

PEARSON IT

CYBERSECURITY CURRICULUM



FOURTH EDITION

COMPUTER SECURITY FUNDAMENTALS

DR. CHUCK EASTTOM

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



Computer Security Fundamentals

Fourth Edition

Dr. Chuck Easttom



Pearson

Computer Security Fundamentals, Fourth Edition

Copyright © 2020 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein.

Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-13-577477-9

ISBN-10: 0-13-577477-2

Library of Congress control number: 2019908181

ScoutAutomatedPrintCode

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Microsoft® Windows®, and Microsoft Office® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose all such documents and related graphics are provided “as is” without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Editor-in-Chief

Mark Taub

Product Line Manager

Brett Bartow

Senior Editor

James Manly

Development Editor

Christopher Cleveland

Managing Editor

Sandra Schroeder

Project Editor

Mandie Frank

Indexer

Erika Millen

Proofreader

Abigail Manheim

Technical Editor

Akhil Behl

Publishing Coordinator

Cindy Teeters

Designer

Chuti Prasertsith

Composer

codeMantra

Credits

Figure Number

Attribution/Credit Line

Figure 2-1	Screenshot of Command prompt © Microsoft 2019
Figure 2-2	Screenshot of Command prompt © Microsoft 2019
Figure 2-3	Screenshot of Command prompt © Microsoft 2019
Figure 2-4	Screenshot of Command prompt © Microsoft 2019
Figure 2-5	Screenshot of Command prompt © Microsoft 2019
Figure 2-6	Screenshot of Command prompt © Microsoft 2019
Figure 2-7	Screenshot of Command prompt © Microsoft 2019
Figure 2-8	Screenshot of Command prompt © Microsoft 2019
Figure 2-9	Screenshot of Command prompt © Microsoft 2019
Figure 3-1	Screenshot of windows © Microsoft 2019
Figure 3-2	Screenshot of windows © Microsoft 2019
Figure 3-3	Screenshot of windows © Microsoft 2019
Figure 3-4	Screenshot of windows © Microsoft 2019
Figure 3-5	Screenshot of windows © Microsoft 2019
Figure 4-1	Screenshot of Command prompt © Microsoft 2019
Figure 4-2	Screenshot of LOIC © Praetox Technologies
Figure 4-3	Screenshot of XOIC © Praetox Technologies
Figure 5-1	Screenshot of Command prompt © Microsoft 2019
Figure 5-2	Screenshot of Counterexploitation © CEXX.ORG
Figure 5-3	Screenshot of SpywareGuide © 2003-2011, Actiance, Inc.
Figure 5-4	Screenshot of SpywareGuide © 2003-2011, Actiance, Inc.
Figure 5-5	Screenshot of SpywareGuide © 2003-2011, Actiance, Inc.
Figure 5-6	Screenshot of Norton Security © 1995 - 2019 Symantec Corporation
Figure 5-7	Screenshot of McAfee AntiVirus © 2019 McAfee, LLC
Figure 5-8	Screenshot of Avast © 1988-2019 Copyright Avast Software s.r.o
Figure 5-9	Screenshot of AVG © 1988-2019 Copyright Avast Software s.r.o
Figure 5-10	Screenshot of Malwarebytes © 2019 Malwarebytes
Figure 5-11	Screenshot of Windows © Microsoft 2019
Figure 6-1	Screenshot of Netcraft © 1995-2019 Netcraft Ltd
Figure 6-2	Screenshot of WayBackMachine BETA © Internet Archive
Figure 6-3	Screenshot of Zenmap © NMAP.ORG
Figure 6-4	Screenshot of Cain © Cain and Abel
Figure 6-5	Screenshot of Shodan © 2013-2019 Shodan
Figure 6-6	Screenshot of Shodan © 2013-2019 Shodan
Figure 6-8	Screenshot of OphCrack © 2019 Slashdot Media
Figure 6-9	Screenshot of TeraBIT Virus Maker © TeraBIT Virus Maker
Figure 6-11	Screenshot of Yahoo © 2019 Verizon Media
Figure 6-12	Screenshot of Peoples Drug Store © 2019 Digital Pharmacist Inc.
Figure 7-2	New Africa/Shutterstock
Figure 7-4	Reed Kaestner/Getty Images
Figure 7-5	Screenshot of VeraCrypt © IDRIX
Figure 7-6	Screenshot of windows © Microsoft 2019
Figure 8-2	Chuck Easttom
Figure 9-1	Screenshot of Windows 10 Firewall © Microsoft 2019
Figure 9-2	Screenshot of Snort Installation © 2019 Cisco
Figure 9-7	Screenshot of Windows-style library © Microsoft 2019

Figure 11-1	Screenshot of Shutting Down a Service in Windows © Microsoft 2019
Figure 11-2	Screenshot of Disabled services © Microsoft 2019
Figure 11-4	Screenshot of Microsoft Baseline Security Analyzer © Microsoft 2019
Figure 11-5	Screenshot of Microsoft Baseline Security Analyzer © Microsoft 2019
Figure 11-6	Screenshot of Microsoft Baseline Security Analyzer © Microsoft 2019
Figure 11-7	Screenshot of Nessus © 2019 Tenable
Figure 11-8	Screenshot of Nessus © 2019 Tenable
Figure 11-9	Screenshot of Nessus © 2019 Tenable
Figure 11-10	Screenshot of Nessus © 2019 Tenable
Figure 11-11	Screenshot of Nessus © 2019 Tenable
Figure 11-12	Screenshot of OWASP ZAP © OWASP
Figure 11-13	Screenshot of OWASP ZAP © OWASP
Figure 11-14	Screenshot of shodan © 2013-2019 Shodan®
Figure 11-15	Screenshot of shodan © 2013-2019 Shodan®
Figure 12-1	Dan Grytsku/123RF
Figure 12-2	Screenshot of Sinn Fein © Sinn Féin
Figure 12-3	Screenshot of BBC News © 2019 BBC
Figure 12-4	Screenshot of Cyberterrorism Preparedness Act
Figure 12-5	Screenshot of Cyberterrorism Preparedness Act
Figure 12-6	Screenshot of Tech Law Journal
Figure 12-7	Screenshot of The Peoples drug store
Figure 12-8	Screenshot of ccPal Store
Figure 13-1	Screenshot of Yahoo © 2019 Verizon Media
Figure 13-2	Screenshot of Yahoo © 2019 Verizon Media
Figure 13-3	Screenshot of Yahoo © 2019 Verizon Media
Figure 13-4	Screenshot of Infobel © 1995 - 2019 Kapitol
Figure 13-6	Screenshot of Federal Bureau of Investigation
Figure 13-7	Screenshot of Texas Department of Public Safety © 2000- 2019 Texas Department of Public Safety.
Figure 13-8	Screenshot of Oklahoma
Figure 13-9	Screenshot of Google access ©2019 Google
Figure 14-1	Screenshot of FTK Imager © Copyright 2019 AccessData
Figure 14-2	Screenshot of FTK Imager © Copyright 2019 AccessData
Figure 14-3	Screenshot of FTK Imager © Copyright 2019 AccessData
Figure 14-4	Screenshot of FTK Imager © Copyright 2019 AccessData
Figure 14-5	Screenshot of FTK Imager © Copyright 2019 AccessData
Figure 14-6	Screenshot of OSForensics Copyright © 2019 PassMark® Software
Figure 14-7	Screenshot of OSForensics Copyright © 2019 PassMark® Software
Figure 14-8	Screenshot of DiskDigger Copyright © 2010-2019 Defiant Technologies, LLC
Figure 14-9	Screenshot of DiskDigger Copyright © 2010-2019 Defiant Technologies, LLC
Figure 14-10	pio3/Shutterstock
Figure 14-11	Screenshot of OSForensics Copyright © 2019 PassMark® Software
Figure 14-12	Screenshot of Command Prompt © Microsoft 2019
Figure 14-13	Screenshot of Command Prompt © Microsoft 2019
Figure 14-14	Screenshot of Command Prompt © Microsoft 2019
Figure 14-15	Screenshot of Command Prompt © Microsoft 2019
Figure 14-16	Screenshot of Windows registry © Microsoft 2019
Figure 14-17	Screenshot of Windows registry © Microsoft 2019
Figure 15-10	Screenshot of Microsoft Excel © Microsoft 2019

Contents at a Glance

Introduction	xxvi
1 Introduction to Computer Security	2
2 Networks and the Internet	32
3 Cyber Stalking, Fraud, and Abuse	66
4 Denial of Service Attacks	96
5 Malware	120
6 Techniques Used by Hackers	152
7 Industrial Espionage in Cyberspace	182
8 Encryption	206
9 Computer Security Technology	244
10 Security Policies	278
11 Network Scanning and Vulnerability Scanning	306
12 Cyber Terrorism and Information Warfare	342
13 Cyber Detective	370
14 Introduction to Forensics	386
15 Cybersecurity Engineering	422
Glossary	442
Appendix A: Resources	448
Appendix B: Answers to the Multiple Choice Questions	450
Index	454

Table of Contents

Introduction	xxvi
Chapter 1: Introduction to Computer Security	2
Introduction	2
How Seriously Should You Take Threats to Network Security?	4
Identifying Types of Threats	7
Malware	8
Compromising System Security	9
DoS Attacks	10
Web Attacks	10
Session Hijacking	13
Insider Threats	13
DNS Poisoning	14
New Attacks	15
Assessing the Likelihood of an Attack on Your Network	16
Basic Security Terminology	16
Hacker Slang	17
Professional Terms	19
Concepts and Approaches	19
How Do Legal Issues Impact Network Security?	22
Online Security Resources	23
CERT	23
Microsoft Security Advisor	24
F-Secure	24
SANS Institute	24
Summary	25
Test Your Skills	25

Chapter 2: Networks and the Internet	32
Introduction	32
Network Basics	33
The Physical Connection: Local Networks	33
Faster Connection Speeds	36
Wireless	36
Bluetooth	38
Other Wireless Protocols	38
Data Transmission	38
How the Internet Works	40
IP Addresses	41
Uniform Resource Locators	46
What Is a Packet?	46
Basic Communications	47
History of the Internet	47
Basic Network Utilities	49
IPConfig	49
Ping	51
Tracert	52
Netstat	53
NSLookup	53
ARP	54
Route	54
Other Network Devices	55
Advanced Network Communications Topics	56
The OSI Model	56
Media Access Control (MAC) Addresses	57
Summary	58
Test Your Skills	58

Chapter 3: Cyber Stalking, Fraud, and Abuse	66
Introduction	66
How Internet Fraud Works	67
Investment Offers	67
Auction Fraud	70
Identity Theft	72
Phishing	73
Cyber Stalking	74
Real Cyber Stalking Cases	75
How to Evaluate Cyber Stalking	78
Crimes Against Children	80
Laws About Internet Fraud	81
Protecting Yourself Against Cybercrime	82
Protecting Against Investment Fraud	82
Protecting Against Identity Theft	83
Secure Browser Settings	84
Protecting Against Auction Fraud	87
Protecting Against Online Harassment	88
Summary	89
Test Your Skills	89
Chapter 4: Denial of Service Attacks	96
Introduction	96
DoS Attacks	97
Illustrating an Attack	97
Distributed Reflection Denial of Service Attacks	99
Common Tools Used for DoS Attacks	99
Low Orbit Ion Cannon	99
XOIC	100

TFN and TFN2K.....	101
Stacheldraht.....	101
DoS Weaknesses.....	102
Specific DoS Attacks.....	102
TCP SYN Flood Attacks.....	102
Smurf IP Attacks.....	105
UDP Flood Attacks.....	107
ICMP Flood Attacks.....	107
The Ping of Death.....	107
Teardrop Attacks.....	108
DHCP Starvation.....	108
HTTP POST DoS Attacks.....	108
PDoS Attacks.....	108
Registration DoS Attacks.....	108
Login DoS Attacks.....	108
Land Attacks.....	109
DDoS Attacks.....	109
Real-World Examples of DoS Attacks.....	109
<i>Boston Globe</i> Attack.....	109
Memcache Attacks.....	109
MyDoom.....	110
DDoS Blackmail.....	111
Mirai.....	111
How to Defend Against DoS Attacks.....	111
Summary.....	113
Test Your Skills.....	113

Chapter 5: Malware	120
Introduction	120
Viruses	121
How a Virus Spreads	121
Types of Viruses	122
Virus Examples	123
The Impact of Viruses	129
Rules for Avoiding Viruses	129
Trojan Horses	129
The Buffer-Overflow Attack	132
The Sasser Virus/Buffer Overflow	133
Spyware	134
Legal Uses of Spyware	135
How Is Spyware Delivered to a Target System?	135
Obtaining Spyware Software	135
Other Forms of Malware	137
Rootkits	137
Malicious Web-Based Code	138
Logic Bombs	139
Spam	139
Advanced Persistent Threats	139
Detecting and Eliminating Viruses and Spyware	140
Antivirus Software	140
Remediation Steps	144
Summary	145
Test Your Skills	145
 Chapter 6: Techniques Used by Hackers	 152
Introduction	152
Basic Terminology	153

The Reconnaissance Phase	153
Passive Scanning Techniques	153
Active Scanning Techniques	155
Actual Attacks	162
SQL Script Injection	162
Cross-Site Scripting	165
Cross-Site Request Forgery	165
Directory Traversal	165
Cookie Poisoning	165
URL Hijacking	166
Wireless Attacks	166
Cell Phone Attacks	166
Password Cracking	166
Malware Creation	168
Windows Hacking Techniques	169
Penetration Testing	171
NIST 800-115	171
The NSA Information Assessment Methodology	171
PCI Penetration Testing Standard	172
The Dark Web	173
Summary	176
Test Your Skills	176
Chapter 7: Industrial Espionage in Cyberspace	182
Introduction	182
What Is Industrial Espionage?	183
Information as an Asset	184
Real-World Examples of Industrial Espionage	187
Example 1: Houston Astros	187
Example 2: University Trade Secrets	188

Example 3: Nuclear Secrets	188
Example 4: Uber	188
Example 5: Foreign Governments and Economic Espionage	188
Trends in Industrial Espionage	189
Industrial Espionage and You	189
How Does Espionage Occur?	189
Low-Tech Industrial Espionage	189
Spyware Used in Industrial Espionage	193
Steganography Used in Industrial Espionage	193
Phone Taps and Bugs	194
Protecting Against Industrial Espionage	194
The Industrial Espionage Act	197
Spear Phishing	198
Summary	199
Test Your Skills	199
Chapter 8: Encryption	206
Introduction	206
Cryptography Basics	207
History of Encryption	207
The Caesar Cipher	209
Atbash	211
Multi-Alphabet Substitution	211
Rail Fence	212
Enigma	213
Binary Operations	214
Modern Cryptography Methods	216
Single-Key (Symmetric) Encryption	216
Modification of Symmetric Methods	223
Public Key (Asymmetric) Encryption	223

PGP	228
Legitimate Versus Fraudulent Encryption Methods	229
Digital Signatures	230
Hashing	230
MD5	231
SHA	231
RIPEMD	231
MAC and HMAC	231
Rainbow Tables	232
Steganography	233
Historical Steganography	234
Steganography Methods and Tools	234
Cryptanalysis	235
Frequency Analysis	235
Modern Cryptanalysis Methods	235
Cryptography Used on the Internet	236
Quantum Computing Cryptography	237
Summary	238
Test Your Skills	238
Chapter 9: Computer Security Technology	244
Introduction	244
Virus Scanners	245
How Does a Virus Scanner Work?	245
Virus-Scanning Techniques	246
Commercial Antivirus Software	248
Firewalls	248
Benefits and Limitations of Firewalls	248
Firewall Types and Components	249
Firewall Configurations	250

Commercial and Free Firewall Products	251
Firewall Logs	253
Antispyware	253
IDSs	254
IDS Categorization	254
Identifying an Intrusion	255
IDS Elements	256
Snort	256
Honey Pots	260
Database Activity Monitoring	261
Other Preemptive Techniques	261
Authentication	262
Digital Certificates	265
SSL/TLS	266
Virtual Private Networks	268
Point-to-Point Tunneling Protocol	269
Layer 2 Tunneling Protocol	269
IPsec	270
Wi-Fi Security	270
Wired Equivalent Privacy	271
Wi-Fi Protected Access	271
WPA2	271
WPA3	271
Summary	272
Test Your Skills	272
Chapter 10: Security Policies	278
Introduction	278
What Is a Policy?	279
ISO 17999	279

Defining User Policies	280
Passwords	281
Internet Use	282
Email Usage	283
Installing/Uninstalling Software	284
Instant Messaging	284
Desktop Configuration	285
Bring Your Own Device	285
Final Thoughts on User Policies	286
Defining System Administration Policies	287
New Employees	287
Departing Employees	287
Change Requests	288
Security Breaches	290
Virus Infection	290
DoS Attacks	291
Intrusion by a Hacker	291
Defining Access Control	292
Development Policies	293
Standards, Guidelines, and Procedures	294
Data Classification	294
DoD Clearances	294
Disaster Recovery	295
Disaster Recovery Plan	295
Business Continuity Plan	295
Impact Analysis	296
Disaster Recovery and Business Continuity Standards	296
Fault Tolerance	296

Important Laws	298
HIPAA	298
Sarbanes-Oxley	299
Payment Card Industry Data Security Standards	299
Summary	300
Test Your Skills	300
Chapter 11: Network Scanning and Vulnerability Scanning	306
Introduction	306
Basics of Assessing a System	307
Patch	307
Ports	308
Protect	311
Policies	312
Probe	314
Physical	314
Securing Computer Systems	315
Securing an Individual Workstation	316
Securing a Server	317
Securing a Network	319
Scanning Your Network	321
MBSA	321
NESSUS	324
OWASP Zap	326
Shodan	328
Getting Professional Help	330
Summary	333
Test Your Skills	333

Chapter 12: Cyber Terrorism and Information Warfare	342
Introduction	342
Actual Cases of Cyber Terrorism	343
The Chinese Eagle Union	344
China's Advanced Persistent Threat	344
India and Pakistan	345
Russian Hackers	345
Weapons of Cyber Warfare	345
Stuxnet	345
Flame	346
StopGeorgia.ru Malware	346
FinFisher	347
BlackEnergy	347
NSA ANT Catalog	347
Economic Attacks	347
Military Operations Attacks	350
General Attacks	350
Supervisory Control and Data Acquisitions (SCADA)	351
Information Warfare	352
Propaganda	352
Information Control	353
Disinformation	355
Actual Cases	355
Future Trends	359
Positive Trends	359
Negative Trends	361
Defense Against Cyber Terrorism	362
Terrorist Recruiting and Communication	362
TOR and the Dark Web	363

Summary	365
Test Your Skills	365
Chapter 13: Cyber Detective	370
Introduction	370
General Searches	371
Facebook	374
Court Records and Criminal Checks	375
Sex Offender Registries	375
Civil Court Records	377
Other Resources	378
Usenet	379
Summary	380
Test Your Skills	380
Chapter 14: Introduction to Forensics	386
Introduction	386
General Guidelines	387
Don't Touch the Suspect Drive	387
Image a Drive with Forensic Toolkit	388
Can You Ever Conduct Forensics on a Live Machine?	391
Document Trail	391
Secure the Evidence	392
Chain of Custody	392
FBI Forensics Guidelines	392
U.S. Secret Service Forensics Guidelines	393
EU Evidence Gathering	394
Scientific Working Group on Digital Evidence	395
Locard's Principle of Transference	395
Tools	396

Finding Evidence on the PC	397
Finding Evidence in the Browser	397
Finding Evidence in System Logs	398
Windows Logs	398
Linux Logs	399
Getting Back Deleted Files	399
Operating System Utilities	402
net sessions	402
openfiles	403
fc	403
netstat	404
The Windows Registry	404
Specific Entries	406
Mobile Forensics: Cell Phone Concepts	408
Cell Concepts Module	408
Cellular Networks	409
iOS	410
Android	410
Windows	411
What You Should Look For	412
The Need for Forensic Certification	413
Expert Witnesses	414
Federal Rule 702	414
Daubert	414
Additional Types of Forensics	415
Network Forensics	415
Virtual Forensics	415
Summary	418
Test Your Skills	418

Chapter 15: Cybersecurity Engineering	422
Introduction	422
Defining Cybersecurity Engineering	423
Cybersecurity and Systems Engineering	424
Applying Engineering to Cybersecurity	424
SecML	430
SecML Concepts	431
Misuse Case Diagram	432
Security Sequence Diagram	436
Data Interface Diagram	438
Security Block Diagram	439
Summary	440
Test Your Skills	440
Glossary	442
Appendix A: Resources	448
Appendix B: Answers to the Multiple Choice Questions	450
Index	454

About the Author

Dr. Chuck Easttom is the author of 26 books, including several on computer security, forensics, and cryptography. He has also authored scientific papers on digital forensics, cyber warfare, cryptography, and applied mathematics. He is an inventor with 16 computer science patents. He holds a Doctor of Science in cyber security (dissertation topic: a study of lattice-based algorithms for post quantum cryptography) and three master's degrees (one in applied computer science, one in education, and one in systems engineering). He also holds 44 industry certifications (CISSP, CEH, etc.) He is a frequent speaker at cybersecurity, computer science, and engineering conferences. He is a Distinguished Speaker of the ACM and a Senior member of the IEEE and a Senior member of the ACM. Dr. Easttom is also a reviewer for five scientific journals and Editor in Chief for the *American Journal of Science and Engineering*. You can find out more about Dr. Easttom and his research at www.ChuckEasttom.com.

About the Technical Reviewer

Akhil Behl, CCIE No. 19564, is a passionate IT executive with key focus on cloud and security. He has more than 16 years of experience in the IT industry working in several leadership, advisory, consultancy, and business development profiles with various organizations. His technology and business specialization includes cloud, security, infrastructure, data center, and business communication technologies.

Akhil is a published author. Over the span of past few years, Akhil authored multiple titles on security and business communication technologies. He has contributed as technical editor for over a dozen books on security, networking, and information technology. He has published several research papers in national and international journals, including IEEE Xplore, and presented at various IEEE conferences, as well as other prominent ICT, security, and telecom events. Writing and mentoring is his passion and a part of his life.

He holds CCIE (Collaboration and Security), CCSK, CHFI, PMP, ITIL, VCP, TOGAF, CEH, ISM, CCDP, and many other industry certifications. He has Bachelor in Technology and Masters in Business Administration degrees.

Dedication

*This book is dedicated to my wife, Teresa,
who has helped me become who I am.*

Acknowledgments

The creation of a book is not a simple process and requires the talents and dedication of many people to make it happen. With this in mind, I would like to thank the folks at Pearson for their commitment to this project. The editors have been integral to making this book a success.

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@community.informit.com

Introduction

It has been more than 14 years since the publication of the original edition of this book. A great deal has happened in the world of computer security since that time. This edition is updated to include newer information, updated issues, and revised content.

The real question is: Who is this book for? This book is a guide for any computer-savvy person. This means system administrators who are not security experts and anyone who has a working knowledge of computers and wishes to know more about cybercrime and cyber terrorism could find this book useful. However, the core audience will be students who wish to take a first course in security but may not have a thorough background in computer networks. The book is in textbook format, making it ideal for introductory computer security courses that have no specific prerequisites. That lack of prerequisites means that people outside the normal computer science and computer information systems departments could also avail themselves of a course based on this book. This might be of particular interest to law enforcement officers, criminal justice majors, and even business majors with an interest in computer security.

As was previously mentioned, this book is intended as an introductory computer security book. In addition to the numerous footnotes, the appendixes will guide you to a plethora of additional resources. There are also review questions and practice exercises with every chapter. Appendix B provides the answers to the multiple choice questions for your review. Exercises and projects are intended to encourage the reader to explore, so answers will vary.

This book assumes that you are a competent computer user. That means you have used a computer at work and at home, are comfortable with email and web browsers, and know what words like RAM and USB mean. For instructors considering using this book as a textbook, students should have a basic understanding of PCs but need not have had formal computer courses. For this reason, the book includes a chapter on basic networking concepts to get those students up to speed. Those with more knowledge, such as system administrators, will find some chapters of more use than others. Feel free to simply skim any chapter that you feel is too elementary for you.

This page intentionally left blank

Chapter

1

Introduction to Computer Security

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Identify the top threats to a network: security breaches, denial of service attacks, and malware
- Assess the likelihood of an attack on your network
- Define key terms such as *cracker*, *penetration tester*, *firewall*, and *authentication*
- Compare and contrast perimeter and layered approaches to network security
- Use online resources to secure your network

Introduction

Since the first edition of this book, the prevalence of online transactions has increased dramatically. In 2004 we had e-commerce via websites; in 2019 we have smart phone apps, the Internet of Things, medical devices that communicate wirelessly, as well as an expanded use of e-commerce websites. We also have Wi-Fi-enabled cars and smart homes. Internet traffic is far more than just humorous YouTube videos or Facebook updates about our vacations. Now it is the heart and soul of commerce, both domestic and international. Internet communication even plays a central role in military operations and diplomatic relations. In addition to smart phones, we now have smart watches and even vehicles that have Wi-Fi hotspots and smart technology. Our lives are inextricably intertwined with the online world. We file our taxes online, shop for homes online, book vacations online, and even look for dates online.

Because so much of our business is transacted online, a great deal of personal information is stored in computers. Medical records, tax records, school records, and more are all stored in computer databases.

Personal information is often called personally identifiable information (PII), and health-related data is usually termed personal health information (PHI). This leads to some very important questions:

- How is information safeguarded?
- What are the vulnerabilities to these systems?
- What steps are taken to ensure that these systems and data are safe?
- Who can access my information?

FYI: Where Is the Internet Going?

Obviously, the Internet has expanded, as previously mentioned. We now have smart phones, smart watches, even smart cars. We have the Internet of Things (IoT), which involves devices communicating on the Internet. Smart homes and medical devices, including implantable medical devices, are the current trends. What do you think the next 10 years will bring?

Unfortunately, not only have technology and Internet access expanded since the original publication of this book, but so have the dangers. How serious is the problem? According to a 2018 article from the *Center for Strategic and International Studies*, cybercrime has reached over \$600 billion a year in damages and is likely to exceed \$1 trillion per year soon. Cybercrime is now an economic and strategic problem that even affects national security.”¹

Forbes magazine reported that there were 2,216 data breaches and more than 53,000 incidents in the 12 months ending March 2018.² The specific number may vary from one study to the next, but the primary point remains the same: Cybercrime is increasing. This is due, in part, to the increasing number of connected devices. Every connected device is yet another potential target. There is also easy access to cybercrime tools and weapons on the Internet. All of these factors increase the opportunity for cybercrime.

In spite of daily horror stories, however, many people (including some law enforcement professionals and trained computer professionals) lack an adequate understanding about the reality of these threats. Clearly the media will focus attention on the most dramatic computer security breaches, not necessarily giving an accurate picture of the most plausible threat scenarios. It is not uncommon to encounter the occasional system administrator whose knowledge of computer security is inadequate.

This chapter outlines current dangers, describes the most common types of attacks on your personal computer and network, teaches you how to speak the lingo of both hackers and security professionals, and outlines the broad strokes of what it takes to secure your computer and your network.

1. <https://www.csis.org/analysis/economic-impact-cybercrime>

2. <https://www.forbes.com/sites/gilpress/2018/12/03/60-cybersecurity-predictions-for-2019/#4b352a144352>

In this book, you will learn how to secure both individual computers and entire networks. You will also find out how to secure data transmission, and you will complete an exercise to find out about your region's laws regarding computer security. Perhaps the most crucial discussion in this chapter is what attacks are commonly attempted and how they are perpetrated. In this first chapter we set the stage for the rest of the book by outlining what exactly the dangers are and introducing you to the terminology used by both network security professionals and hackers. All of these topics are explored more fully in subsequent chapters.

How Seriously Should You Take Threats to Network Security?

The first step in understanding computer and network security is to formulate a realistic assessment of the threats to those systems. You will need a clear picture of the dangers in order to adequately prepare a defense. There seem to be two extreme attitudes regarding computer security. The first group assumes there is no real threat. Subscribers to this belief feel that there is little real danger to computer systems and that much of the negative news is simply unwarranted panic. They often believe taking only minimal security precautions should ensure the safety of their systems. The prevailing sentiment is, if our organization has not been attacked so far, we must be secure. If decision makers subscribe to this point of view, they tend to push a reactive approach to security. They will wait to address security issues until an incident occurs—the proverbial “closing the barn door after the horse has already gotten out.” If you are fortunate, the incident will have only minor impact on your organization and will serve as a much-needed wakeup call. If you are unfortunate, then your organization may face serious and possible catastrophic consequences. One major goal of this book is to encourage a proactive approach to security.

People who subscribe to the opposite viewpoint overestimate the dangers. They tend to assume that numerous talented hackers are an imminent threat to their system. They may believe that any teenager with a laptop can traverse highly secure systems at will. Such a worldview makes excellent movie plots, but it is simply unrealistic. The reality is that many people who call themselves hackers are less knowledgeable than they think they are. These people have a low probability of being able to compromise any system that has implemented even moderate security precautions.

This does not mean that skillful hackers do not exist, of course. However, they must balance the costs (financial, time) against the rewards (ideological, monetary). “Good” hackers tend to target systems that yield the highest rewards. If a hacker doesn't perceive your system as beneficial to these goals, he is less likely to expend the resources to compromise your system. It is also important to understand that real intrusions into a network take time and effort. Hacking is not the dramatic process you see in movies. I often teach courses in hacking and penetration testing, and students are usually surprised to find that the process is actually a bit tedious and requires patience.

Both extremes of attitudes regarding the dangers to computer systems are inaccurate. It is certainly true that there are people who have the understanding of computer systems and the skills to compromise the security of many, if not most, systems. A number of people who call themselves hackers, though, are

not as skilled as they claim to be. They have ascertained a few buzzwords from the Internet and may be convinced of their own digital supremacy, but they are not able to affect any real compromises to even a moderately secure system.

The truly talented hacker is no more common than the truly talented concert pianist. Consider how many people take piano lessons at some point in their lives. Now consider how many of those ever truly become virtuosos. The same is true of computer hackers. There are many people with mediocre skills, but truly skilled hackers are not terribly common. Keep in mind that even those who do possess the requisite skills need to be motivated to expend the time and effort to compromise your system.

A better way to assess the threat level to your system is to weigh the attractiveness of your system to potential intruders against the security measures in place. This is the essence of threat analysis. You examine your risks, vulnerabilities, and threats in order to decide where to put the most effort in cybersecurity.

Keep in mind, too, that the greatest external threat to any system is not hackers but malware and denial of service (DoS) attacks. Malware includes viruses, worms, Trojan horses, and logic bombs. And beyond the external attacks, there is the issue of internal problems due to malfeasance or simple ignorance.

Security audits always begin with a risk assessment, and that is what we are describing here. First you need to identify your assets. Clearly, the actual computers, routers, switches and other devices that make up your network are assets. But it is more likely that your most important assets lie in the information on your network. Identifying assets begins with evaluating the information your network stores and its value. Does your network contain personal information for bank accounts? Perhaps medical information, health care records? In other cases, your network might contain intellectual property, trade secrets, or even classified military data.

Once you have identified the assets, you need to take inventory of the threats to your assets. Certainly, any threat is possible, but some are more likely than others. This is very much like what one does when selecting home insurance. If you live in a flood plain, then flood insurance is critical. If you live at a high altitude in a desert, it may be less critical. We do the same thing with our data. If you are working for a defense contractor, then foreign state-sponsored hackers are a significant threat. However, if you are the network administrator for a school district, then your greatest threat is likely to be juveniles attempting to breach the network. It is always important to realize what the threats are for your network.

Once you have identified your assets and inventoried the threats, you need to find out what vulnerabilities your system has. Every system has vulnerabilities. Identifying your network's specific vulnerabilities is a major part of risk assessment.

The knowledge of your assets, threats, and vulnerabilities will give you the information needed to decide what security measures are appropriate for your network. You will always have budget constraints, so you need to make wise decisions in selecting security controls. Using good risk assessment is how you make wise security decisions.

Note

There are a number of industry certifications that emphasize risk assessment. The Certified Information Systems Security Professional (CISSP) puts significant emphasis on this issue. The Certified Information Systems Auditor (CISA) places even more focus on risk assessment. One or more appropriate industry certifications can enhance your skillset and make you more marketable as a security professional. There are many other certifications, including the CompTIA Advanced Security Practitioner (CASP) and Security+ certifications.

There are methods and formulas for quantifying risk. A few simple formulas are provided here. In order to calculate the loss from a single incident, you multiply the asset value by the percentage of that asset that is exposed:

$$\text{Single Loss Expectancy (SLE)} = \text{Asset Value (AV)} \times \text{Exposure Factor (EF)}$$

What this formula means is that in order to calculate the loss from a single incident, you start with the asset value, and multiple that times what percentage of that asset is exposed. Let us assume you have a laptop that was purchased for \$1000. It has depreciated by 20%, meaning there is 80% of its value left. If that laptop is lost or stolen, $\$1000 (AV) \times .8 (EF) = \$800 (SLE)$. Now this is rather oversimplified and does not account for the value of the data. But it does illustrate the point of the formula. Now to go forward and calculate the loss per year, you use the following formula:

$$\text{Annualized Loss Expectancy (ALE)} = \text{Single Loss Expectancy (SLE)} \times \text{Annual Rate of Occurrence (ARO)}$$

Using the previous SLE of \$800, if you expect to lose 3 laptops per year, then the $ARO = \$800 \times 3$, or \$2400.

Obviously, these formulas have some subjectiveness to them. (For example, ARO is usually estimated from industry trends and past incidents.) But they can help you to understand the risk you have. This will help to guide you in determining what resources to allocate to addressing the risk.

Once you have identified a risk, you really have only four choices:

- **Acceptance:** This means you find the impact of the risk to be less than the cost of addressing it, or the probability is so remote that you do nothing. This is not the most common approach but is appropriate in some scenarios.
- **Avoidance:** This means ensuring that there is zero chance of the risk occurring. If you are concerned about a virus being introduced to your network via USB and you shut down all USB ports, you have avoided the risk.
- **Transference:** This involves transferring responsibility for the damages should the risk be realized. This is commonly done via cyber threat insurance.

- **Mitigation:** With this approach, which is the most common approach, you take steps to reduce either the likelihood of the event occurring or the impact. For example, if you are concerned about computer viruses, you might mitigate that via antivirus software and policies about attachments and links.

This is basic risk assessment. Before spending resources to address a threat, you must do this type of basic threat assessment. How likely is the threat to be realized? If it is realized, how much damage would it cause you? For example, I personally don't employ any security on my website. Yes, someone could hack it, but if they did, the impact would be negligible. There is no data on that website at all—no database back end, no files, no logins, and so on. The only information on the website is information I freely give to anyone, without even recording who gets the information. Thus, for this website, the impact of a breach is only negligible, thus making expenditure of resources on security unacceptable. At the other extreme are major e-commerce sites. These sites invest a great deal of resources on security because breach of such a website would immediately cost significant money and damage the organization's reputation in the long term.

Identifying Types of Threats

As discussed in the previous section, identifying your threats is a key part of risk assessment. Some threats are common to all networks; others are more likely with specific types of networks. Various sources have divided threats into different categories based on specific criteria. In this section we will examine threats that have been divided into categories based on the nature of the attack. Most attacks can be categorized as one of seven broad classes:

- **Malware:** This is a generic term for software that has a malicious purpose. It includes virus attacks, worms, adware, Trojan horses, and spyware. This is the most prevalent danger to your system. One reason the relatively generic term *malware* is now widely used is that many times a piece of malware does not fit neatly into one of these categories.
- **Security breaches:** This group of attacks includes any attempt to gain unauthorized access to your system. This includes cracking passwords, elevating privileges, breaking into a server...all the things you probably associate with the term *hacking*.
- **DoS attacks:** These are designed to prevent legitimate access to your system. And, as you will see in later chapters, this includes distributed denial of service (DDoS).
- **Web attacks:** This is any attack that attempts to breach your website. Two of the most common such attacks are SQL injection and cross-site scripting.
- **Session hijacking:** These attacks are rather advanced and involve an attacker attempting to take over a session.

- **Insider threats:** These are breaches based on someone who has access to your network misusing his access to steal data or compromise security.
- **DNS poisoning:** This type of attack seeks to compromise a DNS server so that users can be redirected to malicious websites, including phishing websites.

There are other attacks, such as social engineering. The foregoing list is just an attempt to provide a broad categorization of attack types. This section offers a broad description of each type of attack. Later chapters go into greater detail on each specific attack, how it is accomplished, and how to avoid it.

Malware

Malware is a generic term for software that has a malicious purpose. This section discusses four types of malware: viruses, Trojan horses, spyware, and logic bombs. Trojan horses and viruses are the most widely encountered. One could also include rootkits in the malware category, but these usually spread as viruses and thus are regarded as simply a specific type of virus.

According to Malwarebytes:

Malware, or “malicious software,” is an umbrella term that describes any malicious program or code that is harmful to systems. Hostile, intrusive, and intentionally nasty, malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device’s operations. Like the human flu, it interferes with normal functioning.”³

We still think primarily of computer viruses when we think of malware. The key characteristic of a computer virus is that it self-replicates. A computer virus is similar to a biological virus; both are designed to replicate and spread. The most common method for spreading a virus is using the victim’s email account to spread the virus to everyone in his address book. Some viruses don’t actually harm the system itself, but *almost all* of them cause network slowdowns due to the heavy network traffic caused by virus replication.

The *Trojan horse* gets its name from an ancient tale. The city of Troy was besieged for an extended period of time. The attackers could not gain entrance, so they constructed a huge wooden horse and one night left it in front of the gates of Troy. The next morning the residents of Troy saw the horse and assumed it to be a gift, so they rolled the wooden horse into the city. Unbeknownst to them, several soldiers were hidden inside the horse. That evening the soldiers left the horse, opened the city gates, and let their fellow attackers into the city. An electronic Trojan horse works similarly, appearing to be benign software but secretly downloading a virus or some other type of malware onto a computer from within.

3. <https://www.malwarebytes.com/malware/>

Another category of malware currently on the rise is *spyware*. Spyware is simply software that literally spies on what you do on your computer. Spyware can be as simple as a *cookie*—a text file that your browser creates and stores on your hard drive—that a website you have visited downloads to your machine and uses to recognize you when you return to the site. However, that flat file can then be read by the website or by other websites. Any data that the file saves can be retrieved by any website, so your entire Internet browsing history can be tracked. Spyware may also consist of software that takes periodic screenshots of the activity on your computer and sends them to the attacker.

Another form of spyware, called a *key logger*, records all of your keystrokes. Some key loggers also take periodic screenshots of your computer. Data is then either stored for later retrieval by the person who installed the key logger or is sent immediately back via email. We will discuss specific types of key loggers later in this book.

A *logic bomb* is software that lays dormant until some specific condition is met. That condition is usually a date and time. When the condition is met, the software does some malicious act, such as delete files, alter system configuration, or perhaps release a virus. In Chapter 5, “Malware,” we will examine logic bombs and other types of malware in detail.

Compromising System Security

Next we will look at attacks that breach your system’s security. This activity is commonly referred to as *hacking*, though that is not the term hackers themselves use. We will delve into appropriate terminology in just a few pages; however, it should be noted at this point that *cracking* is the appropriate word for intruding into a system without permission, usually with malevolent intent. Any attack that is designed to breach your security, either via some operating system flaw or any other means, can be classified as cracking.

Essentially any technique to bypass security, crack passwords, breach Wi-Fi, or in any way actually gain access to the target network fits into this category. That makes this a very broad category indeed.

However, not all breaches involve technical exploits. In fact, some of the most successful breaches are entirely nontechnical. *Social engineering* is a technique for breaching a system’s security by exploiting human nature rather than technology. This was the path that the famous hacker Kevin Mitnick most often used. Social engineering uses standard con techniques to get users to give up the information needed to gain access to a target system. The way this method works is rather simple: The perpetrator gets preliminary information about a target organization and leverages it to obtain additional information from the system’s users.

Following is an example of social engineering in action. Armed with the name of a system administrator, you might call someone in the business’s accounting department and claim to be one of the company’s technical support personnel. Mentioning the system administrator’s name would help validate that claim, allowing you to ask questions in an attempt to ascertain more details about the system’s specifications. A savvy intruder might even get the accounting person to say a username and password. As you can see, the success of this method is based on how well the prospective intruder can manipulate people and actually has little to do with computer skills.

The growing popularity of wireless networks gave rise to new kinds of attacks. One such activity is *war-driving*. This type of attack is an offshoot of *war-dialing*. With war-dialing, a hacker sets up a computer to call phone numbers in sequence until another computer answers to try to gain entry to its system. War-driving is much the same concept, applied to locating vulnerable wireless networks. In this scenario, the hacker simply drives around trying to locate wireless networks. Many people forget that their wireless network signal often extends as much as 100 feet (thus, past walls). At the 2004 DEF CON convention for hackers, there was a war-driving contest where contestants drove around the city trying to locate as many vulnerable wireless networks as they could. These sorts of contests are now common at various hacking conventions. (DEF CON is the largest and oldest hacking conference in the world.)

Recent technological innovations have introduced new variations of war driving/dialing. Now we have war flying. The attacker uses a small private drone equipped with Wi-Fi sniffing and cracking software, flies the drone in the area of interest, and attempts to gain access to wireless networks.

Of course, Wi-Fi hacking is only one sort of breach. Password cracking tools are now commonly available on the Internet. We will examine some of these later in this book. There are also exploits of software vulnerabilities that allow one to gain access to the target computer.

DoS Attacks

In a DoS, the attacker does not actually access the system. Rather, this person simply blocks access from legitimate users. One common way to prevent legitimate service is to flood the targeted system with so many false connection requests that the system cannot respond to legitimate requests. DoS is a very common attack because it is so easy.

In recent years a proliferation of DoS tools have been available on the Internet. One of the most common such tools is the Low Orbit Ion Cannon (LOIC). Because these tools can be downloaded for free from the Internet, anyone can execute a DoS attack, even without technical skill.

We also have variations, such as the DDoS attack. This attack uses multiple machines to attack the target. Given that many modern websites are hosted in network clusters or even in clouds, it is very difficult for a single attacking machine to generate enough traffic to take down a web server. But a network of hundreds or even thousands of computers certainly can. We will explore DoS and DDoS attacks in more detail in Chapter 4, “Denial of Service Attacks.”

Web Attacks

By their nature, web servers have to allow communications. Oftentimes, websites allow users to interact with the website. Any part of a website that allows for user interaction is also a potential point for attempting a web-based attack. SQL injections involve entering SQL (Structured Query Language) commands into login forms (username and password text fields) in an attempt to trick the server into executing those commands. The most common purpose is to force the server to log the attacker on, even though the attacker does not have a legitimate username and password. While SQL injection is just one type of web attack, it is the most common.

SQL Injection

SQL injection is still quite common, though it has been known for many years. Unfortunately, not enough web developers take the appropriate steps to remediate the vulnerabilities that make such an attack possible. Given the prevalence of this type of attack, it warrants a bit more detailed description.

Consider one of the simplest forms of SQL injection, used to bypass login screens. The website was developed in some web programming language, such as PHP or ASP.NET. The database is most likely a basic relational database such as Oracle, SQL Server, MySQL, or PostgreSQL is used to communicate with the database, so we need to put SQL statements into the web page that was written into some programming language. That will allow us to query the database and see if the username and password are valid.

SQL is relatively easy to understand; in fact, it looks a lot like English. There are commands like `SELECT` to get data, `INSERT` to put data in, and `UPDATE` to change data. In order to log in to a website, the web page has to query a database table to see if that username and password are correct. The general structure of SQL is like this:

```
select column1, column2 from tablename
```

or:

```
select * from tablename;
Conditions:
select columns from tablename where condition;
```

For example:

```
SELECT * FROM tblUsers WHERE USERNAME = 'jsmith'
```

This statement retrieves all the columns or fields from a table named `tblUsers` where the username is `jsmith`.

The problem arises when we try to put SQL statements into our web page. Recall that the web page was written in some web language such as PHP or ASP.NET. If you just place SQL statements directly in the web page code, an error will be generated. The SQL statements in the programming code for the website have to use quotation marks to separate the SQL code from the programming code. A typical SQL statement might look something like this:

```
"SELECT * FROM tblUsers WHERE USERNAME = '" + txtUsername.Text + ' AND PASSWORD = '" + txtPassword.Text + "'" .
```

If you enter username `'jdoe'` and the password `'password'`, this code produces this SQL command:

```
SELECT * FROM tblUsers WHERE USERNAME = 'jdoe' AND PASSWORD = 'password'
```

This is fairly easy to understand even for nonprogrammers. And it is effective. If there is a match in the database, that means the username and password match. If no records are returned from the database, that means there was no match, and this is not a valid login.

The most basic form of SQL injection seeks to subvert this process. The idea is to create a statement that will always be true. For example, instead of putting an actual username and password into the appropriate text fields, the attacker will enter ' or '1' = '1 into the username and password boxes. This will cause the program to create this query:

```
SELECT * FROM tblUsers WHERE USERNAME = '' or '1' = '1' AND PASSWORD = '' or  
'1' = '1'.
```

So you are telling the database and application to return all records where username and password are blank or if 1 = 1. It is highly unlikely that the username and password are blank. But I am certain that 1 = 1 always. Any true statement can be substituted. Examples are a = a and bob = bob.

The tragedy of this attack is that it is so easy to prevent. If the web programmer would simply filter all input prior to processing it, then this type of SQL injection would be impossible. Filtering means that before any user input is processed, the web page programming code looks through that code for common SQL injection symbols, scripting symbols, and similar items. It is true that each year fewer and fewer websites are susceptible to these attacks. However, there are still many sites that are vulnerable. SQL injection is still one of the top vulnerabilities found in websites according to OWASP (The Open Web Application Security Project). Subsequent chapters provide more coverage of most of these attacks, including tools used for them.

Cross-Site Scripting

Cross-site scripting is a type of attack that is closely related to SQL injection. It involves entering data other than what was intended, and its success depends on the web programmer not filtering input. The perpetrator finds some area of a website that allows users to type in text that other users will see and then instead injects client-side script into those fields.

Note

Before I describe this particular crime, I would point out that the major online retailers such as eBay and Amazon.com are not susceptible to this attack; they do filter user input.

To better understand this process, let's look at a hypothetical scenario. Let's assume that ABC Online Book Sales has a website. In addition to shopping, users can have accounts with credit cards stored, post reviews, and more. The attacker first sets up an alternate web page that looks as close to the real one as possible. Then the attacker goes to the real ABC Online Book Sales website and finds a rather popular book. He goes to the review section, but instead of typing in a review, he types in this:

```
<script> window.location = "http://www.fakesite.com"; </script>
```

Now when users go to that book, this script will redirect them to the fake site, which looks a great deal like the real one. The attacker then can have the website tell the user that his session has timed out and to please log in again. That would allow the attacker to gather a lot of account and password information. That is only one scenario, but it illustrates the attack.

Session Hijacking

Performing session hijacking can be rather complex. For that reason, it is not a very common form of attack. Simply put, the attacker monitors an authenticated session between the client machine and the server and takes over that session. We will explore specific methods of how this is done later in this book.

A 1985 paper written by Robert T. Morris, titled “A Weakness in the 4.2BSD Unix TCP/IP Software,” defined the original session hijacking. By predicting the initial sequence number, Morris was able to spoof the identity of a trusted client to a server. This is much harder to do today.

In addition to flags (syn, ack, syn-ack), the packet header will contain the sequence number that is intended to be used by the client to reconstitute the data sent over the stream in the correct order. (We will explore network packet flags in Chapter 2, “Networks and the Internet.”)

The Morris attack and several other session hijacking attacks require the attacker to be connected to the network and to simultaneously knock the legitimate user offline and then pretend to be that user. As you can probably imagine, it is a complex attack.

Insider Threats

Insider threats are a type of security breach. However, they present such a significant issue that we will deal with them separately. An insider threat occurs when someone inside your organization either misuses his access to data or accesses data he is not authorized to access.

The most obvious case is that of Edward Snowden. For our purposes, we can ignore the political issues connected with his case and instead focus solely on the issue of insiders accessing information and using it in a way other than what was authorized.

In 2009 Edward Snowden was working as a contractor for Dell, which manages computer systems for several U.S. government agencies. In March 2012 he was assigned to an NSA location in Hawaii. While there he convinced several people at that location to provide him with their login and password information, under the pretense of performing network administrative duties. Some sources dispute whether or not this is the specific method he used, but it is the one most widely reported. Whatever method he used, he accessed and downloaded thousands of documents that he was not authorized to access.

Again, ignoring the political issues and the content of the documents, our focus is on the security issues. Clearly, there were inadequate security controls in place to detect Edward Snowden’s activities and to prevent him from disclosing the content of confidential documents. While your organization may not have the high profile that the NSA has, any organization is susceptible to insider threats. Theft

of trade secrets by insiders is a common business concern and has been the focus of many lawsuits against former employees. In both Chapter 7, “Industrial Espionage in Cyberspace,” and Chapter 9, “Computer Security Technology,” we will see some countermeasures to mitigate this threat.

While Edward Snowden is an obvious example of insider threats, that is only one example. A common scenario is when someone who has legitimate access to some particular source of data chooses either to access data he is not authorized to access or to use the data in a manner other than how he has been authorized to use it. Here are a few examples:

- A hospital employee who accesses patient records to use the data to steal a patient’s identity, or someone with no access at all who accesses records
- A salesperson who takes a list of contacts with him when he leaves the company

This is actually a much greater problem than many people appreciate. Within an organization, information security is often more lax than it should be. Most people are more concerned with external security than internal security, so it is often rather easy to access data within an organization. In my career as a security consultant, I have seen networks where sensitive data is simply placed on a shared drive with no limiting of access to it. That means anyone on the network can access that data. In a case such as this, when information is taken, no crime has been committed. However, in other cases, employees purposefully circumvent security measures to access data they are not authorized to. The most common method is to simply log in with someone else’s password. That enables the perpetrator to access the resources and data to which that other person has been granted access. Unfortunately, many people use weak passwords or, worse, they write their password somewhere on their desk. Some users even share passwords. For example, suppose a sales manager is out sick but wants to check to see if a client has emailed her. So she calls her assistant and gives him her login so he can check her email. This sort of behavior should be strictly prohibited by company security policies, but it still occurs. The problem is that now two people have the sales manager’s login. Either one could use it or reveal it to someone else (accidentally or on purpose). So there is a greater chance of someone using that manager’s login to access data he has not been authorized to access.

DNS Poisoning

Most of your communication on the Internet will involve DNS, or Domain Name System. DNS is what translates the domain names you and I understand (like www.ChuckEasttom.com) into IP addresses that computers and routers understand. DNS poisoning uses one of several techniques to compromise that process and redirect traffic to an illicit site, often for the purpose of stealing personal information.

Here is one scenario whereby an attacker might execute a DNS poisoning attack: First the attacker creates a phishing website. It spoofs a bank that we will call ABC Bank. The attacker wants to lure users there so he can steal their passwords and use them on the real bank website. Since many users are too smart to click on links, he will use DNS poisoning to trick them.

The attacker creates his own DNS server. (Actually, this part is relatively easy.) Then he puts two records in that DNS server. The first is for the ABC Bank website, pointing to his fake site rather than the real

bank site. The second entry is for a domain that does not exist. The attacker can search domain registries until he finds one that does not exist. For illustration purposes, we will refer to this as XYZ domain.

Then the attacker sends a request to a DNS server on the target network. That request purports to be from any IP address within the target network and is requesting the DNS server resolve the XYZ domain.

Obviously, the DNS server does not have an entry for the XYZ domain since it does not exist. So, it begins to propagate the request up its chain of command and eventually to its service provider DNS server. At any point in that process, the attacker sends a flood of spoofed responses claiming to be from a DNS server that the target server is trying to request records from but that are actually coming from his DNS server and offering the IP address for XYZ domain. At that point the hacker's DNS server offers to do a zone transfer, exchanging all information with the target server. That information includes the spoofed address for ABC Bank. Now the target DNS server has an entry for ABC Bank that points to the hacker's website rather than the real ABC Bank website. Should users on that network type in the URL for ABC Bank, their own DNS server will direct them to the hacker's site.

This attack, like so many, depends on vulnerabilities in the target system. A properly configured DNS server should never perform a zone transfer with any DNS server that is not already authenticated in the domain. However, the unfortunate fact is that there are plenty of DNS servers that are not properly configured.

New Attacks

Many of the threats discussed in the first three editions of this book are still plaguing network security. Malware, DoS, and other such attacks are just as common today as they were 5 years ago or even 10 years ago.

One new phenomenon is *doxing*, which is the process of finding personal information about an individual and broadcasting it, often via the Internet. This can be any personal information about any person. However, it is most often used against public figures. It has even been the case that a previous director of the CIA was the target of doxing.⁴

Hacking of medical devices is another new type of attack. Hacker Barnaby Jack first revealed a vulnerability in an insulin pump that could allow an attacker to take control of the pump and cause it to dispense the entire reservoir of insulin in a single dose, thus killing the patient. To date there are no confirmed incidents of this having actually been done, but it is disturbing nonetheless. Similar security flaws have been found in pacemakers. In 2018, the U.S. Food and Drug Administration (FDA) published a list of medical devices that are not secure. So, this problem appears to be getting worse.

In July 2015 it was revealed that Jeep vehicles could be hacked and shut down during normal operation. This means that a hacker could cause a Jeep to stop in the middle of heavy, high-speed traffic, potentially causing a serious automobile accident. The hacking of cars has become more widespread. DEF CON in 2016 had a car hacking village.

4. <http://gawker.com/wikileaks-just-doxxed-the-head-of-the-cia-1737871619>

More recently, the Internet of Things has created a new set of targets for attackers. Smart homes and offices, with their integrated Internet-enabled devices, make attractive targets for attackers. For example, ransomware has been created for smart thermostats.

All of these attacks show a common theme: As our lives become more interconnected with technology, new vulnerabilities emerge. Some of these vulnerabilities are not merely endangering data and computer systems but potentially endangering lives.

Assessing the Likelihood of an Attack on Your Network

How likely are these attacks? What are the real dangers facing you as an individual or your organization? What are the most likely attacks, and what are your vulnerabilities? Let's take a look at what threats are out there and which ones are the most likely to cause you or your organization problems.

At one time, the most likely threat to individuals and large organizations was the computer virus. And it is still true that in any given month, several new virus outbreaks will be documented. New viruses are being created all the time, and old ones are still out there. However, there are other very common attacks, such as spyware. Spyware is quickly becoming an even bigger problem than viruses.

After viruses, the most common attack is unauthorized usage of computer systems. Unauthorized usage includes everything from DoS attacks to outright intrusion of your system. It also includes internal employees misusing system resources. The first edition of this book referenced a survey by the Computer Security Institute of 223 computer professionals showing over \$445 million in losses due to computer security breaches. In 75% of the cases, an Internet connection was the point of attack, while 33% of the professionals cited the location as their internal systems. A rather astonishing 78% of those surveyed detected employee abuse of systems/Internet. This statistic means that in any organization, one of the chief dangers might be its own employees. In 2019 similar threats still exist, with only slight changes in the percentages.

The 2014 Data Breach Investigation Report from Verizon surveyed 63,437 security incidents with 1367 confirmed breaches in 95 countries. This survey showed significant employee abuse of the network as well as many of the familiar attacks we have already discussed in this chapter. The 2015 Data Breach Investigation Report did not show significant improvement. In 2019, the situation was not improved. In fact, as mentioned earlier in the chapter, it is expected that cybercrime will cost more than \$1 trillion per year.

Basic Security Terminology

Before you embark on the rest of this chapter and this book, it is important to know some basic terminology. The security and hacking terms in this section provide a basic introduction to computer security terminology, but they are an excellent starting point to help you prepare for learning more

about computer security. Additional terms will be introduced throughout the text and listed in the Glossary at the end of this book.

The world of computer security takes its vocabulary from both the professional security community and the hacker community.

Hacker Slang

You probably have heard the term *hacker* used in movies and in news broadcasts. Most people use it to describe any person who breaks into a computer system. In the hacking community, however, a *hacker* is an expert on a particular system or systems, a person who simply wants to learn more about the system. Hackers feel that looking at a system's flaws is the best way to learn about that system. For example, someone well versed in the Linux operating system who works to understand that system by learning its weaknesses and flaws would be a hacker.

This process does often mean seeing if a flaw can be exploited to gain access to a system. This "exploiting" part of the process is where hackers differentiate themselves into three groups:

- A *white hat hacker*, upon finding some flaw in a system, will report the flaw to the vendor of that system. For example, if a white hat hacker were to discover some flaw in Red Hat Linux, he would email the Red Hat company (probably anonymously) and explain exactly what the flaw is and how it was exploited. White hat hackers are often hired specifically by companies to do penetration tests. The EC Council even has a certification test for white hat hackers: the Certified Ethical Hacker test.
- A *black hat hacker* is the person normally depicted in the media. Once she gains access to a system, her goal is to cause some type of harm. She might steal data, erase files, or deface websites. Black hat hackers are sometimes referred to as *crackers*.
- A *gray hat hacker* is normally a law-abiding citizen but in some cases will venture into illegal activities.

Regardless of how hackers view themselves, intruding on any system is illegal. This means that technically speaking all hackers, regardless of the color of the metaphorical hat they may wear, are in violation of the law. However, many people feel that white hat hackers actually perform a service by finding flaws and informing vendors before those flaws are exploited by less ethically inclined individuals.

Script Kiddies

A hacker is an expert in a given system. As with any profession, it includes its share of frauds. So, what is the term for someone who calls himself a hacker but lacks the expertise? The most common term for this sort of person is *script kiddie*). Yes, that is an older resource, but the term still means the same thing. The name comes from the fact that the Internet is full of utilities and scripts that one can download

to perform some hacking tasks. Many of these tools have easy-to-use graphical user interfaces that allow those with very little or no skill to operate them. A classic example is the Low Orbit Ion Cannon tool for executing a DoS attack. Someone who downloads such a tool without really understanding the target system is considered a script kiddy. A significant number of the people you are likely to encounter who call themselves hackers are, in reality, mere script kiddies.

Ethical Hacking: Penetration Testers

When and why would someone give permission to another party to hack his system? The most common answer is in order to assess system vulnerabilities. Such a person used to be called a *sneaker*, but now the term *penetration tester* is far more widely used. Whatever the term, the person legally breaks into a system in order to assess security deficiencies, as portrayed in the 1992 film *Sneakers*, starring Robert Redford, Dan Aykroyd, and Sidney Poitier. More and more companies are soliciting the services of such individuals or firms to assess their vulnerabilities.

Anyone hired to assess the vulnerabilities of a system should be both technically proficient and ethical. Run a criminal background check and avoid those people with problematic pasts. There are plenty of legitimate security professionals available who know and understand hacker skills but have never committed security crimes. If you take to its logical conclusion the argument that hiring convicted hackers means hiring talented people, you could surmise that obviously those in question are not as good at hacking as they would like to think because they were caught.

Most importantly, giving a person with a criminal background access to your systems is on par with hiring a person with multiple DWI convictions to be your driver. In both cases, you are inviting problems and perhaps assuming significant civil liabilities.

Also, some review of their qualifications is clearly in order. Just as there are people who claim to be highly skilled hackers yet are not, there are those who will claim to be skilled penetration testers yet lack the skills truly needed. You would not want to inadvertently hire a script kiddy who thinks she is a penetration tester. Such a person might then pronounce your system quite sound when, in fact, it was simply a lack of skills that prevented the script kiddy from successfully breaching your security. Later in this book, in Chapter 11, “Network Scanning and Vulnerability Scanning,” we discuss the basics of assessing a target system. In Chapter 11 we also discuss the qualifications you should seek in any consultant you might hire for this purpose.

Phreaking

One specialty type of hacking involves breaking into telephone systems. This subspecialty of hacking is referred to as *phreaking*. The *New Hacker’s Dictionary* actually defines phreaking as “the action of using mischievous and mostly illegal ways in order to not pay for some sort of telecommunications bill, order, transfer, or other service” Phreaking requires a rather significant knowledge of telecommunications, and many phreakers have some professional experience working for a phone company or other telecommunications business. Often this type of activity is dependent upon specific technology required to compromise phone systems more than simply knowing certain techniques.

Professional Terms

Most hacker terminology, as you may have noticed, is concerned with the activity (phreaking) or the person performing the activity (penetration tester). In contrast, security professional terminology describes defensive barrier devices, procedures, and policies. This is quite logical because hacking is an offensive activity centered on attackers and attack methodologies, whereas security is a defensive activity concerned with defensive barriers and procedures.

Security Devices

The most basic security device is the *firewall*. A firewall is a barrier between a network and the outside world. Sometimes a firewall takes the form of a standalone server, sometimes a router, and sometimes software running on a machine. Whatever its physical form, a firewall filters traffic entering and exiting the network. A *proxy server* is often used with a firewall to hide the internal network's IP address and present a single IP address (its own) to the outside world.

Firewalls and proxy servers guard the perimeter by analyzing traffic (at least inbound traffic and in many cases outbound traffic as well) and blocking traffic that has been disallowed by the administrator. These two safeguards are often augmented by an *intrusion detection system* (IDS). An IDS simply monitors traffic, looking for suspicious activity that might indicate an attempted intrusion. We will examine these technologies and others in Chapter 9.

Security Activities

In addition to devices, there are security activities. *Authentication* is the most basic security activity. It is merely the process of determining if the credentials given by a user or another system (such as a username and password) are authorized to access the network resource in question. When you log in with your username and password, the system will attempt to authenticate that username and password. If it is authenticated, you will be granted access.

Another crucial safeguard is *auditing*, which is the process of reviewing logs, records, and procedures to determine if these items meet standards. This activity will be mentioned in many places throughout this book and will be a definite focus in a few chapters.

The security and hacking terms that we have just covered are only an introduction to computer security terminology, but they provide an excellent starting point that will help you prepare for learning more about computer security. Additional terms will be introduced throughout the text as needed and compiled in the Glossary at the end of the book.

Concepts and Approaches

The approach you take toward security influences all subsequent security decisions and sets the tone for the entire organization's network security infrastructure. Before we delve into various network security paradigms, let us take a moment to examine a few concepts that should permeate your thinking about security.

The first concept is the *CIA triangle*. This does not refer to clandestine operations involving the Central Intelligence Agency; rather, it is a reference to the three pillars of security: confidentiality, integrity, and availability. When you are thinking about security, your thought processes should always be guided by these three principles. First and foremost, are you keeping the data confidential? Does your approach help guarantee the integrity of data? And does your approach still make the data readily available to authorized users?

While the CIA triangle is a staple of all security courses and certifications, more sophisticated models have been developed. A multi-faceted approach to describing security is found in The McCumber cube. The McCumber cube is a way of evaluating security of a network, looking at all aspects. It was described in detail in 2004 in the book *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*. It looks at security as a three-dimensional cube. The dimensions are goals, information states, and safeguards. The McCumber cube has the advantage of being a natural expansion of the CIA triangle into three dimensions. This is advantageous because the CIA triangle is widely known and understood in the cyber-security community. This makes the transition to the McCumber cube, and subsequently a taxonomy based on the McCumber cube, easier. Any taxonomy must be readily learned and applied by security professionals in order to be effective. You can see the McCumber cube in Figure 1.1:

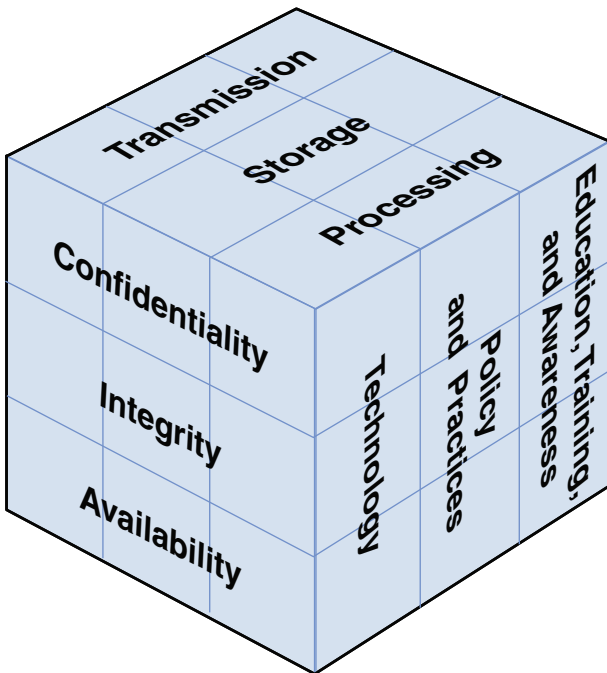


FIGURE 1.1 The McCumber cube.

Another important concept to keep in mind is *least privileges*. This means that each user or service running on your network should have the least number of privileges/access required to do her job. No one should be granted access to anything unless it is absolutely required for the job.

Network security paradigms can be classified based on either the scope of security measures taken (perimeter, layered) or how proactive the system is.

In a *perimeter security approach*, the bulk of security efforts are focused on the perimeter of the network. This focus might include firewalls, proxy servers, password policies, or any technology or procedure to make unauthorized access of the network less likely. Little or no effort is put into securing the systems within the network. In this approach, the perimeter is secured, but the various systems within that perimeter are often vulnerable.

There are additional issues regarding perimeter security that include physical security. These issues can include fences, closed-circuit TV, guards, locks, and so on, depending on the security needs of the organization.

The perimeter approach is clearly flawed, so why do some companies use it? Small organizations might use the perimeter approach if they have budget constraints or inexperienced network administrators. A perimeter method might be adequate for small organizations that do not store sensitive data, but it rarely works in a larger corporate setting.

A *layered security approach* is one in which not only is the perimeter secured, but individual systems within the network are also secured. All servers, workstations, routers, and hubs within the network are secure. One way to accomplish this is to divide the network into segments and secure each segment as if it were a separate network, so if the perimeter security is compromised, not all the internal systems are affected. This is the preferred method and should be used whenever possible.

You should also measure your security approach by how proactive/reactive it is. This is done by gauging how much of the system's security infrastructure and policies are dedicated to preventive measures and how much of the security system is designed to respond to attack. A passive security approach takes few or no steps to prevent an attack. A dynamic or proactive defense is one in which steps are taken to prevent attacks before they occur.

One example of this defense is the use of IDSs, which work to detect attempts to circumvent security measures. These systems can tell a system administrator that an attempt to breach security has been made, even if that attempt is not successful. IDSs can also be used to detect various techniques intruders use to assess a target system, thus alerting a network administrator to the potential for an attempted breach before the attempt is even initiated.

In the real world, network security is usually not completely in one paradigm or another; it is usually a hybrid approach. Networks generally include elements of both security paradigms. The two categories also combine. One can have a network that is predominantly passive but layered or one that is primarily perimeter but proactive. It can be helpful to consider approaches to computer security along a Cartesian coordinate system, as illustrated in Figure 1.2, with the x axis representing the level of passive–active approaches and the y axis depicting the range from perimeter to layered defense.

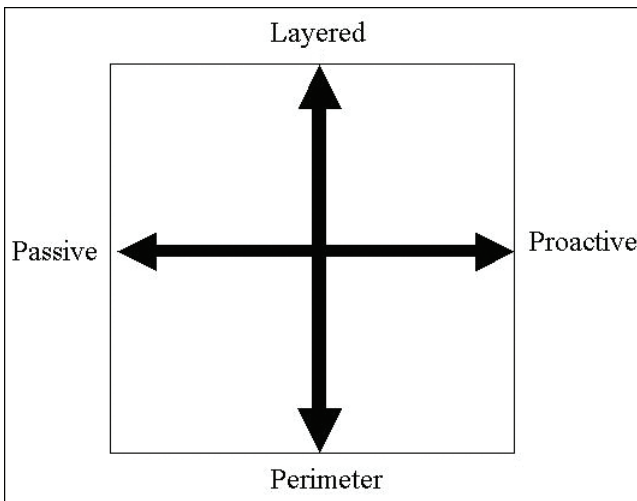


FIGURE 1.2 The security approach guide.

The most desirable hybrid approach is a layered paradigm that is dynamic—that is, in the upper-right quadrant of the figure.

How Do Legal Issues Impact Network Security?

An increasing number of legal issues affect how one approaches computer security. If your organization is a publicly traded company or a government agency or does business with either one, there may be legal constraints regarding your network security. Even if your network is not legally bound to these security guidelines, it's useful to understand the various laws impacting computer security. You may choose to apply them to your own security standards.

One of the oldest pieces of legislation in the United States that affects computer security is the Computer Security Act of 1987. It requires government agencies to identify sensitive systems, conduct computer security training, and develop computer security plans. This law was a vague mandate ordering federal agencies in the United States to establish security measures, but it did not specify standards.

This legislation established a legal mandate to enact specific standards, paving the way for future guidelines and regulations. It also helped define terms, such as what information is considered “sensitive.” This quote is found in the legislation itself:

The term “sensitive information” means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

This definition of the word *sensitive* should be kept in mind because it indicated that more than just Social Security information and medical history information must be secured.

When considering what information needs to be secured, simply answer this question: Would the unauthorized access or modification of this information adversely affect your organization? If the answer is yes, then you must consider that information sensitive and in need of security precautions.

Another more specific federal law that applied to mandated security for government systems was OMB Circular A-130 (specifically, Appendix III). This document required that federal agencies establish security programs containing specified elements. It also described requirements for developing standards for computer systems and for records held by government agencies.

Most states have specific laws regarding computer security, such as legislation like the Computer Crimes Act of Florida, the Computer Crime Act of Alabama, and the Computer Crimes Act of Oklahoma. If you're responsible for network security, you might find yourself part of a criminal investigation. This could be an investigation into a hacking incident or employee misuse of computer resources. A list of computer crime laws (organized by state) can be found at <http://criminal.findlaw.com/criminal-charges/cyber-crimes.html>.

Caution

Privacy Laws

It is critical to keep in mind that any law that governs privacy (such as the Health Insurance Portability and Accountability Act of 1996 [HIPAA]) also has a direct impact on computer security. If your system is compromised, and thus data that is covered under any privacy statute is compromised, you may need to prove that you exercised due diligence in protecting that data. If it can be shown that you did not take proper precautions, you might be found civilly liable.

Online Security Resources

As you read this book, and when you move out into the professional world, you will have frequent need for additional security resources. Appendix A, "Resources," includes a more complete list of resources, but this section highlights a few of the most important ones you may find useful now.

CERT

The *Computer Emergency Response Team* (CERT; www.cert.org) is sponsored by Carnegie-Mellon University. CERT was the first computer incident-response team, and it is still one of the most respected in the industry. Anyone interested in network security should visit the site routinely. On the website you will find a wealth of documentation, including guidelines for security policies, cutting-edge security research, and more.

Microsoft Security Advisor

Because so many computers today run Microsoft operating systems, another good resource is the Microsoft Security Advisor website: <https://www.microsoft.com/en-us/msrc?rtc=1>. This site is a portal to all Microsoft security information, tools, and updates. If you use any Microsoft software, you should visit this website regularly.

F-Secure

The F-Secure corporation maintains a website at www.f-secure.com. This site is, among other things, a repository for detailed information on virus outbreaks. Here you will find not only notifications about a particular virus but detailed information about the virus, such as how the virus spreads, and ways to recognize the virus, and, possibly, specific tools for cleaning an infected system of a particular virus.

SANS Institute

The SANS Institute website (www.sans.org) is a vast repository of security-related documentation. On this site you will find detailed documentation on virtually every aspect of computer security you can imagine. The SANS Institute also sponsors a number of security research projects and publishes information about those projects on its website.

Summary

Network security is a complex and constantly evolving field. Practitioners must stay on top of new threats and solutions and be proactive in assessing risk and protecting their networks. The first step to understanding network security is to become acquainted with the actual threats posed to a network. Without a realistic idea of what threats might affect your systems, you will be unable to effectively protect them. It is also critical that you acquire a basic understanding of the terminology used by both security professionals and those who would seek to compromise your security.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. You are trying to explain security to a nontechnical manager. She has taken a rather extreme view of computer security. Which of the following is one of the extreme viewpoints about computer security discussed in this chapter?
 - A. The federal government will handle security.
 - B. Microsoft will handle security.
 - C. There are no imminent dangers to your system.
 - D. There is no danger if you use Linux.
2. You have just taken over as network security administrator for a small community college. You want to take steps to secure your network. Before you can formulate a defense for a network, what do you need?
 - A. Appropriate security certifications
 - B. A clear picture of the dangers to be defended against
 - C. To finish this textbook
 - D. The help of an outside consultant
3. Mary is teaching an introductory cybersecurity course to freshmen. She is explaining to them the major threats. Which of the following is not one of the three major classes of threats?
 - A. Attempts to intrude on the system
 - B. Online auction fraud
 - C. Denial of service attacks
 - D. A computer virus

4. Being able to define attack terms is an important skill for a cybersecurity professional. What is a computer virus?
 - A. Any program that is downloaded to your system without your permission
 - B. Any program that self-replicates
 - C. Any program that causes harm to your system
 - D. Any program that can change your Windows Registry

5. Being able to define attack terms is an important skill for a cybersecurity professional. What is spyware?
 - A. Any software that monitors your system
 - B. Only software that logs keystrokes
 - C. Any software used to gather intelligence
 - D. Only software that monitors what websites you visit

6. What is a penetration tester?
 - A. A person who hacks a system without being caught
 - B. A person who hacks a system by faking a legitimate password
 - C. A person who hacks a system to test its vulnerabilities
 - D. A person who is an amateur hacker

7. Elizabeth is explaining various hacking terms to a class. She is in the process of discussing the history of phone system hacking. What is the term for hacking a phone system?
 - A. Telco-hacking
 - B. Hacking
 - C. Cracking
 - D. Phreaking

8. What is malware?
 - A. Software that has some malicious purpose
 - B. Software that is not functioning properly
 - C. Software that damages your system
 - D. Software that is not properly configured for your system

9. What is war-driving?
 - A. Driving and seeking a computer job
 - B. Driving while using a wireless connection for hacking
 - C. Driving looking for wireless networks to hack
 - D. Driving and seeking rival hackers
10. What is the name for the hacking technique that involves using persuasion and deception to get a person to provide information to help compromise security?
 - A. Social engineering
 - B. Conning
 - C. Human intel
 - D. Soft hacking
11. There are many threats on the Internet. Which one is currently the most common may change over time, but certain threats have always been more common than others. Which of the following is the most common threat on the Internet?
 - A. Auction fraud
 - B. Phreaking
 - C. Computer viruses
 - D. Illegal software
12. What are the three approaches to security?
 - A. Perimeter, layered, hybrid
 - B. High security, medium security, low security
 - C. Internal, external, and hybrid
 - D. Perimeter, complete, none
13. Defining your security strategy is an important step in securing a network. You are trying to classify devices based on the approach they take to security. An intrusion detection system is an example of which of the following?
 - A. Proactive security
 - B. Perimeter security
 - C. Hybrid security
 - D. Good security practices

14. Which of the following is the most basic security activity?
 - A. Authentication
 - B. Firewalls
 - C. Password protection
 - D. Auditing

15. The most desirable approach to security is one that is which of the following?
 - A. Perimeter and dynamic
 - B. Layered and dynamic
 - C. Perimeter and static
 - D. Layered and static

16. According to a survey of 223 computer professionals prepared by the Computer Security Institute, which of the following was most often cited as an issue by respondents?
 - A. Internal systems
 - B. Employee abuse
 - C. Routers
 - D. Internet connection

17. Which of the following types of privacy law affects computer security?
 - A. Any state privacy law
 - B. Any privacy law applicable to your organization
 - C. Any privacy law
 - D. Any federal privacy law

18. The first computer incident-response team is affiliated with what university?
 - A. Massachusetts Institute of Technology
 - B. Carnegie-Mellon University
 - C. Harvard University
 - D. California Technical University

19. Which of the following is the best definition of the term *sensitive information*?
 - A. Any information that has an impact on national security
 - B. Any information that is worth more than \$1,000
 - C. Any information that if accessed by unauthorized personnel could damage your organization in any way
 - D. Any information that is protected by privacy laws

20. Which of the following is a major resource for detailed information on a computer virus?
- A. The MIT Virus Library
 - B. The Microsoft Virus Library
 - C. The F-Secure Virus Library
 - D. The National Virus Repository

EXERCISES

EXERCISE 1.1: How Many Virus Attacks Have Occurred This Month?

1. Using some website resource, such as www.f-secure.com, look up recent computer virus outbreaks.
2. How many virus outbreaks have occurred in the past 7 days?
3. Write down how many outbreaks have occurred in the past 30 days, 90 days, and 1 year.
4. Are virus attacks increasing in frequency?

EXERCISE 1.2: Learning About Cookies as Spyware

1. Get an idea of what kind of information cookies store. You might find the following websites helpful:
www.allaboutcookies.org
www.howstuffworks.com/cookie1.htm
2. Write a brief essay explaining in what way cookies can invade privacy.

EXERCISE 1.3: Hacker Terminology

1. Use the *Hacker's Dictionary* at http://www.outpost9.com/reference/jargon/jargon_toc.html to define the following hacker terms:
 - A. Alpha geek
 - B. Grok
 - C. Red Book
 - D. Wank

EXERCISE 1.4: Using Security Resources

1. Using one of the preferred web resources listed in this chapter, find three policy or procedure documents from that resource.
2. List the documents you selected.
3. Write a brief essay explaining why those particular documents are important to your organization's security.

EXERCISE 1.5: Learning About the Law

1. Using the Web, journals, books, or other resources, find out if your state or territory has any laws specific to computer security. You might find the following websites helpful:

www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html

www.cybercrime.gov

2. List three laws that you find for your region and provide a brief one- or two-sentence description of each.

PROJECTS**PROJECT 1.1: Learning About a Virus**

1. Using web resources from Appendix A and sites such as www.f-secure.com, find a virus that has been released in the past 6 months.
2. Research how the virus spread and what damage it caused.
3. Write a brief (half to one page) paper on this virus. Explain how the virus worked, how it spread, and any other essential information you can find.

PROJECT 1.2: Considering the Law (a Group Project)

Write a description of a computer law that you would like to have passed, along with specifics related to its implementation, enforcement, and justification.

PROJECT 1.3: Recommending Security

1. Using the Web, journals, or books, locate security recommendations from any reputable source, such as the SANS Institute. Any of the sites mentioned in the “Online Security Resources” section of this chapter would be a good choice.

2. List five of those recommendations.
3. Explain why you agree or disagree with each of these five recommendations.

Case Study

In this case study we will consider a network administrator for a small, family-oriented video store. The store is not part of a chain of stores and has a very limited security budget. It has five machines for employees to use to check out movies and one server on which to keep centralized records. That server is in the manager's office. The administrator takes the following security precautions:

- Each machine is upgraded to Windows 10, with the personal firewall turned on.
- Antivirus software has been installed on all machines.
- A tape backup is added to the server, and tapes are kept in a file cabinet in the manager's office.
- Internet access to employee machines is removed.

Now consider these questions:

1. What have these actions accomplished?
2. What additional actions might you recommend?

Symbols

- # (pound sign), 260
- 2G, 409
- 2nd Thought, 137
- 3DES (Triple DES), 219
- 3G, 409
- 4G, 409
- 56-bit cipher key (DES), 217
- 60 Minutes, 351
- 802.11 standard, 36–37

A

- abelian groups, 221
- Absolute Keylogger, 135
- Abvast, 142
- acceptance of risk, 6
- access control, 292–293
- AccessData Forensic Toolkit, 388–391, 396
- active IDSs (intrusion detection systems), 255
- active scanning
 - active code scanning, 247
 - enumeration, 159–160
 - MBSA (Microsoft Baseline Security Analyzer), 321–323
 - Nessus, 324–326
 - OWASP (Open Web Application Security Project), 326–327
 - port scanning, 155–158

- Shodan, 160–162, 328–329
- vulnerability assessment, 158–159
- activities, IDS, 256**
- Address Resolution Protocol (ARP), 54–55**
- addresses**
 - IPv4
 - CIDR (classless interdomain routing), 44
 - loopback addresses, 42
 - network classes, 41–43
 - public versus private, 43
 - subnetting, 43–44
 - IPv6, 44–45
 - MAC (Media Access Control), 35, 57
- AddRoundKey step (AES), 220**
- Adleman, Len, 224**
- Advanced Encryption Standard (AES), 38, 220–222**
- advanced persistent threats (APTs), 139–140, 344–345**
- Advanced Research Projects Agency (ARPA), 48**
- adware, 137**
- AES (Advanced Encryption Standard), 38, 220–222**
- AFCC (Air Force Cyber Command), 343**
- Agent.btz, 344**
- AHs (authentication headers), 270**
- Air Force Cyber Command (AFCC), 343**
- Airbus, 357**
- ALE (Annualized Loss Expectancy), 6**
- alerts, IDS, 256**
- algorithms**
 - Diffie-Hellman, 227
 - ElGamal, 227
 - Elliptic Curve, 228
 - HMAC, 231–232
 - MAC, 231–232
 - MD5, 231
 - MQV, 227
 - RIPEMD, 231
 - RSA, 224–227
 - SHA, 231
- Allen, James, 76**
- Amazon, 12**
- The Amnesiac Incognito Live System (TAILS), 175**
- amplifiers, 35**
- analyzers, IDS, 256**
- AND operation, 214**
- Android, forensics fr, 410–411**
- Annualized Loss Expectancy (ALE), 6**
- ANT+38**
- antispymware software, 194, 253–254**
- antivirus software, 140–143, 248**
- Apple Inc., industrial espionage at, 183**
- Apple Viruses, 128**
- application gateways, 250**
- Application log, 398**
- application proxies, 250**
- apport.log file, 399**
- APTs (advanced persistent threats), 139–140, 344–345**
- armored viruses, 122**
- ARP (Address Resolution Protocol), 54–55**
- ARPA (Advanced Research Projects Agency), 48**
- ARPANET, 48**
- ASs (authentication servers), 264**
- assessment, system security**
 - patches, 307–308
 - physical security, 314–315
 - policies, 312–314
 - ports, 308–311
 - probes, 314
 - protective software and devices, 311–312
- asset identification, 184–187**
- asymmetric algorithms**
 - Diffie-Hellman, 227
 - ElGamal, 227

Elliptic Curve, 228
 MQV, 227
 RSA, 224–227
asymmetric encryption. See public key encryption
Asynchronous Transfer Mode (ATM), 269
Atbash cipher, 211
Atlanta, ransomware attack in, 125
ATM (Asynchronous Transfer Mode), 269
attachments, security policies for, 283–284
attacks. See threats
auction fraud
 protecting against, 87–88
 types of, 70–72
audit trails, 394
auditing, 19
auditpol, 398
authentication, 19, 262–265
authentication headers (AHs), 270
authentication servers (ASs), 264
autostart locations, 407
AVG, 129
AVG AntiVirus, 248
AVG antivirus, 142
avoidance of risk, 6

B

backups, 296–297
bandwidth, 34–35
Barriss, Tyler, 78
BCPs (business continuity plans), 295–296
Bellaso, Giovan Battista, 212
Berners-Lee, Tim, 49
BIA (business impact assessment), 296
bid shielding, 71
bid siphoning, 71–72
.bin files, 416
binary numbers, converting, 41
binary operations, 214

BitLocker, 195
bits, 34–35, 38–39
black hat hackers, 17, 152–153
black holes, 112
BlackEnergy, 347, 357
blackmail, DoS (denial of service) attacks, 111
block ciphers
 Blowfish, 222
 defined, 217
 Serpent, 222
 Skipjack, 222
 Twofish, 220
Blowfish, 222
blue jacking, 166
blue teams, 153
bluebugging, 166
bluesnarfing, 166
Bluetooth, 38
boot sector viruses, 123
Bosselaers, Antoon, 231
***Boston Globe* attack, 109**
botnets, 109
breaches, defined, 7
Bring Your Own Device (BYOD), 285
Broadband Guide, 311
browser forensics, 397–398
browser security, 84–87
brute force, 210
brute force techniques, 235
Budapest Convention on Cybercrime, 394–395
buffer-overflow attacks
 explained, 132–133
 Sasser, 133–134
buffers, 132–133
Bureau of Federal Prisons, 378
business continuity
 BCPs (business continuity plans), 295–296
 standards, 296

business continuity plans (BCPs), 295–296
 business continuity standards, 296
 business impact assessment (BIA), 296
 BYOD (Bring Your Own Device), 285
 bytes, 38–39

C

CAB (change approval board) process, 289
 cables, 33–35
 Caesar cipher, 209–210
 Cain and Abel, 159
 CAPTCHA, 108
 carriers, 233
 CAs (certificate authorities), 265–266
 CASP (CompTIA Advanced Security Practitioner), 6, 331
 CBC (cipher block chaining) mode, 223
 CBI (Central Bureau of Investigation), 344
 CCB (change control board) process, 289
 CCMP (Cipher Block Chaining Message Authentication Code Protocol), 38, 271
 cell phones
 Android, 410–411
 attacks on, 166
 cellular networks, 409
 general principles, 412
 ICCID (Integrated Circuit Card Identification), 408
 IMSI (International Mobile Subscriber Identity), 408
 iOS, 410
 SIM (Subscriber Identity Module), 408
 Windows, 411
Cellebrite, 397
 cellular networks, 409
CENTCOM, 344
 Center for Internet Security, 315
 Center for Strategic and International Studies, 3, 357
 Central Bureau of Investigation (CBI), 344
 Cerf, Vince, 48
 CERT (Computer Emergency Response Team), 23, 128
 certificate authorities (CAs), 265–266
 certificate revocation lists (CRLs), 266
 certificates, digital, 265–266
 certifications, 6, 152, 330–332, 413–414
 Certified Advanced Security Practitioner (CASP), 331
 Certified Ethical Hacker, 331
 Certified Forensic Computer Examiner (CFCE), 413
 Certified Information Systems Auditor (CISA), 6
 Certified Information Systems Security Professional (CISSP), 6, 331
 CGNPC (China General Nuclear Power Company), 188
 chain of custody, 392
 Challenge Handshake Authentication Protocol (CHAP), 262, 269
 change approval board (CAB) process, 289
 change control board (CCB) process, 289
 change requests, 288–290
 channels, 233
 CHAP (Challenge Handshake Authentication Protocol), 262, 269
 Chen, Jizhong, 183
 CHFI (Computer Hacking Forensic Investigator), 413
 children, crimes against, 80–81
 China
 APTs (advanced persistent threats), 344–345
 China General Nuclear Power Company (CGNPC), 188
 Chinese Eagle Union, 344
Choose Your Own Device (CYOD), 285
 chosen plain text, 236
 Chrome security settings, 87
 CIA triangle, 20

CIDR (classless interdomain routing), 44

cipher block chaining (CBC) mode, 223

Cipher Block Chaining Message

Authentication Code Protocol (CCMP), 38, 271

ciphers

Atbash, 211

Blowfish, 222

Caesar, 209–210

cipher text-only attacks, 236

Enigma, 213–214

Feistel, 216–217

multi-alphabet substitution, 211–212

rail fence, 212–213

Rijndael, 220

Serpent, 222

Skipjack, 222

Twofish, 220

Vigenère, 212

CISA (Certified Information Systems Auditor), 6

CISSP (Certified Information Systems Security Professional), 6, 331

Citrix, 312

CIW Security Analyst, 331

classification, data, 294–295

classless interdomain routing (CIDR), 44

clearance levels (DoD), 294–295

client errors, 46

cloud forensics, 416–417

commands

arp, 54–55

fc, 403

ipconfig, 49–51

net sessions, 402

netstat, 53, 404

nslookup, 53

openfiles, 403

ping, 51–52

DoS (denial of service) attacks, 97–99, 107–108

ping of death (PoD), 107–108

ping scans, 156

route, 54–55

snort, 260

tracert, 52

commutative groups, 221

CommView, 415

Comodo, 266

company-owned and provided equipment (COPE), 285

CompTIA, 6, 331

Computer Crimes Acts, 23

Computer Emergency Response Team (CERT), 23, 128

Computer Fraud and Abuse Act (1986), 128

Computer Hacking Forensic Investigator (CHFI), 413

Computer Security Act, 22

confidential information, 294

configuration, desktop, 285

./config/VirtualBox file, 416

connect scans, 156

content length, POST messages, 108

continuity, business

BCPs (business continuity plans), 295–296

standards, 296

cookies, 83

cookie poisoning, 165–166

RST, 104

SYN, 103–104

COPE (company-owned and provided equipment), 285

co-prime numbers, 224

copying drives, 387–391

Council of Europe Convention on Cybercrime, 394–395

Council of Europe's Electronic Evidence Guide, 394–395

- Counterexploitation website, 135**
 - cracking, 9, 152–153**
 - credibility, online threats, 78**
 - Creeper, 128**
 - CRLs (certificate revocation lists), 266**
 - cross-site request forgery, 165**
 - cross-site scripting, 12–13, 73, 165**
 - Cruz, Cassandra, 75**
 - cryptanalysis**
 - birthday attacks
 - differential cryptanalysis, 236
 - linear cryptanalysis, 236
 - brute force, 235
 - chosen plain text, 236
 - cipher text only, 236
 - frequency analysis, 235
 - goals of, 235
 - known plain text, 236
 - related-key attacks, 236
 - CryptoLocker, 124–125**
 - cryptologic bomb, 213**
 - CryptoWall, 124–125**
 - custody, chain of, 392**
 - cyber espionage. See espionage**
 - cyber investigation. See investigation techniques**
 - cyber stalking**
 - assessment of, 78–79
 - crimes against children, 80–81
 - defined, 74
 - protecting against, 88
 - real-world examples, 75–78
 - swatting, 78
 - cyber terrorism and cyber warfare**
 - APTs (advanced persistent threats), 139–140, 344–345
 - defense against, 362
 - disinformation, 355
 - economic attacks, 347–349
 - future trends, 359–361
 - general attacks, 350–351
 - hacktivists, 356
 - information control, 353–355
 - information warfare, 352
 - malware
 - BlackEnergy, 347
 - FinFisher, 347
 - Flame, 346
 - NSA ANT catalog, 347
 - StopGeorgia.ru, 346
 - Stuxnet, 345–346
 - military operations attacks, 350
 - propaganda, 352–353
 - real-world examples, 343–344, 355–359
 - Chinese Eagle Union, 344
 - India/Pakistan, 345
 - Russian hackers, 345
 - SCADA (Supervisory Control and Data Acquisitions), 351–352
 - scope of problem, 342–343
 - terrorist recruiting and communication, 362–363
 - TOR and dark web, 363–364
 - cybercrime. See Internet fraud; threats**
 - cybersecurity engineering. See systems engineering**
 - Cybersecurity Research and Education Act (2002), 359**
 - Cyberterrorism Preparedness Act (2002), 359**
 - cyclic groups, 221**
 - CYOD (Choose Your Own Device), 285**
-
- D**
- Daemen, John, 220**
 - DAM (database activity monitoring), 261**
 - DAMP (database activity monitoring and prevention), 261**
 - Dark Web, 173–175, 363–364**

DARPA (Defense Advanced Research Projects Agency), 363

Das, Mittesh, 139

data classification, 294–295

Data Encryption Standard (DES), 216–219

data integrity, 394

data interface diagrams, 438–439

data sources, IDS, 256

data transmission

overview of, 38–39

ports, 40

TCP/IP protocols, 39–40

database activity monitoring and prevention (DAMP), 261

database activity monitoring (DAM), 261

Daubert standard, 414

DCC (Defence Cyber Command), 360

DDoS (distributed denial of service) attacks, 10, 99, 109

decryption, 207

cryptanalysis

brute force, 235

chosen plain text, 236

cipher text only, 236

differential cryptanalysis, 236

frequency analysis, 235

goals of, 235

known plain text, 236

linear cryptanalysis, 236

related-key attacks, 236

steganography, 234

dedicated parity, striped disks with, 297

Defence Cyber Command (DCC), 360

Defense Advanced Research Projects Agency (DARPA), 363

deleted files, recovering, 399–402

demilitarized zone (DMZ), 320

denial of service. See DoS (denial of service) attacks

departing employees, security policies for, 287–288

Department of Defense clearance levels, 294–295

DES (Data Encryption Standard), 216–219

desktop configuration, security policies for, 285

detective investigation. See investigation techniques

developmental policies, 293

DHCP (Dynamic Host Control Protocol) starvation, 108

diagrams

data interface, 438–439

misuse case, 432–436

security block, 439

security sequence, 436–438

use-case, 428

DIDs (data interface diagrams), 438–439

differential backups, 296–297

differential cryptanalysis, 236

Diffie, Whitfield, 227

Diffie-Hellman, 227

DigiCert, 266

digital certificates, 265–266

Digital Signature Algorithm (DSA), 228

digital signatures, 230

directory traversal, 165

disabled services, 309–310

disaster, defined, 295

disaster recovery

BCPs (business continuity plans), 295–296

business continuity standards, 296

DRPs (disaster recovery plans), 295, 312

impact analysis, 296

disinformation, 355

DiskDigger, 399–402

distributed denial of service (DDoS) attacks, 10, 99, 109

distributed parity, striped disks with, 298

DMZ (demilitarized zone), 320

DNS (Domain Name System), 39

DNS (Domain Name System) poisoning, 8, 14–15

Dobbertin, Hans, 231

documentation, forensics, 391–393

Domain Name System (DNS), 39

DoS (denial of service) attacks

DDoS (distributed denial of service), 10, 99, 109

defending against, 111–112

defined, 7, 10

DHCP starvation, 108

Fraggle attacks, 106

HTTP POST DoS attacks, 108

ICMP (Internet Control Message Protocol) flood attacks, 107

illustration of, 97–99

land attacks, 109

login DoS attacks, 108

PDoS (permanent denial of service), 108

PoD (ping of death), 107–108

real-world examples, 109–111

registration DoS attacks, 108

scope of problem, 97

security policies for, 291

Smurf IP attacks, 105–106

TCP (Transmission Control Protocol) SYN flood attacks

micro blocks, 103

overview of, 102–103

RST cookies, 104

SPI firewalls, 105

stack tweaking, 104

SYN cookies, 103–104

teardrop attacks, 108

tools for

HOIC (High Orbit Ion Cannon), 100

LOIC (Low Orbit Ion Cannon), 99–100

Stacheldraht, 101

TFN (Tribal Flood Network), 101

TFN2K, 101

Trinoo DDoS tool, 101

XOIC, 100

UDP (User Datagram Protocol) flood attacks, 107

DoSHTTP, 346

download scanning, 246

doxing, 15

drive imaging, 387–391

DRPs (disaster recovery plans), 295, 312

DS0 connection lines, 36

DSA (Digital Signature Algorithm), 228

dual parity, striped disks with, 298

dual-homed hosts, 251

dumpster diving, 370

Duronio, Roger, 139

Dynamic Host Control Protocol (DHCP) starvation, 108

E

EAP (Extensible Authentication Protocol), 262, 269

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), 262

eBay, 12

ECB (electronic codebook) mode, 223

ECC (Elliptic Curve Cryptography), 228

EC-Council Certified Ethical Hacker, 152, 331

economic attacks, 347–349

economic espionage, 188–189

Economic Espionage Act (1996), 183

EDGE (Enhanced Data Rates for GSM Evolution), 409

Edge browser, 84

Edwards, John, 359

EffeTech HTTP Sniffer, 415

EFS (Encrypted File System), 195–196

electronic codebook (ECB) mode, 223

Electronic Evidence Guide, 394–395

Elgamal, Taher, 227

eLiTeWrap, 131–132

Elliptic Curve, 228

Ellison, Larry, 189

email

attachments, security policies for, 283–284

phishing, 73–74, 139, 198

scanning, 246

spam, 139

employees, security policies for

departing employees, 287–288

new employees, 287

nondisclosure and noncompete agreements, 184

Encapsulating Security Payload (ESP), 270

EnCase, 396

Encrypted File System, 195–196

encryption, 194

binary operations, 214

decryption, 207

cryptanalysis, 235

steganography, 234

defined, 206–207

digital certificates, 265–266

digital signatures, 230

Encrypted File System, 195–196

fraudulent encryption claims, identifying,
229–230

history of

Atbash cipher, 211

Caesar cipher, 209–210

Enigma, 213–214

multi-alphabet substitution, 211–212

online resources, 207–209

rail fence, 212–213

Vigenère, 212

legitimate versus fraudulent encryption meth-
ods, 229–230

PGP (Pretty Good Privacy), 228–229

public key

defined, 223–224

Diffie-Hellman, 227

ElGamal, 227

Elliptic Curve, 228

MQV (Menezes-Qu-Vanstone), 227

PGP (Pretty Good Privacy), 228–229

RSA method, 224–227

quantum cryptography, 237

single-key (symmetric), 207

3DES (Triple DES), 219

AES (Advanced Encryption Standard),
220–222

Blowfish, 222

defined, 216

DES (Data Encryption Standard), 216–219

modification of, 223

Serpent, 222

Skipjack, 222

Twofish, 220

Energy Technology International, 188

engineering. See systems engineering

**Enhanced Data Rates for GSM Evolution
(EDGE), 409**

Enigma, 213–214

enumeration, 159–160

errors, client/server, 46

ESP (Encapsulating Security Payload), 270

espionage. See industrial espionage

ethical hacking, 18

**ETSI (European Telecommunications
Standards Institute), 409**

Euler's totient, 225

events, IDS, 256

evidence

Android, 410–411

browser, 397–398

- cell phone, 408
 - cellular networks, 409
 - ICCID (Integrated Circuit Card Identification), 408
 - IMSI (International Mobile Subscriber Identity), 408
 - SIM (Subscriber Identity Module), 408
- chain of custody, 392
- deleted files, recovering, 399–402
- iOS, 410
- operating system utilities, 402–404
 - fc, 403
 - net sessions, 402
 - netstat, 404
 - openfiles, 403
- system log
 - Linux logs, 399
 - Windows logs, 398
- Windows, 398, 404–407, 411

evil twin attack, 166

expert witnesses, 414

expulsion, 286

Extensible Authentication Protocol (EAP), 262, 269

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), 262

F

Facebook, 374–375

faillog file, 399

FakeAV, 125

false positives/negatives, 247

Fannie Mae, 139

FastMail, 111

fault tolerance, 296–298

FBAR (thin-film bulk acoustic resonator) technology, 188

FBI (Federal Bureau of Investigation) forensics guidelines, 392–393

fc command, 403

FDISK utility, 170

federal prison records, 378

Feistel cipher, 216–217

fields, AES (Advanced Encryption Standard), 222

file recovery, 399–402

file scanning, 246

File Transfer Protocol (FTP), 39

filtering, packet, 249

FinFisher, 347

Firefox security settings, 85–87

firewalls

- benefits and limitations of, 248–249

- configurations, 250–251

- defined, 19, 55–56, 248

- firewall logs, 253

- selection of, 311–312

- SPI, 105

- types of, 249–250

- Windows 10 Windows Defender, 252–253

- ZoneAlarm, 252

Flame, 128, 345–346

flooding

- TCP (Transmission Control Protocol) SYN flood attacks

- micro blocks, 103

- overview of, 102–103

- RST cookies, 104

- SPI firewalls, 105

- stack tweaking, 104

- SYN cookies, 103–104

- UDP (User Datagram Protocol) flood attacks, 107

footprinting, 348

foreign economic espionage, 188–189

Forensic Toolkit, 388–391, 396

forensics. *See also* evidence

- certifications, 332, 413–414

- expert witnesses, 414

- goal of, 386–387
 - Locard's principle of transference, 395
 - mobile devices
 - Android, 410–411
 - cell phone components, 408
 - cellular networks, 409
 - general principles, 412
 - iOS, 410
 - Windows, 411
 - network, 415
 - principles for
 - chain of custody, 392
 - Council of Europe's Electronic Evidence Guide, 394–395
 - documentation, 391–392
 - drive imaging, 387–391
 - FBI (Federal Bureau of Investigation) forensics guidelines, 392–393
 - SWGDE (Scientific Working Group on Digital Evidence) guidelines, 395
 - U.S. Secret Service guidelines, 393–394
 - tools
 - AccessData Forensic Toolkit, 388–391, 396
 - cell phone components, 408
 - Cellebrite, 397
 - EnCase, 396
 - FTK Imager, 388–391
 - OSForensics, 390–391, 396
 - Oxygen, 396
 - Sleuth Kit, 396
 - virtual
 - cloud, 416–417
 - VMs (virtual machines), 415–416
 - Forwarded Events log, 398**
 - Fraggle attacks, 106**
 - framework-specific modeling languages (FSMLs), 431**
 - fraud. See Internet fraud**
 - frequency, online threats, 79**
 - frequency analysis, 235**
 - F-Secure, 24**
 - FSMLs (framework-specific modeling languages), 431**
 - FTK Imager, 388–391**
 - FTP (File Transfer Protocol), 39**
 - full backups, 296–297**
 - functions, hash, 230–231**
 - HMAC, 231–232
 - MAC, 231–232
 - MD5, 231
 - rainbow tables, 232–233
 - RIPEMD (RACE Integrity Primitives Evaluation Message Digest), 231
 - SHA (Secure Hash Algorithm), 231
- ## G
-
- Gameover ZeuS, 124**
 - gateways, 250**
 - GCFA (GIAC Certified Forensic Analyst), 332, 414**
 - GCFE (GIAC Certified Forensic Examiner), 332, 414**
 - general cyber attacks, 350–351**
 - general searches, 371–374**
 - GhostNet, 356**
 - GIAC certifications, 332, 414**
 - Gigabit Ethernet, 34**
 - GitHub, DoS (denial of service) attacks against, 99, 109**
 - Global System for Mobile Communications (GSM), 409**
 - The Gobbler, 108**
 - GoDaddy, 266**
 - Gonzalez, Amy, 77**
 - Google Chrome security settings, 87**
 - GPEN certification, 332**
 - gray hat hackers, 17, 153**
 - grooming, 80**
 - groups, AES (Advanced Encryption Standard), 221**

GSEC certification, 332

GSM (Global System for Mobile Communications), 409

Guidance Software, EnCase, 396

guidelines, defined, 294

H

hacking. See also malware

active scanning

enumeration, 159–160

MBSA (Microsoft Baseline Security Analyzer), 321–323

Nessus, 324–326

OWASP (Open Web Application Security Project), 326–327

port scanning, 155–158

Shodan, 160–162, 328–329

vulnerability assessment, 158–159

black hat hackers, 17, 152–153

cell phone attacks, 166

cookie poisoning, 165–166

cross-site request forgery, 165

cross-site scripting, 12–13, 73, 165

Dark Web, 173–175

defined, 9

directory traversal, 165

gray hat hackers, 17, 153

hacker intrusions, 291–292

hacktivists, 356

of medical devices, 15

new vulnerabilities, 15–16

passive scanning, 153–155

password cracking, 166–168

penetration testing

defined, 171

NIST 800–115, 171

NSA information assessment methodology, 171–172

overview of, 18, 152

PCI DSS (Payment Card Industry Data Security Standard), 172–173

red/blue teams, 153

phreaking, 18, 153

reconnaissance phase, 153

Russian hackers, 345

script kiddies, 17–18, 153

security policies SANS Institute, 291–292

SQL injection, 11–12, 162–164

URL hijacking, 166

white hat hackers, 17, 152–153

Windows hacking techniques

login as system, 170

net user script, 169–170

pass the hash, 169–170

wireless attacks, 166

hacktivists, 356

harassment. See cyber stalking

hash functions

HMAC, 231–232

MAC, 231–232

MD5, 231

overview of, 104, 230–231

rainbow tables, 232–233

RIPEMD, 231

SHA, 231

hashing message authentication code (HMAC), 231–232

Health Insurance Portability and Accountability Act (HIPAA), 23, 298

Hellman, Martin, 227, 232

heuristic scanning, 245–246

heuristics, 245–246

High Orbit Ion Cannon (HOIC), 100

high-speed connections, 36

hijacking

session, 7, 13

URL, 166

HIPAA (Health Insurance Portability and Accountability Act), 23, 298

HMAC (hashing message authentication code), 231–232

HMI (human-machine interface), 351

Ho, Allen, 188

hoax viruses, 127–128

HOIC (High Orbit Ion Cannon), 100

Home PC Firewall Guide, 311

honey pots, 260–261

hosts, 251

Houston Astros, 187

HTML (Hypertext Markup Language), 49

HTTP (Hypertext Transfer Protocol), 39

development of, 49

HTTPS, 40

POST DoS attacks, 108

hubs, 35

human-machine interface (HMI), 351

Hutchins, Marcus, 124

hybrid security approach, 21

Hypertext Markup Language (HTML), 49

Hypertext Transfer Protocol. See HTTP (Hypertext Transfer Protocol)

I

IBM DES (Data Encryption Standard), 216–219

ICCID (Integrated Circuit Card Identification), 408

ICMP (Internet Control Message Protocol)

ICMP flood attacks, 107

ICMP packets, blocking, 112

Smurf IP attacks, 105–106

iDEN (Integrated Digitally Enhanced Network), 405–409

identity theft

cross-site scripting, 73

phishing, 73–74

protecting against, 83–87

scope of problem, 72–73

Identity Theft and Assumption Deterrence Act (1998), 81

IDSs (intrusion detection systems), 19, 155, 261

active, 255

attack identification methods, 255

defined, 254

elements of, 256

passive, 255

Snort, 256–260

IEEE (Institute of Electrical and Electronics Engineers), 36–37

IETF (Internet Engineering Task Force), 48–49

IIN (Issuer Identification Number), 408

IKE (Internet Key Exchange), 270

IM (instant messaging), security policies for, 284

image searches, 374

imaging drives, 387–391

IMAP (Internet Message Access Protocol), 39

IMAPS (Internet Message Access Protocol Secure), 40

***The Imitation Game*, 214**

impact analysis, 296

IMSI (International Mobile Subscriber Identity), 408

incremental backups, 296–297

India, cyber terrorism in, 345

industrial espionage

asset identification, 184–187

defined, 183–184

employee nondisclosure and noncompete agreements, 184

Industrial Espionage Act (1996), 197

low-tech, 189–192

phishing, 198

protecting against, 194–197

real-world examples, 187–189

scope of problem, 182–183, 189

spyware used in, 193–194

trends in, 189

- Industrial Espionage Act (1996), 197**
- Infobel searches, 373–374**
- information control, 353–355**
- Information Systems Security Architecture Professional (ISSAP), 331**
- Information Systems Security Engineering Professional (ISSEP), 331**
- Information Systems Security Management Professional (ISSMP), 331**
- information warfare, 352**
- initialization vector (IV), 37, 271**
- InPrivate Browsing option (Microsoft Edge), 84–85**
- input validation, 164**
- insider threats, 8, 13–14**
- installation, security policies for, 284**
- instant messaging (IM), security policies, 284**
- Institute of Electrical and Electronics Engineers (IEEE), 36–37**
- Integrated Circuit Card Identification (ICCID), 408**
- Integrated Digitally Enhanced Network (iDEN), 405–409**
- intensity, online threats, 79**
- International Council on Systems Engineering (INCOSE), 424**
- International Mobile Subscriber Identity (IMSI), 408**
- Internet. *See also* Internet fraud**
 - basic communications, 47
 - connections, 36
 - Dark Web, 173–175, 363–364
 - history of, 47–49
 - Internet transactions, growth of, 2–4
 - IoT (Internet of Things), 2–3, 16
 - IP addresses
 - IPv4, 41–45
 - IPv6, 44–45
 - ISPs (Internet service providers), 40–41
 - packets
 - defined, 46–47
 - filtering, 249
 - structure of, 40–41
 - URLs (uniform resource locators), 46
 - use policies, 282–283
- Internet Black Tigers, 356**
- Internet Control Message Protocol (ICMP)**
 - ICMP flood attacks, 107
 - ICMP packets, blocking, 112
 - Smurf IP attacks, 105–106
- Internet Engineering Task Force (IETF), 48–49**
- Internet fraud**
 - auction fraud
 - protecting against, 87–88
 - types of, 70–72
 - cyber stalking
 - assessment of, 78–79
 - crimes against children, 80–81
 - defined, 74
 - protecting against, 88
 - real-world examples, 75–78
 - swatting, 78
 - fraudulent encryption, 229–230
 - how it works, 67
 - identity theft
 - phishing, 73–74
 - protecting against, 83–87
 - scope of problem, 72–73
 - investment fraud
 - common schemes, 67–68
 - protecting against, 82
 - pump and dump scams, 68–69
 - laws about, 81–82
 - protecting against, 82–88
 - scope of problem, 66–67
- Internet Key Exchange (IKE), 270**
- Internet Message Access Protocol (IMAP), 39**
- Internet Message Access Protocol Secure (IMAPS), 40**

Internet of Things (IoT), 2–3

Internet Protocol. See IP (Internet Protocol)

Internet Protocol Security (IPsec), 270

Internet Relay Chat (IRC), 39

Internet Security Association and Key Management Protocol (ISAKMP), 270

intrusion detection systems. See IDSs (intrusion detection systems)

intrusion deterrence, 261

intrusion prevention systems (IPSs), 112

investigation techniques, 370–371

- Facebook, 374–375
- general searches, 371–374
- mistaken identity, 377
- online resources, 378
- sex offender registries, 375–377
- Usenet, 379

investment fraud

- common schemes, 67–68
- protecting against, 82
- pump and dump scams, 68–69

Invisible Secrets, 193, 234

iOS forensics, 410

IoT (Internet of Things), 2–3, 16

IP (Internet Protocol)

- IPsec (Internet Protocol Security), 270
- IPv4 addresses
 - CIDR (classless interdomain routing), 44
 - loopback addresses, 42
 - network classes, 41–43
 - public versus private, 43
 - subnetting, 43–44
- IPv6 addresses, 44–45
- Smurf IP attacks, 105–106

ipchains, 312

ipconfig command, 49–51

IPsec (Internet Protocol Security), 270

IPSs (intrusion prevention systems), 112

iptables, 312

IRC (Internet Relay Chat), 39

Irish Republican Army (IRA), 352

ISAKMP (Internet Security Association and Key Management Protocol), 270

ISDN connection lines, 36

ISO 17799 standard, 279–280

ISPs (Internet service providers), 40–41

ISSAP (Information Systems Security Architecture Professional), 331

ISSEP (Information Systems Security Engineering Professional), 331

ISSMP (Information Systems Security Management Professional), 331

Issuer Identification Number (IIN), 408

IV (initialization vector), 37, 271

J-K

Jacob, Richard, 188

Jeep, attacks targeting, 16

Kaspersky, 129, 248, 357

KDCs (key distribution centers), 264

Kedi RAT (Remote Access Trojan), 125

Kerberos, 263–265

Kerckhoffs, Auguste, 229

Kerckhoffs's principle, 229

kern.log file, 399

key distribution centers (KDCs), 264

key loggers, 9, 135–136

key schedules, 217–218

key space, 210

KillDisk, 347

known plain text, 236

Koblitz, Neal, 228

Kosovo conflict, 356

Kurzynski, Joel, 75, 77

L

L2TP (Layer 2 Tunneling Protocol), 269

land attacks, 109

last visited sites, viewing, 407

Latigo, Heriberto, 75

Layer 2 Tunneling Protocol (L2TP), 269

layered security approach, 21

LEAP (Lightweight Extensible Authentication Protocol), 262

least privileges, 21, 170, 194

least significant bit (lsb), 233

legislation, 22–23

Computer Fraud and Abuse Act (1986), 128

Computer Security Act, 22

Cybersecurity Research and Education Act (2002), 359

Cyberterrorism Preparedness Act (2002), 359

Economic Espionage Act (1996), 183

HIPAA (Health Insurance Portability and Accountability Act), 298

Identity Theft and Assumption Deterrence Act (1998), 81

Industrial Espionage Act (1996), 197

Internet fraud laws, 81–82

PATRIOT Act, 359–360

SOX (Sarbanes-Oxley), 299

Levandowsky, Anthony, 188

life cycle, system development, 427

Lightweight Extensible Authentication Protocol (LEAP), 262

Lin, Ryan, 75

linear cryptanalysis, 236

Linksys, 311

Linux

firewalls, 312

system logs, 399

local network connections

cables, 33–35

hubs, 35

repeaters, 35

routers, 35–36

switches, 35

Locard, Edmond, 395

Locard's principle of transference, 395

log files, 416

Linux logs, 399

Windows logs, 398

logic bombs, 9, 139

login as system attacks, 170

login DoS (denial of service) attacks, 108

logs, 398

firewall, 253

Linux logs, 399

Windows logs, 398

LOIC (Low Orbit Ion Cannon), 10, 99–100

Long Term Evolution (LTE), 409

loopback addresses, 42

Low Orbit Ion Cannon (LOIC), 10, 99–100

low-tech industrial espionage, 189–192

lpr.log file, 399

LSASS.EXE, 133–134

lsb (least significant bit), 233

LTE (Long Term Evolution), 409

Luhnnow, Jeff, 187

M

MAC (Media Access Control) addresses, 35, 57

MAC (message authentication code), 231–232

MacDefender, 125

machine learning, 247

macro viruses, 122

mail.* file, 399

Makwana, Rajendrainh, 139

malicious web-based code, 138

malware

Agent.btz, 344

antivirus software, 140–143

APTs (advanced persistent threats), 139–140

BlackEnergy, 347

buffer-overflow attacks

explained, 132–133

Sasser, 133–134

creating, 168–169

- defined, 7
 - dynamic nature of, 121
 - FinFisher, 347
 - Flame, 346
 - key loggers, 9
 - logic bombs, 9, 139
 - malicious web-based code, 138
 - NSA ANT catalog, 347
 - remediation steps, 144
 - rootkits, 137–138
 - spam, 139
 - spyware
 - antispymware software, 194, 253–254
 - defined, 9
 - delivery of, 135
 - explained, 134–135
 - legal uses of, 135
 - obtaining, 135–137
 - StopGeorgia.ru, 346
 - Stuxnet, 345–346
 - Trojan horses, 8, 129–132
 - viruses, 110. *See also* virus scanners
 - antivirus software, 140–143
 - avoiding, 129
 - defined, 8, 121
 - impact of, 129
 - MyDoom, 110–111
 - real-world examples, 123–128
 - security policies for, 290–291
 - spread of, 121–122
 - types of, 122–123
 - worms, 110
- Malwarebytes, 142–143, 248**
- MATLAB, 428**
- Matusiewicz, David, 77**
- Matusiewicz, Lenore, 77**
- maximum tolerable downtime (MTD), 296**
- MBSA (Microsoft Baseline Security Analyzer), 321–323**
- McAfee, 129, 141, 248, 308, 312**
- MCC (mobile country code), 408**
- McCullum, Juan R.77**
- McCumber cube, 19–20**
- MCDs (misuse case diagrams), 432–436**
- MD5, 231**
- mean percentage error (MPE), 429**
- mean squared deviation (MSD), 429**
- mean time between failures (MTBF), 429–430**
- mean time to repair (MTTR), 296, 430**
- Media Access Control (MAC) addresses, 35, 57**
- medical devices, hacking of, 15**
- Medico, Joseph, 76**
- memcache attacks, 109**
- memory-resident viruses, 122**
- Menezes-Qu-Vanstone (MQV), 227**
- message authentication code (MAC), 231–232**
- messages, Kerberos, 264–265**
- metamorphic viruses, 123**
- metrics, 428–430**
- micro blocks, 103**
- Microsoft Baseline Security Analyzer (MBSA), 321–323**
- Microsoft Edge security settings, 84**
- Microsoft Outlook, virus spread in, 121–122**
- Microsoft Point-to-Point Encryption (MPPE), 269**
- Microsoft Security Advisor, 24**
- military operations attacks, 350**
- Miller, Victor, 228**
- Mimail, 127**
- MIMO (multiple-input multiple-output), 37**
- minors, cyber stalking incidents involving, 80–81**
- Mirai, 111**
- mirroring disks, 297**
- mistaken identity, 377**
- misuse case diagrams, 432–436**
- mitigation of risk, 7**

MixColumns step (AES), 221

mobile country code (MCC), 408

mobile devices, forensics for

- Android, 410–411
- cell phone components, 408
- cellular networks, 409
- general principles, 412
- ICCID (Integrated Circuit Card Identification), 408
- IMSI (International Mobile Subscriber Identity), 408
- iOS, 410
- SIM (Subscriber Identity Module), 408
- Windows, 411

mobile subscription identifier number (MSIN), 408

modeling and simulation, 431

- need for, 428
- SecML (Security Modeling Language)
 - data interface diagrams, 438–439
 - misuse case diagrams, 432–436
 - overview of, 428, 430–432
 - security block diagrams, 439
 - security sequence diagrams, 436–438
- UML (Unified Modeling Language), 428, 439

Modern Cryptography (Easttom), 230

modulus, 225

mono-alphabet substitution, 210

Morris, Robert Tappan, Jr.13, 128

Morris attack, 13

MP3Stego, 234

MPE (mean percentage error), 429

MPPE (Microsoft Point-to-Point Encryption), 269

MQV (Menezes-Qu-Vanstone), 227

MSD (mean squared deviation), 429

MSIN (mobile subscription identifier number), 408

MTBF (mean time between failures), 429–430

MTD (maximum tolerable downtime), 296

MTTR (mean time to repair), 296, 430

multi-alphabet substitution, 211–212

multi-partite viruses, 122

multiple-input multiple-output (MIMO), 37

Murphy, Robert James, 76

MyDoom, 110–111, 350–351

mysql.* file, 399

N

NACLC (National Agency Check with Law and Credit), 294

NAPs (network access points), 40–41

NAT (network address translation), 43

National Agency Check with Law and Credit (NACLC), 294

National Center for State Courts, 378

National Counterintelligence and Security Center (NCSC), 188

National Institute of Standards and Technology (NIST), 171, 237

National Security Agency (NSA), 171–172, 315, 347

NCSC (National Counterintelligence and Security Center), 188

negatives, false, 247

Nessus, 324–326

net sessions command, 402

net user script, 169–170

NetBIOS, 39

netstat command, 53, 404

network address translation (NAT), 43

network host-based firewalls, 250

network interface cards (NICs), 33

Network News Transfer Protocol (NNTP), 39

networks, 40–41. See also firewalls

- certifications, 330–332
- concept of, 33
- data transmission

- overview of, 38–39
- ports, 40
- TCP/IP protocols, 39–40
- forensics, 415
- high-speed connections, 36
- Internet
 - basic communications, 47
 - Dark Web, 173–175
 - dark web, 363–364
 - history of, 47–49
 - IPv4 addresses, 41–45
 - IPv6 addresses, 44–45
 - packets, 46–47
 - structure of, 40–41
 - URLs (uniform resource locators), 46
- MAC (Media Access Control) addresses, 35, 57
- NICs (network interface cards), 33
- OSI (Open Systems Interconnection) model, 56–57
- physical connections, 33–36
 - cables, 33–35
 - hubs, 35
 - repeaters, 35
 - routers, 35–36
 - switches, 35
- professional consultants, 330–332
- scanning
 - MBSA (Microsoft Baseline Security Analyzer), 321–323
 - Nessus, 324–326
 - OWASP (Open Web Application Security Project), 326–327
 - Shodan, 328–329
- securing, 319–321
- security approaches
 - hybrid, 21
 - industrial espionage protection, 194–197
 - layered, 21
 - perimeter, 21
- utilities
 - arp, 54–55
 - FDISK, 170
 - ipconfig, 49–51
 - netstat, 53
 - nslookup, 53
 - ping, 51–52
 - route, 54–55
 - tracert, 52
- VPNs (virtual private networks), 268–270
- wireless
 - 802.11 standard, 36–38
 - ANT+38
 - Bluetooth, 38
 - security, 37–38
 - Wi-Fi security, 270–271
 - ZigBee, 38
 - Z-Wave, 38
- new employees, security policies for, 287**
- New York Stock Exchange, DoS attacks on, 358**
- NGFWs (next-generation firewalls), 105**
- ngrep, 415**
- NICs (network interface cards), 33**
- Nigerian fraud, 67–68**
- NIST (National Institute of Standards and Technology), 171, 237**
- Nmap, 156–158**
- NNTP (Network News Transfer Protocol), 39**
- nonces, 223**
- noncompete agreements, 184**
- nondisclosure agreements, 184**
- nonrepudiation, 230**
- nonvirus viruses, 127–128**
- Norton, 129**
 - Personal Firewall, 312
 - Security, 140–141, 248
- notifications, IDS, 256**
- NSA (National Security Agency), 171–172, 315, 347**
- nslookup command, 53**

nuclear secrets, industrial espionage incidents, 188

numbers, binary, 41

O

Object Management Group (OMG),
430–431

OC3 connection lines, 36

OC12 connection lines, 36

OC48 connection lines, 36

octets, 41

Offender Locator, 377

Offensive Security, 152, 331

OMB Circular A-130, 23

OMG (Object Management Group),
430–431

on-demand virus scanners, 246

ongoing virus scanners, 246

The Onion Router (TOR) project, 363–364

onion routing, 173, 363

online harassment. *See* cyber stalking

Open Systems Interconnection (OSI) model,
56–57

Open Web Application Security Project
(OWASP), 326–327

openfiles command, 403

Operation Ababil, 358

operators, IDS, 256

OphCrack, 167–168

Oracle Box, 144

Oracle Corporation, 189

OR operation, 215

OSForensics, 390–391, 396

OSI (Open Systems Interconnection) model,
56–57

Outlook, virus spread in, 121–122

OWASP (Open Web Application Security
Project), 326–327

Oxley, Michael, 299

Oxygen, 396

P

Pacer, 378

packets

defined, 46–47

filtering, 46–47, 249

Pakistan, cyber terrorism by, 345

PAP (Password Authentication Protocol), 262

pass the hash attacks, 169–170

passive IDSs (intrusion detection systems),
255

passive scanning, 153–155

PassMark Software OSForensics, 396

Password Authentication Protocol (PAP), 262

passwords

cracking, 166–168

policies, 313

security policies for, 281

patches, 307–308

Patel, Nimesh, 139

PATRIOT Act, 359–360

payloads, 233

PCI DSS (Payment Card Industry Data
Security Standard), 172–173, 299

PDoS (permanent denial of service), 108

PEAP (Protected Extensible Authentication
Protocol), 263

penetration testing, 18, 152, 153

defined, 171

NIST 800–115, 171

NSA information assessment methodology,
171–172

PCI DSS (Payment Card Industry Data Security
Standard), 172–173

red/blue teams, 153

Penetration Testing Fundamentals (Easttom),
173, 176

People's Drug Store, 175

perimeter security approach, 21

permanent denial of service (PDoS) attacks,
108

- personal health information (PHI), 2–3**
- personal identification number (PIN), 408**
- personal unblocking code (PUK), 408**
- personally identifiable information (PII), 2–3**
- Petya, 124**
- PGP (Pretty Good Privacy), 228–229, 266**
- PHI (personal health information), 2–3**
- phishing, 73–74, 198**
- phlashing, 108**
- phone taps and bugs, 194**
- phreaking, 18, 153**
- physical security, 314–315**
- PII (personally identifiable information), 2–3**
- PIN (personal identification number), 408**
- ping command, 51–52**
 - DoS (denial of service) attacks, 97–99, 107–108
 - ping of death (PoD), 107–108
 - ping scans, 156
- plain text attacks, 236**
- plans**
 - BCPs (business continuity plans), 295–296
 - DRPs (disaster recovery plans), 295, 312
- Plaskett, Stacey, 77**
- PLC (programmable logic controller), 345**
- PoD (ping of death), 107–108**
- pod slurping, 166**
- Point-to-Point Protocol (PPP), 269**
- Point-to-Point Tunneling Protocol (PPTP), 269**
- policies**
 - assessment of, 312–314
 - data classification, 294–295
 - disaster recovery
 - BCPs (business continuity plans), 295–296
 - business continuity standards, 296
 - DRPs (disaster recovery plans), 295
 - impact analysis, 296
 - fault tolerance, 296–298
 - guidelines, 294
 - ISO 17799 standard, 279–280
 - laws governing, 298–299
 - procedures, 294
 - purpose of, 279
 - standards, 294
 - system administration policies
 - access control, 292–293
 - change requests, 288–290
 - departing employees, 287–288
 - developmental policies, 293
 - need for, 287
 - new employees, 287
 - security breaches, 290–293
 - user policies
 - BYOD (Bring Your Own Device), 285
 - consequences for violating, 286–287
 - CYOD (Choose Your Own Device), 285
 - defining, 280
 - desktop configuration, 285
 - e-mail attachments, 283–284
 - instant messaging, 284
 - Internet use, 282–283
 - passwords, 281
 - software installation and removal, 284
 - termination or expulsion and, 286
- polymorphic viruses, 123**
- POP3 (Post Office Protocol version 3), 39**
- POP3S (Post Office Protocol version 3 Secure), 40**
- ports, 35, 40**
 - assessment of, 308–311
 - port scanning, 155–158
- positives, false, 247**
- POST DoS attacks, 108**
- Post Office Protocol version 3 (POP3), 39**
- Post Office Protocol version 3 Secure (POP3S), 40**
- pound sign (#), 260**
- PPP (Point-to-Point Protocol), 269**

PPTP (Point-to-Point Tunneling Protocol), 269

Preneel, Bart, 231

Pretty Good Privacy (PGP), 228–229, 266

prime numbers, 224

principals, Kerberos, 264

prison searches, 378

privacy

- browser settings, 84–88
- Privacy Act, 22
- private information, 294
- private IP addresses, 43

Privacy Act, 22

private keys, 223

probes, assessment of, 314

procedures, defined, 294

professional consultants, 330–332

programmable logic controller (PLC), 345

propaganda, 352–353

Protected Extensible Authentication Protocol (PEAP), 263

protective software and devices, assessment of, 311–312

proxies

- application proxies, 250
- proxy servers, 19, 56

public information, 294

public IP addresses, 43

public key encryption, 207

- defined, 223–224
- Diffie-Hellman, 227
- ElGamal, 227
- Elliptic Curve, 228
- MQV (Menezes-Qu-Vanstone), 227
- PGP (Pretty Good Privacy), 228–229
- RSA method, 224–227

public keys, 223

public records, 378

PUK (personal unblocking code), 408

pump and dump scams, 68–69

Q

quantum computing, 237

quantum cryptography, 237

qubits, 237

QuickStego, 193, 234

R

RACE Integrity Primitives Evaluation Message Digest (RIPEMD), 231

RAID (redundant array of independent disks), 297–298

rail fence, 212–213

rainbow tables, 232–233

Ramos, Jeron, 77

Ranum, Marcus, 355

RAs (registration authorities), 266

readability analysis, 428

Reaper, 128

recent documents, viewing, 407

reconnaissance, 153

recovery. *See* disaster recovery

red teams, 153

redundant array of independent disks (RAID), 297–298

registration authorities (RAs), 266

registration DoS (denial of service) attacks, 108

Rejewski, Marian, 213

related-key attacks, 236

remediation steps (malware), 144

remote terminal units (RTUs), 351

removing software

- security policies for, 284
- uninstalled software, finding, 407

repeaters, 35

requests, change, 288–290

requirements engineering, 424–426

Richardson, Edward, 77

Rijmen, Vincent, 220

Rijndael cipher, 220
rings, AES (Advanced Encryption Standard), 222
RIPEMD (RACE Integrity Primitives Evaluation Message Digest), 231
risk assessment, 4–7, 16
Rivest, Ron, 224, 231
RJ-11 jacks, 33
RJ-45 jacks, 33
Romanian cybercrime law, 82
Rombertik, 124
rootkits, 137–138
route command, 54–55
router-based firewalls, 251
routers, 35–36
Rozycki, Jerzy, 213
RSA method, 224–227
RTUs (remote terminal units), 351
Rule 702, 414
Russian hackers, 345

S

sandboxes, 247
Sandworm, 357
SANS Institute, 24, 112, 152, 293, 315, 414
Santa Cruz Operations (SCO), 110
Sarbanes, Paul, 299
Sarbanes-Oxley (SOX), 299
SAs (security associations), 270
Sasser, 133–134
SCADA (Supervisory Control and Data Acquisitions), 351–352
scanning
 active
 active code scanning, 247
 enumeration, 159–160
 MBSA (Microsoft Baseline Security Analyzer), 321–323
 Nessus, 324–326

OWASP (Open Web Application Security Project), 326–327
 port scanning, 155–158
 Shodan, 160–162, 328–329
 vulnerability assessment, 158–159
 passive, 153–155
Scherbius, Arthur, 213
Schneier, Bruce, 222
SCI (sensitive compartmented information), 294
Scientific Working Group on Digital Evidence (SWGDE), 395
SCO (Santa Cruz Operations), 110
screened hosts, 251
script kiddies, 17–18, 153
scripting, cross-site, 12–13
searches
 Facebook, 374–375
 general, 371–374
 mistaken identity, 377
 online resources, 378
 sex offender registries, 375–377
 Usenet, 379
SEC (Securities and Exchange Commission), 672
SecML (Security Modeling Language)
 data interface diagrams, 438–439
 misuse case diagrams, 432–436
 overview of, 428, 430–432
 security block diagrams, 439
 security sequence diagrams, 436–438
secret information, 294
Secret Service forensics guidelines, 393–394
Secure Hash Algorithm (SHA), 231
Secure Shell (SSH), 39
Secure Sockets Layer (SSL), 266–268
Securities and Exchange Commission (SEC), 672
security activities, 19
security associations (SAs), 270

security audits, 394**security block diagrams, 439****security breaches, 290. See also hacking; industrial espionage; threats**

- cracking, 9

- defined, 7

- insider threats, 13–14

- social engineering, 9, 191

- war-dialing, 10

- war-driving, 10

- war-flying, 10

security devices, 19**security information event management (SIEM), 436****Security log, 398****Security Modeling Language. See SecML (Security Modeling Language)****security policies**

- data classification, 294–295

- disaster recovery

- BCPs (business continuity plans), 295–296

- business continuity standards, 296

- DRPs (disaster recovery plans), 295

- impact analysis, 296

- fault tolerance, 296–298

- guidelines, 294

- ISO 17799 standard, 279–280

- laws governing, 298–299

- procedures, 294

- purpose of, 279

- standards, 294

- system administration policies

- access control, 292–293

- change requests, 288–290

- departing employees, 287–288

- developmental policies, 293

- need for, 287

- new employees, 287

- security breaches, 290–293

- user policies

- BYOD (Bring Your Own Device), 285

- consequences for violating, 286–287

- CYOD (Choose Your Own Device), 285

- defining, 280

- desktop configuration, 285

- e-mail attachments, 283–284

- instant messaging, 284

- Internet use, 282–283

- passwords, 281

- software installation and removal, 284

- termination or expulsion and, 286

security resources, 23–24**security sequence diagrams, 436–438****security technology**

- antispysware software, 194, 253–254

- antivirus software, 140–143, 248

- authentication, 262–265

- DAM (database activity monitoring), 261

- DAMP (database activity monitoring and prevention), 261

- digital certificates, 265–266

- firewalls

- benefits and limitations of, 248–249

- configurations, 250–251

- defined, 19, 55–56, 248

- firewall logs, 253

- selection of, 311–312

- SPI, 105

- types of, 249–250

- Windows 10 Windows Defender, 252–253

- ZoneAlarm, 252

- honey pots, 260–261

- IDSs (intrusion detection systems)

- active, 255

- attack identification methods, 255

- defined, 254

- elements of, 256

- passive, 255
- Snort, 256–260
- intrusion deflection, 261
- intrusion deterrence, 261
- SSL (Secure Sockets Layer), 266–268
- TLS (Transport Layer Security), 266–268
- virus scanners
 - defined, 245
 - how they work, 245–246, 247
 - scanning techniques, 246–247
- VPNs (virtual private networks), 268–270
- Wi-Fi security, 270–271
- Security+ certification, 331**
- sensitive compartmented information (SCI), 294**
- sensors, IDS, 256**
- Serpent, 222**
- Server Message Block (SMB), 40**
- servers**
 - ASs (authentication servers), 264
 - errors, 46
 - proxy, 19, 56
 - securing, 317–319
 - TGSs (ticket-granting servers), 264
- services, shutting down, 309–310**
- Services log, 398**
- session hijacking, 7, 13**
- sex offender registries, 81, 375–377**
- sexual predators, 80–81**
- SHA (Secure Hash Algorithm), 231**
- Shamir, Adi, 224**
- Shamoon, 124, 356**
- Shannon, Claude, 229**
- Shannon's maxim, 229**
- “sheep dip” machines, 247**
- shielded twisted-pair (STP) cable, 34**
- ShiftRows step (AES), 221**
- shill bidding, 71**
- Shiva Password Authentication Protocol (SPAP), 262**
- Shodan, 160–162, 328–329**
- SIEM (security information event management), 436**
- Siemens Step7 software, 345**
- signals, 35**
- signatures, digital, 230**
- Silk Road, 364**
- SillyFDC worm, 344**
- SIM (Subscriber Identity Module), 408**
- Simple Mail Transfer Protocol Secure (SMTPS), 40**
- Simple Mail Transfer Protocol (SMTP), 39**
- Simple Network Management Protocol (SNMP), 156**
- Single Loss Expectancy (SLE), 6**
- Single Scope Background Investigation (SSBI), 295**
- single-key (symmetric) encryption, 207**
 - 3DES (Triple DES), 219
 - AES (Advanced Encryption Standard), 220–222
 - Blowfish, 222
 - defined, 216
 - DES (Data Encryption Standard), 216–219
 - modification of, 223
 - Skipjack, 222
 - Twofish, 220
- sinkholes, 112**
- Sinn Féin, 352**
- Skipjack, 222**
- SLE (Single Loss Expectancy), 6**
- Sleuth Kit, 396**
- SMB (Server Message Block), 40**
- SMTP (Simple Mail Transfer Protocol), 39**
- SMTPS (Simple Mail Transfer Protocol Secure), 40**
- Smurf IP attacks, 105–106**
- Sneakers, 18**
- SNMP (Simple Network Management Protocol), 156**

- Snort**, 256–260
- Snow**, 234
- Snowden, Edward**, 14
- Sobig virus**, 126
- social engineering**, 9, 191
- social media**, 374–375
- sockets**, 40
- SoftPerfect Network Protocol Analyzer**, 415
- software installation, security policies for**, 284
- SOX (Sarbanes-Oxley)**, 299
- spam**, 139
- SPAP (Shiva Password Authentication Protocol)**, 262
- sparse infector viruses**, 123
- spear phishing**, 198
- specialist support**, 394
- specificity, online threats**, 79
- Specter**, 260–261
- SPI (stateful packet inspection)**, 105, 249
- spyware**
 - antispyware software, 194, 253–254
 - defined, 9
 - delivery of, 135
 - explained, 134–135
 - FinFisher, 347
 - in industrial espionage, 193–194
 - legal uses of, 135
 - obtaining, 135–137
- SpywareGuide website**, 135–136
- SQL (Structured Query Language) injection**, 11–12, 162–164
- SSBI (Single Scope Background Investigation)**, 295
- SSDs (security sequence diagrams)**, 436–438
- SSH (Secure Shell)**, 39
- SSL (Secure Sockets Layer)**, 266–268
- Stacheldraht**, 101
- stack tweaking**, 104
- standards, defined**, 294
- stateful packet inspection (SPI)**, 105, 249
- Stealth Files 4**, 234
- steganography**, 193, 234
- StegVideo**, 234
- StopGeorgia.ru**, 346
- STP (shielded twisted-pair) cable**, 34
- stream ciphers**, 217
- striped disks**, 297
- striped disks with dedicated parity**, 297
- striped disks with distributed parity**, 298
- striped disks with dual parity**, 298
- Structured Query Language (SQL) injection**, 11–12
- Stuxnet**, 345–346
- SubBytpe step (AES)**, 221
- subnetting**, 43–44
- Subscriber Identity Module (SIM)**, 408
- substitution alphabet**, 210
- substitution ciphers**
 - Caesar cipher, 209–210
 - multi-alphabet substitution, 211–212
 - rail fence, 212–213
 - Vigenère, 212
- Super Wi-Fi**, 37
- Supervisory Control and Data Acquisitions (SCADA)**, 351–352
- swatting**, 78
- SWGDE (Scientific Working Group on Digital Evidence)**, 395
- SWGDE Model Standard Operation Procedures for Computer Forensics**, 395
- switches**, 35
- Symantec**, 266
- symmetric encryption. See single-key (symmetric) encryption**
- SYN (synchronize) requests**
 - SYN flood attacks
 - micro blocks, 103
 - overview of, 102–103

- RST cookies, 104
- SPI firewalls, 105
- stack tweaking, 104
- SYN cookies, 103–104
- SYN scans, 156
- SYN_RECEIVED state, 112

SysML (or Systems Modeling Language)
SysML (Systems Modeling Language), 428

system administration policies

- access control, 292–293
- change requests, 288–290
- departing employees, 287–288
- developmental policies, 293
- need for, 287
- new employees, 287
- security breaches, 290
 - DoS (denial of service), 291
 - hacker intrusions, 291–292
 - viruses, 290–291

system assessment

- patches, 307–308
- physical security, 314–315
- policies, 312–314
- ports, 308–311
- probes, 314
- protective software and devices, 311–312

system development life cycle, 427

system logs, 398

- firewall, 253
- Linux logs, 399
- Windows logs, 398

system security

- networks, 319–321
- servers, 317–319
- templates, 315
- workstations, 316–317

systems engineering

- cybersecurity and, 424
- defined, 423–424

- metrics, 428–430
- need for, 422–423
- readability analysis, 428
- requirements engineering, 424–426
- SecML (Security Modeling Language)
 - data interface diagrams, 438–439
 - misuse case diagrams, 432–436
 - overview of, 428, 430–432
 - security block diagrams, 439
 - security sequence diagrams, 436–438
- system development life cycle, 427
- use-case diagrams, 428
- WBS (Work Breakdown Structure), 426–427

Systems Modeling Language (SysML), 428

T

T1 connection lines, 36

T3 connection lines, 36

tables, rainbow, 232–233

TAILS (The Amnesiac Incognito Live System), 175

Taiwan Semiconductor Manufacturing Company, 129

TCP (Transmission Control Protocol) SYN flood attacks

- micro blocks, 103
- overview of, 102–103
- RST cookies, 104
- SPI firewalls, 105
- stack tweaking, 104
- SYN cookies, 103–104

TCP/IP protocols, 39–40

teardrop attacks, 108

Telnet, 39

templates, system security, 315

Temporal Key Integrity Protocol (TKIP), 37, 271

TeraBIT Virus Maker, 168–169

terminate and stay resident (TSR), 245

- termination, security policies and, 286**
- terminators, 33**
- terrorism. See cyber terrorism and cyber warfare**
- TFN (Tribal Flood Network), 101**
- TFN2K, 101**
- TFTP (Trivial File Transfer Protocol), 39**
- TGSs (ticket-granting servers), 264**
- Thawte, 266**
- thin-film bulk acoustic resonator (FBAR) technology, 188**
- Thomas, Bob, 128**
- threats. See also hacking; industrial espionage; security policies; security technology**
 - cyber stalking
 - assessment of, 78–79
 - crimes against children, 80–81
 - defined, 74
 - real-world examples, 75–78
 - cyber terrorism
 - disinformation, 355
 - economic attacks, 347–349
 - future trends, 359–361
 - general attacks, 350–351
 - information control, 353–355
 - information warfare, 352
 - military operations attacks, 350
 - propaganda, 352–353
 - real-world examples, 343–347, 355–359
 - SCADA (Supervisory Control and Data Acquisitions), 351–352
 - scope of problem, 342–343
 - DNS poisoning, 8, 14–15
 - DoS (denial of service) attacks, 291
 - DDoS (distributed denial of service) attacks, 10, 99, 109
 - defending against, 111–112
 - defined, 7, 10
 - DHCP starvation, 108
 - Fraggle attacks, 106
 - HTTP POST DoS attacks, 108
 - ICMP (Internet Control Message Protocol) flood attacks, 107
 - illustration of, 97–99
 - land attacks, 109
 - login DoS attacks, 108
 - PDoS (permanent denial of service), 108
 - PoD (ping of death), 107–108
 - real-world examples, 109–111
 - registration DoS attacks, 108
 - scope of problem, 97
 - security policies for, 291
 - Smurf IP attacks, 105–106
 - TCP (Transmission Control Protocol) SYN flood attacks, 102–105
 - teardrop attacks, 108
 - tools for, 99–101
 - UDP (User Datagram Protocol) flood attacks, 107
 - doxxing, 15
 - dumpster diving, 370
 - identity theft
 - cross-site scripting, 73
 - phishing, 73–74
 - scope of problem, 72–73
 - insider, 8, 13–14
 - Internet fraud
 - auction fraud, 70–72
 - how it works, 67
 - investment fraud, 67–69
 - scope of problem, 66–67
 - key loggers, 9
 - logic bombs, 9
 - malware
 - Agent.btz, 344
 - antivirus software, 140–143
 - APTs (advanced persistent threats), 139–140
 - BlackEnergy, 347
 - buffer-overflow attacks, 132–133

- creating, 168–169
- defined, 7
- dynamic nature of, 121
- FinFisher, 347
- Flame, 346
- logic bombs, 139
- malicious web-based code, 138
- NSA ANT catalog, 347
- remediation steps, 144
- rootkits, 137–138
- spam, 139
- spyware, 9, 134–137, 253–254
- StopGeorgia.ru, 346
- Stuxnet, 345–346
- Trojan horses, 8, 129–132
- viruses, 8, 110, 121–129, 290–291. *See also* virus scanners
- worms, 110

risk assessment, 4–7, 16

scope of problem, 3

security activities, 19

security breaches. *See also* hacking

- cracking, 9
- defined, 7
- insider threats, 13–14
- social engineering, 9, 191
- war-dialing, 10
- war-driving, 10
- war-flying, 10

security devices, 19

security policies for, 290

session hijacking, 7, 13

web attacks

- cell phone attacks, 166
- cookie poisoning, 165–166
- cross-site request forgery, 165
- cross-site scripting, 12–13, 165
- defined, 7
- directory traversal, 165

- password cracking, 166–168
- SQL injection, 11–12, 162–164
- URL hijacking, 166
- wireless, 166

Tiajin University, 188

ticket-granting servers (TGSs), 264

Tiny Keylogger, 135

TKIP (Temporal Key Integrity Protocol), 37, 271

TLS (Transport Layer Security), 266–268

tool certifications, 413

top secret information, 294

top secret SCI (sensitive compartmented information), 294

TOR network, 173–175, 363–364

totient, 225

traceability matrix, 426

tracert command, 52

transference

= risk, 6

Locard's principle of, 395

Transmission Control Protocol. *See* TCP (Transmission Control Protocol) SYN flood attacks

Transport Layer Security (TLS), 266–268

Tribal Flood Network (TFN), 101

Trinoo DDoS tool, 101

Triple DES (3DES), 219

Trithemius, Johannes, 234

Trivial File Transfer Protocol (TFTP), 39

Trojan horses, 8, 129–132

Turing, Alan, 214

Twofish, 220

TypO, 135

U

Uber Technologies Inc. 188

UDP (User Datagram Protocol) flood attacks, 107

Ulbricht, Ross, 364

- UML (Unified Modeling Language), 428, 431, 439**
 - UMTS (Universal Mobile Telecommunications System), 409**
 - Unified Modeling Language (UML), 428, 431, 439**
 - uniform resource locators (URLs), 46, 166**
 - uninstalled software, finding, 407**
 - UNIT 61398 (China), 140, 345**
 - Universal Mobile Telecommunications System (UMTS), 409**
 - University of Dayton School of Law, 82**
 - university trade secrets, industrial espionage incidents involving, 188**
 - unshielded twisted-pair (UTP) cable, 34**
 - URLs (uniform resource locators), 46, 166**
 - U.S. Cyber Command (USCYBERCOM), 360**
 - U.S. Department of Defense clearance levels, 294–295**
 - U.S. Office of Personnel Management, breach of, 358**
 - U.S. Secret Service forensics guidelines, 393–394**
 - USB information, 406–407**
 - USBSTOR key, 406**
 - use-case diagrams, 428**
 - Usenet, 379**
 - User Datagram Protocol (UDP) flood attacks, 107**
 - user policies**
 - BYOD (Bring Your Own Device), 285
 - consequences for violating, 286–287
 - CYOD (Choose Your Own Device), 285
 - defining, 280
 - desktop configuration, 285
 - e-mail attachments, 283–284
 - instant messaging, 284
 - Internet use, 282–283
 - ISO 17799 standard, 279–280
 - passwords, 281
 - purpose of, 279
 - software installation and removal, 284
 - termination or expulsion and, 286
 - user.log file, 399**
 - utilities, network**
 - arp, 54–55
 - FDISK, 170
 - ipconfig, 49–51
 - netstat, 53
 - nslookup, 53
 - ping, 51–52, 156
 - DoS (denial of service) attacks, 97–99, 107–108
 - ping of death (PoD), 107–108
 - ping scans, 156
 - route, 54–55
 - tracert, 52
 - UTP (unshielded twisted-pair) cable, 34**
-
- ## V
- /var/log/apache2/*399**
 - /var/log/appport.log, 399**
 - /var/log/faillog, 399**
 - /var/log/kern.log, 399**
 - /var/log/lighttpd/*399**
 - /var/log/lpr.log, 399**
 - /var/log/mail.*399**
 - /var/log/mysql.*399**
 - /var/log/user.log, 399**
 - VBA (Visual Basic for Applications), 122**
 - .vbox file, 416**
 - .vdi file, 416**
 - vehicles, attacks targeting, 16**
 - VeraCrypt, 195–196**
 - Verisign, 266**
 - .vhx file, 416**
 - Vigenère, Blaise de, 212**
 - virtual forensics**
 - cloud, 416–417
 - VMs (virtual machines), 415–416

virtual machines (VMs), 144, 415–416

virtual private networks (VPNs), 268–270

virtualization, 415

virus scanners

defined, 245

how they work, 245–246, 247

scanning techniques, 246–247

viruses, 110. See also virus scanners

antivirus software, 140–143

avoiding, 129

defined, 8, 121

hoaxes, 127–128

impact of, 129

MyDoom, 110–111

real-world examples, 123–128

Atlanta's ransomware attack, 125

Bagle, 127

CryptoLocker, 124–125

CryptoWall, 124–125

earliest viruses, 128

FakeAV, 125

Flame, 128

Gameover ZeuS, 124

hoaxes, 127–128

Kedi RAT (Remote Access Trojan), 125

MacDefender, 125

Mimail, 127

Petya, 124

Rombertik, 124

Shamoon, 124

Sobig, 126

WannaCry, 123–124

security policies for, 290–291

Serpent, 222

spread of, 121–122

types of, 122–123

virulence of, 126

Visual Basic for Applications (VBA), 122

visual inspection, 395

.vmdk file, 416

.vmem file, 416

VMs (virtual machines), 144, 415–416

.vmsd file, 416

.vmsn file, 416

VMware, 144

VPNs (virtual private networks), 268–270

vulnerability assessment, 158–159

MBSA (Microsoft Baseline Security Analyzer),
321–323

Nessus, 324–326

OWASP (Open Web Application Security
Project), 326–327

professional consultants, 330–332

Shodan, 328–329

W

Wabbit, 128

WannaCry, 123–124

WAPs (wireless access points), 166, 271

war-dialing, 10

war-driving, 10

warfare. See cyber terrorism and cyber warfare

war-flying, 10

Waymo, 188

WBS (Work Breakdown Structure), 426–427

web attacks

cell phone attacks, 166

cookie poisoning, 165–166

cross-site request forgery, 165

cross-site scripting, 12–13, 165

defined, 7

directory traversal, 165

password cracking, 166–168

SQL injection, 11–12, 162–164

URL hijacking, 166

wireless, 166

web-based mobile code, 138

WEP (Wired Equivalent Privacy), 37, 271

whaling, 198

white hat hackers, 17, 152–153

White-Fi, 37

Whois, 39

Wi-Fi, 36–38, 270–271, 412

WPA (Wi-Fi Protected Access), 37–38, 271

WPS (Wi-Fi Protected Setup), 166

Williamson, Malcolm J.227

Windows 10 Windows Defender, 252–253

Windows configuration

commands

fc, 403

net sessions, 402

netstat, 404

openfiles, 403

registry settings, 404–407

services, shutting down, 309–310

system logs, 398

Windows Defender, 143, 252–253

Windows EFS (Encrypted File System), 195–196

Windows forensics, 411

Windows hacking techniques

login as system, 170

net user script, 169–170

pass the hash, 169–170

WinZapper, 398

Wired Equivalent Privacy (WEP), 37, 271

wireless access points (WAPs), 166, 271

wireless attacks, 166

wireless networks

802.11 standard, 36–38

ANT+38

Bluetooth, 38

security, 37–38

Wi-Fi security, 270–271

ZigBee, 38

Z-Wave, 38

Wireshark, 415

Work Breakdown Structure (WBS), 426–427

workstation security, 316–317

worms, 110. See also malware

WPA (Wi-Fi Protected Access), 37–38, 271

WPS (Wi-Fi Protected Setup), 166

Writing Snort Rules website, 260

X

X.25 networks, 269

X.509 certificates, 265–266

.xml files, 416

XOIC, 100

XOR operation, 215–216

Y-Z

Yahoo! People Search, 372–373

Yung, Ho Ka Terence, 77

Zenmap, 156

Zhang, Hao, 188

ZigBee, 38

Zimmermann, Phil, 228

zone transfers, 57

ZoneAlarm, 252

Z-Wave, 38

Zygalski, Henryk, 213