, 269-270
taking one party offline, 270
window size, botnets and, 538
TCP ACK packets, transport layer tunneling, 221
TCP/IP (Transmission Control Protocol/Internet Protocol) model, 57
application layer, 59
common ports/protocols table, 60-61
DHCP, 61
DNS, 62
FTP, 61
HTTP, 63
SMTP, 62
SNMP, 63
Telnet, 61
TFTP, 63
encapsulation, 58
Internet layer, 66
ICMP, 70-72
IP fragmentation, 68-70
IPv4 addressing, 67-68
IPv4 headers, 67
IPv6 headers, 67
source routing, 72
traceroute, 72-74
network access layer
ARP, 76
MAC addresses, 75-76
transport layer
TCP, 63-65
UDP, 66
TCPdump
dynamic malware analysis, 237
sniffing, 265
TCPView
dynamic malware analysis, 237
malware detection, 229
teardrop attacks, 70, 283
technical password attacks, 164
keylogging (keystroke loggers), 168-169
passwords
guessing, 165-167
sniffing, 167-168
Teflon Oil Patch, 216
Telnet, 61
banner grabbing, 133
web server scanning, 305
tension wrenches, picking locks, 452
testing
application testing, 22
authentication system testing, 22
communication system testing, 22

database testing, 22
DoS testing, 21
network gear testing, 21
penetration testing, 20-21
physical security testing, 22
planning tests
business reasons for testing, 24-25
establishing goals, 26-27
ethical hacking reports, 28-29
getting approval, 27
phases of testing, 25
researching vulnerabilities, 29
scope of assessment, 24
security testing
ethical hacker's process, 53
full-knowledge (white box) testing, 14
goal of, 13
high-level assessments/audits (Level I assessments), 15
network evaluation (Level II assessments), 15
NIST SP 800-15, 53
no-knowledge (black box) testing, 13-14
OCTAVE, 53
OSSTMM, 54
partial-knowledge (gray box) testing, 14
penetration tests (Level III assessments), 15
TOE, 13
types of tests, 15
wireless network testing, 22

text
chosen cipher-text attacks, 510
chosen plain-text attacks, 510
cipher-text only attacks, 510
encryption, 486
known plain-text attacks, 510

TFN (Tribal Flood Network), DDoS attacks, 285

TFTP (Trivial File Transfer Protocol), 63, 425

THC-Amap, 127

THC-Hydra encryption-cracking tool, 330, 514

THC-Wardrive, Wi-Fi network discovery, 382

theft and physical security, 445

third-party authorization attacks, 465

ThreatExpert static malware analysis, 235

threats, defined, 9-10

Three Musketeers hack, 358

throttling, DoS/DDoS attacks, 287

tidal waves (tsunamis) and physical security, 444

timing attacks, 217

Tini, 211

TKIP (Temporal Key Integrity Protocol), 375

TOE (Target Of Evaluation), defined, 13

token authentication (physical security), 462

token ID, application layer (TCP) hijacking, 271

tracebacks, botnets and, 538

traceroute, 72-74
firewalls, port scanning, 417
network ranges, determining, 113
Sealand, 136

tracking DDoS attack sources, 289

tracks, covering, 18
attacker's process, 51
ethical hacker's process, 52
file hiding, 184-185
logs
clearing log files, 181
disabling, 181
rootkits, 182-184

traffic analysis (wireless), WLAN and, 383

training
employees for physical security, 447
organizational security process, 52
Tramp.A, 366
transient (power anomalies), 446
transmission methods of viruses, 198-199
transport layer
firewalls, bypassing, 422
tunneling, covert communication and, 220-221
transport layer (Layer 4), OSI model, 56
transport layer (TCP) session hijacking, 267
controlling sessions, 270
identifying/finding active sessions, 268
predicting sequence numbers, 269-270
taking one party offline, 270
transport layer (TCP/IP model)
TCP, 63-65
UDP, 66
trapdoor functions (asymmetric encryption), 493
Trend Micro RootkitBuster, 184
triangulation/GPS tracking (smartphones), 457-458
trigger routines (viruses), 200
Triludan the War, 31
Trinoo, DDoS attacks, 286
Tripwire, 228, 237
Trojan Man wrappers, 216
Trojans, 194
Amitis, 212
Apple products and, 213
backdoors, 207
Banking Trojans, 535
Beast, 212
browser bugs, 209
communication methods, 206-208
crypters, 215-216
data hiding, 206
delivery mechanisms, 208-210
distributing, 213-216
DNSChanger, 213
DoS attacks, 206
E-banking, 206
effects of, 210
email attachments, 209
freeware, 209
FTP, 206
Gh0st RAT Trojan, 467
goals of, 208
Hell Raiser, 213
IM, 209
infection mechanisms, 208-210
IRC, 209
legal issues, 210
MoSucker, 212
P2P networks, 209
packers, 214-216
Phatbot, 212
physical access as delivery method, 209
poison apple attacks, 207
ports, 206-208
proxies, 206
RAT, 206
BlackHole RAT, *211*
Gh0st RAT, *212*
Jumper, *212*
Let Me Rule RAT, *212*
NetBus, *211*
Poison Ivy, *211*
Shady Rat, *211*
security software disablers, 206
social engineering and, 213
Tini, 211
tools, 210-213
types of, 205-206
Visual Basic Trojans, 212
watering holes, 209
wrappers, 213-216
Zombzm.B, 212

tropical storms (hurricanes) and physical security, 444
Trout, 114
true/false matrix, IDS, 401
trust models (PKI), 504
hierarchical trust model, 505
signed certificates, 506
single-authority trust model, 505
web of trust model, 506
TShark, 265
tsunamis (tidal waves) and physical security, 444
TTL (Time To Live), 109-111, 114-115, 129, 538
Tumbler, memes, 200
tumbler locks, physical security, 450
tumbling attacks, 360
tunneling
application layer tunneling, covert communication, 221-222
firewalls, bypassing, 423
HTTP tunneling, 223
Internet layer tunneling, covert communication, 218-220
PPTP, 509
transport layer tunneling, covert communication, 220-221
turnstiles (physical security, facility controls), 460
TV (satellite), 358-359
Twitter, memes, 200
type of service fingerprinting, 131

U

U.S. federal laws, 30
18 USC 1028, 361
18 USC 1029, 361
CIPA, 34
Computer Fraud and Abuse Act of 1984, 32
Cyber Security Enhancement Act of 2002, 32
Economic Espionage Act of 1996, 33
Electronic Communication Privacy Act, 32
Federal Sentencing Guidelines of 1991, 33
FISMA, 32
GLBA, 33
HIPAA, 33
SOX Act, 33
U.S. Code Title 18, 31
USA PATRIOT Act of 2001, 32
UDP (User Datagram Protocol), 56, 66
echo packets, Fraggle bandwidth attacks, 281
firewalls, bypassing, 422
scanning, 122
transport layer tunneling, 221
UDP tunneling, 221
UEFI (Unified Extensible Firmware Interface), Windows Phone boot process, 367
Ufasoft Snif, ARP spoofing, 257
UID (User ID), 154
unauthorized AP (Access Points), WLAN, 379
unicast MAC addresses, 76
Unicode
directory (path) traversal, 312
encoding, web application hacking, 328
Unicode Web Traversal exploit, 203
union SQL injection attacks, 342
United Kingdom, hacking and British law, 31
United States 2012 presidential election campaign, memes and, 200
UNIX enumeration, 161-162
unroutable addresses, NAT, 413
unvalidated input, web application hacking, 321

updates, Windows Server Update Services and web server security, 318
UPX static malware analysis, 235
URL (Uniform Resource Locators), web application hacking
encoding, 328
obfuscation, 334-335
USA PATRIOT Act of 2001, 32
usability versus security, 6
Usenet, footprinting/scanning information-gathering process, 103-104
user awareness and social engineering policies/procedures, 471-472
user name authentication, 485
Uuencode, weak encryption, 513

V

validating unvalidated input, web application hacking, 321
vandalism and physical security, 445
Veriato Investigator, 169, 226
verifying system files, 228
vertical privilege escalation, 172
Videocipher II satellite encryption, 358
Virdem, history of viruses, 201
viruses, 9, 194, 197
antidetection routines, 200
antivirus programs, 230
activity blockers, 232
EICAR and, 232
heuristic scanning programs, 232
integrity checking, 232
Jotti's malware scanning service, 232
online virus/malware scanning sites, 233
signature-scanning programs, 231
appenders, 200
Brain, 201
clusters, 198
components of, 200
fast infections, 199
file infections, 198
Flame, 199
history of, 201
hoaxes, 199
infection routines, 200
macro infections, 198
master boot record infections, 198
Melissa, 202
memes, 199-200
multipartite viruses, 199
payloads, 200
polymorphic viruses, 199
prependers, 200
prevention plans, 230-231
ransomware, 203
search routines, 200
sparse infections, 199
tools, 204-205
transmission methods, 198-199
trigger routines, 200
types of, 198-200
well-known viruses, 202-203
VirusTotal static malware analysis, 236
visibility shields, physical security, 451
Visual Basic Trojans, 212
VisualRoute, 114
voice recognition (biometric access control), 463
Void11, WLAN and, 383
VPN (Virtual Private Networks), 485
vulnerabilities
defined, 10
exploiting, 169
buffer overflow, 170-171
StickyKeys, 170
IIS vulnerabilities, web server hacking, 315-316
researching (test plans), 29
scanning, 303
Acunetix Web Vulnerability Scanner, 320
disadvantages, 50

IBM Internet Scanner, *320*
Retina C S, *320*
web server security, *319-320*
web server vulnerabilities, identifying, 309

W

WAF (Web Application Firewalls), 335
walls (physical security, area controls), 456
war chalking, WLAN, 376
war driving, 129, 377
war flying, WLAN, 377
warded locks, physical security, 450
watering hole attacks, 172, 209
watermarks (digital), 502
WaveStumbler, Wi-Fi network discovery, 382
Wayback Machine, 92
weak authentication, 485
weak encryption
Base64, 512
Uuencode, 513
XOR, 512
weather (natural disasters), 9
web applications
hacking, 298, 320
authentication attacks, *328-329*
brute-force attacks, *329*
buffer overflows, *326-327*
CSRF, *323-324*
dictionary attacks, *329*
Direct OS commands, *327*
DoS attacks, *327*
Hex encoding, *328*
hidden field attacks, *325-326*
hybrid attacks, *329*
injection flaws, *322*
parameter/form tampering, *321-322*
password cracking, *329-334*
path traversal, *328*
session fixation, *327*
SOAP injection, *327*
Unicode encoding, *328*
unvalidated input, *321*
URL encoding, *328*
URL obfuscation, *334-335*
web traffic interception, *335-337*
XSS, *323*
scanning tools, 338
securing, 337-339
WAF, 335
web browsers
application layer (TCP) hijacking, 272
browser bugs, Trojans and, 209
man-in-the-browser attacks, 272
web of trust model (PKI), 506
web pages (archived), viewing, 92
web resources
exploit database, 50
GHDB, 101
vulnerability research websites, 29
web servers
authentication, password cracking, 314
hacking, 298
automated exploit tools, *316-317*
banner grabbing, *303-309*
DDoS attacks, *310*
directory (path) traversal, *311-313*
DNS amplification attacks, *310-311*
DNS server hijacking, *310-311*
DoS attacks, *310*
encryption, *316*
enumeration, *303-309*
HTTP response splitting, *314*
IIS vulnerabilities, *315-316*
man-in-the-middle attacks, *313*
password cracking, *314*
port scanning, *303*
securing servers, *318*
vulnerability identification, *309*

vulnerability scanning, 303
web server misconfiguration, 313
web server scanning, 304
website defacement, 313
HTML, 302
HTTP, 302
misconfiguring, web server hacking, 313
password cracking, web server hacking, 314
scanning, 304
securing, 318
vulnerabilities, identifying, 309
web traffic interception, web application hacking, 335-337
WebCracker password-cracking tool, web application hacking, 330
WebDAV (Web Distributed Authoring and Versioning), 315, 319
WebInspect, web application security, 339
websites
capture-the-flag sites, 545
defacing, web server hacking, 313
online virus/malware scanning sites, 233
organization websites
footprinting information-gathering process, 91-93
scanning information-gathering process, 91-93
social engineering and, 465
vulnerability research websites, 29
WEP (Wired Equivalent Privacy) protocol
cracking, 384
WLAN security, 373-375
Wget, web server hacking, 309
whaling, 466
Whisker, web application security, 338
white box (full-knowledge) testing, 14
white hat hackers, defined, 17
Whois, 105, 107
Wi-Fi
networks
cracking/compromising, 384
discovery tools, WLAN and, 381-382
WIFI pineapples, 379
WikiLeaks, 310
Wikto, web server hacking, 307
WinARPAttacker, ARP spoofing, 257
WinDNSSpoof, DNS spoofing, 261
Windows
architecture, 153
authentication, 168, 173-174
enumeration, 152-155
ethical hacker skill requirements, 20
LSASS, 167
passwords, cracking, 175-177
security
AD, 155
GID, 154
LSASS, 155
RID, 154, 158
SAM database, 155
SID, 154, 158
UID, 154
Windows Phone mobile device platform, 367
Windows Registry, scanning for changes, 228
Windows Server Update Services, web server security, 318
Windows XP, 156
Windtalkers, 487
WinDump, sniffing, 265
Winfingerprint, active fingerprinting, 132
wireless network testing (ethical hacking), 22
wireless NIC (Network Interface Cards), promiscuous mode, 378
wireless technologies
Bluetooth, 368-369

cell phones (smart phones)
1G, 360-363
2G, 361
2.5G, 361
3G, 361-362
4G, 361-362
Android platform, 364-366
application sandbox issues, 363
BlackBerry platform, 367
bump attacks, 363
BYOD policies, 364
Cellebrite forensic tool, 363
cloning, 360
data confidentiality, 364
data disposal, 364
data exfiltration, 362
data leakage, 364
device support, 364
eavesdropping, 360
geolocation/location-based services, 362
iOS platform, 366-367
jailbreaking, 363, 366-367
malware, 362
managing, 368
mixing personal/private data, 364
securing, 368
spoofing cell towers, 363
spread spectrum technologies, 361
subscription fraud, 360
tumbling attacks, 360
Windows Phone platform, 367
cordless phones, 359
history of, 358
mobile devices
1G, 360-363
2G, 361
2.5G, 361
3G, 361-362
4G, 361-362
Android platform, 364-366
application sandbox issues, 363
BlackBerry platform, 367
bump attacks, 363
BYOD policies, 364
Cellebrite forensic tool, 363
cloning, 360
data confidentiality, 364
data disposal, 364
data exfiltration, 362
data leakage, 364
device support, 364
eavesdropping, 360
geolocation/location-based services, 362
iOS platform, 366-367
jailbreaking, 363, 366-367
malware, 362
managing, 368
mixing personal/private data, 364
securing, 368
spoofing cell towers, 363
spread spectrum technologies, 361
subscription fraud, 360
tumbling attacks, 360
Windows Phone platform, 367
satellite TV, 358-359
Three Musketeers hack, 358
Videocipher II satellite encryption, 358
WLAN, 370
802.11 standard, 372
ad hoc mode, 371
AP spoofing, 379-381
cantennas, 377
cracking/compromising Wi-Fi networks, 384
CSMA/CA, 372
CSMA/CD Ethernet, 372
defense in depth concept, 384-386
EAP, 388
eavesdropping, 378
evil-twin attacks, 379

frequencies, *372*
GPS mapping, *383*
host routing, *380*
IDS, *389*
infrastructure mode, *371*
launching wireless attacks, *383*
misuse detection, *389*
OSA, *378*
rogue/unauthorized AP, *379*
security, *373-375*, *384-389*
site surveys, *386-387*
spread spectrum technology, *372*
SSID, *371*, *385*
threats, *376-381*
war chalking, *376*
war driving, *377*
war flying, *377*
WEP, *373-375*
Wi-Fi network discovery, *381-382*
wireless traffic analysis, *383*
WPA, *375*
WPA2, *375*
wireless traffic analysis, WLAN and, 383
Wireshark, 59
dynamic malware analysis, 237
filters, 264-265
reverse DNS lookups, 267
sniffing, 262-265
TShark, 265
WLAN (Wireless Local Area Networks), 370
802.11 standard, 372
ad hoc mode, 371
cantennas, 377
CSMA/CA, 372
CSMA/CD Ethernet, 372
frequencies, 372
infrastructure mode, 371
security
defense in depth concept, *384-386*
EAP, *388*
IDS, *389*
misuse detection, *389*
site surveys, *386-387*
SSID, *385*
WEP, *373-375*
WPA, *375*
WPA2, *375*
spread spectrum technology, 372
SSID, 371
threats
AP spoofing, *379*
DoS attacks, *380-381*
eavesdropping, *378*
evil-twin attacks, *379*
host routing, *380*
OSA, *378*
rogue/unauthorized AP, *379*
war chalking, *376*
war driving, *377*
war flying, *377*
tools
cracking/compromising Wi-Fi networks, *384*
GPS mapping, *383*
launching wireless attacks, *383*
Wi-Fi network discovery, *381-382*
wireless traffic analysis, *383*
WordPress, 330
worms, 194, 197
Code Red, 202
Conficker, 203
MyDoom, 203
Nimda, 203
Nimda worm, 312-313
RTM worm, 202
Sasser, 203
Slammer, 203

Storm, 203
well-known worms, 202-203
WPA (Wi-Fi Protected Access)
encryption, 384
WLAN security, 375
WPA2 (Wi-Fi Protected Access version 2), WLAN security, 375
wrappers, Trojans and, 213-216
wrapping attacks, cloud computing, 532
wrenches (tension), picking locks, 452

X

X.509 standard
digital signatures, 503
PKI framework, 504
XML (Extensible Markup Language) injection, web application hacking, 322
XOR
weak encryption, 512
XORing, 373-374
Xprobe2, active fingerprinting, 132
XSS (Cross-Site Scripting), 272
cloud computing, 532
web application hacking, 323

Y - Z

Yahoo!, 7
Yarochkin, Fyodor, 123
Yoda's Crypter, 216

Zenmap, 126
Zeroaccess rootkit, 183
Zeus, E-banking, 206
ZitMo, 368
Zombam.B Trojan, 212
zombie computers. *See* botnets
zone transfers, 109-111, 163