

DAVID L. PROWSE



Cert Guide

Learn, prepare, and practice for exam success



CompTIA® Security+ SY0-501



PEARSON IT
CERTIFICATION

**Save 10%
on Exam
Voucher**

See Inside

FEATURES

Three Complete Practice Exams, More Than
30 Videos and 30 Interactive Exercises

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



CompTIA® Security+

SY0-501 Cert Guide

Fourth Edition

David L. Prowse

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

CompTIA® Security+ SY0-501 Cert Guide Fourth Edition

Copyright © 2018 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: 978-0-7897-5899-6

ISBN-10: 0-7897-5899-7

Library of Congress Control Number: 2017951236

Printed in the United States of America

1 17

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification 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.

CompTIA is a registered trademark of CompTIA, Inc.

Chapter opener image copyright

Charlie Edwards/Photodisc/Getty Images.

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.

Editor-in-Chief

Mark Taub

Product Line Manager

Brett Bartow

Acquisitions Editor

Michelle Newcomb

Development Editor

Eleanor Bru

Managing Editor

Sandra Schroeder

Senior Project Editor

Tonya Simpson

Copy Editor

Bill McManus

Indexer

Ken Johnson

Proofreader

Paula Lowell

Technical Editor

Chris Crayton

Publishing Coordinator

Vanessa Evans

Cover Designer

Chuti Prasertsith

Compositor

Studio Galou

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 screenshots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. 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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Contents at a Glance

Introduction xxiv

CHAPTER 1	Introduction to Security	3
CHAPTER 2	Computer Systems Security Part I	19
CHAPTER 3	Computer Systems Security Part II	53
CHAPTER 4	OS Hardening and Virtualization	89
CHAPTER 5	Application Security	127
CHAPTER 6	Network Design Elements	173
CHAPTER 7	Networking Protocols and Threats	217
CHAPTER 8	Network Perimeter Security	255
CHAPTER 9	Securing Network Media and Devices	285
CHAPTER 10	Physical Security and Authentication Models	321
CHAPTER 11	Access Control Methods and Models	361
CHAPTER 12	Vulnerability and Risk Assessment	397
CHAPTER 13	Monitoring and Auditing	435
CHAPTER 14	Encryption and Hashing Concepts	477
CHAPTER 15	PKI and Encryption Protocols	521
CHAPTER 16	Redundancy and Disaster Recovery	547
CHAPTER 17	Social Engineering, User Education, and Facilities Security	583
CHAPTER 18	Policies and Procedures	613
CHAPTER 19	Taking the Real Exam	647
	Practice Exam I: SY0-501	657
	Glossary	719
	Index	749

Elements Available Online

View Recommended Resources

Real-World Scenarios

Table of Contents

Introduction xxiv

Chapter 1 Introduction to Security 3

Foundation Topics 4

Security 101 4

The CIA of Computer Security 4

The Basics of Information Security 6

Think Like a Hacker 9

Threat Actor Types and Attributes 10

Chapter Review Activities 12

Review Key Topics 12

Define Key Terms 12

Review Questions 13

Answers and Explanations 15

Chapter 2 Computer Systems Security Part I 19

Foundation Topics 19

Malicious Software Types 19

Viruses 20

Worms 21

Trojan Horses 22

Ransomware 22

Spyware 23

Rootkits 24

Spam 25

Summary of Malware Threats 25

Delivery of Malware 26

Via Software, Messaging, and Media 26

Botnets and Zombies 28

Active Interception 28

Privilege Escalation 29

Backdoors 29

Logic Bombs 29

Preventing and Troubleshooting Malware	30
Preventing and Troubleshooting Viruses	31
Preventing and Troubleshooting Worms and Trojans	35
Preventing and Troubleshooting Spyware	35
Preventing and Troubleshooting Rootkits	38
Preventing and Troubleshooting Spam	38
You Can't Save Every Computer from Malware!	40
Summary of Malware Prevention Techniques	40
Chapter Summary	41
Chapter Review Activities	42
Review Key Topics	42
Define Key Terms	42
Complete the Real-World Scenarios	43
Review Questions	43
Answers and Explanations	48
Chapter 3 Computer Systems Security Part II	53
Foundation Topics	53
Implementing Security Applications	53
Personal Software Firewalls	53
Host-Based Intrusion Detection Systems	55
Pop-Up Blockers	57
Data Loss Prevention Systems	59
Securing Computer Hardware and Peripherals	59
Securing the BIOS	60
Securing Storage Devices	62
<i>Removable Storage</i>	62
<i>Network Attached Storage</i>	63
<i>Whole Disk Encryption</i>	64
<i>Hardware Security Modules</i>	65
Securing Wireless Peripherals	66
Securing Mobile Devices	66
Malware	67
Botnet Activity	68
SIM Cloning and Carrier Unlocking	68

	Wireless Attacks	69
	Theft	70
	Application Security	71
	BYOD Concerns	74
	Chapter Summary	78
	Chapter Review Activities	79
	Review Key Topics	79
	Define Key Terms	79
	Complete the Real-World Scenarios	80
	Review Questions	80
	Answers and Explanations	83
Chapter 4	OS Hardening and Virtualization	89
	Foundation Topics	89
	Hardening Operating Systems	89
	Removing Unnecessary Applications and Services	90
	Windows Update, Patches, and Hotfixes	97
	<i>Patches and Hotfixes</i>	99
	<i>Patch Management</i>	101
	Group Policies, Security Templates, and Configuration Baselines	102
	Hardening File Systems and Hard Drives	105
	Virtualization Technology	109
	Types of Virtualization and Their Purposes	110
	Hypervisor	111
	Securing Virtual Machines	113
	Chapter Summary	115
	Chapter Review Activities	117
	Review Key Topics	117
	Define Key Terms	118
	Complete the Real-World Scenarios	118
	Review Questions	118
	Answers and Explanations	122
Chapter 5	Application Security	127
	Foundation Topics	127
	Securing the Browser	127

General Browser Security Procedures	129
<i>Implement Policies</i>	129
<i>Train Your Users</i>	133
<i>Use a Proxy and Content Filter</i>	133
<i>Secure Against Malicious Code</i>	135
Web Browser Concerns and Security Methods	135
<i>Basic Browser Security</i>	135
<i>Cookies</i>	136
<i>LSOs</i>	137
<i>Add-ons</i>	137
<i>Advanced Browser Security</i>	138
Securing Other Applications	140
Secure Programming	144
Software Development Life Cycle	145
Core SDLC and DevOps Principles	146
Programming Testing Methods	149
<i>White-box and Black-box Testing</i>	149
<i>Compile-Time Errors Versus Runtime Errors</i>	150
<i>Input Validation</i>	150
<i>Static and Dynamic Code Analysis</i>	151
<i>Fuzz Testing</i>	152
Programming Vulnerabilities and Attacks	152
<i>Backdoors</i>	153
<i>Memory/Buffer Vulnerabilities</i>	153
<i>Arbitrary Code Execution/Remote Code Execution</i>	155
<i>XSS and XSRF</i>	155
<i>More Code Injection Examples</i>	156
<i>Directory Traversal</i>	158
<i>Zero Day Attack</i>	158
Chapter Summary	160
Chapter Review Activities	161
Review Key Topics	161
Define Key Terms	162
Complete the Real-World Scenarios	162

	Review Questions	162
	Answers and Explanations	167
Chapter 6	Network Design Elements	173
	Foundation Topics	173
	Network Design	173
	The OSI Model	173
	Network Devices	175
	<i>Switch</i>	175
	<i>Bridge</i>	178
	<i>Router</i>	178
	Network Address Translation, and Private Versus Public IP	180
	Network Zones and Interconnections	182
	<i>LAN Versus WAN</i>	182
	<i>Internet</i>	183
	<i>Demilitarized Zone (DMZ)</i>	183
	<i>Intranets and Extranets</i>	184
	Network Access Control (NAC)	185
	Subnetting	186
	Virtual Local Area Network (VLAN)	188
	Telephony	190
	<i>Modems</i>	190
	<i>PBX Equipment</i>	191
	<i>VoIP</i>	191
	Cloud Security and Server Defense	192
	Cloud Computing	192
	Cloud Security	195
	Server Defense	198
	<i>File Servers</i>	198
	<i>Network Controllers</i>	199
	<i>E-mail Servers</i>	199
	<i>Web Servers</i>	200
	<i>FTP Server</i>	202
	Chapter Summary	203
	Chapter Review Activities	205

	Review Key Topics	205
	Define Key Terms	205
	Complete the Real-World Scenarios	205
	Review Questions	206
	Answers and Explanations	210
Chapter 7	Networking Protocols and Threats	217
	Foundation Topics	217
	Ports and Protocols	217
	Port Ranges, Inbound Versus Outbound, and Common Ports	217
	Protocols That Can Cause Anxiety on the Exam	225
	Malicious Attacks	226
	DoS	226
	DDoS	229
	Sinkholes and Blackholes	230
	Spoofing	231
	Session Hijacking	232
	Replay	234
	Null Sessions	235
	Transitive Access and Client-Side Attacks	236
	DNS Poisoning and Other DNS Attacks	236
	ARP Poisoning	238
	Summary of Network Attacks	238
	Chapter Summary	242
	Chapter Review Activities	243
	Review Key Topics	243
	Define Key Terms	243
	Complete the Real-World Scenarios	243
	Review Questions	244
	Answers and Explanations	250
Chapter 8	Network Perimeter Security	255
	Foundation Topics	256
	Firewalls and Network Security	256
	Firewalls	256
	Proxy Servers	263

	Honeypots and Honeynets	266
	Data Loss Prevention (DLP)	267
	NIDS Versus NIPS	268
	NIDS	268
	NIPS	269
	Summary of NIDS Versus NIPS	271
	The Protocol Analyzer's Role in NIDS and NIPS	271
	Unified Threat Management	272
	Chapter Summary	273
	Chapter Review Activities	274
	Review Key Topics	274
	Define Key Terms	274
	Complete the Real-World Scenarios	274
	Review Questions	275
	Answers and Explanations	280
Chapter 9	Securing Network Media and Devices	285
	Foundation Topics	285
	Securing Wired Networks and Devices	285
	Network Device Vulnerabilities	285
	<i>Default Accounts</i>	286
	<i>Weak Passwords</i>	286
	<i>Privilege Escalation</i>	287
	<i>Back Doors</i>	288
	<i>Network Attacks</i>	289
	<i>Other Network Device Considerations</i>	289
	Cable Media Vulnerabilities	289
	<i>Interference</i>	290
	<i>Crosstalk</i>	291
	<i>Data Emanation</i>	292
	<i>Tapping into Data and Conversations</i>	293
	Securing Wireless Networks	295
	Wireless Access Point Vulnerabilities	295
	<i>The Administration Interface</i>	295
	<i>SSID Broadcast</i>	296

<i>Rogue Access Points</i>	296
<i>Evil Twin</i>	297
<i>Weak Encryption</i>	297
<i>Wi-Fi Protected Setup</i>	299
<i>Ad Hoc Networks</i>	299
<i>VPN over Open Wireless</i>	300
Wireless Access Point Security Strategies	300
Wireless Transmission Vulnerabilities	304
Bluetooth and Other Wireless Technology Vulnerabilities	305
<i>Bluejacking</i>	306
<i>Bluesnarfing</i>	306
<i>RFID and NFC</i>	307
<i>More Wireless Technologies</i>	308
Chapter Summary	310
Chapter Review Activities	312
Review Key Topics	312
Define Key Terms	312
Complete the Real-World Scenarios	312
Review Questions	313
Answers and Explanations	317
Chapter 10 Physical Security and Authentication Models	321
Foundation Topics	322
Physical Security	322
General Building and Server Room Security	323
Door Access	324
Biometric Readers	326
Authentication Models and Components	327
Authentication Models	327
Localized Authentication Technologies	329
<i>802.1X and EAP</i>	330
<i>LDAP</i>	333
<i>Kerberos and Mutual Authentication</i>	334
<i>Remote Desktop Services</i>	336
Remote Authentication Technologies	337

	<i>Remote Access Service</i>	337
	<i>Virtual Private Networks</i>	340
	<i>RADIUS Versus TACACS</i>	343
	Chapter Summary	345
	Chapter Review Activities	346
	Review Key Topics	346
	Define Key Terms	347
	Complete the Real-World Scenarios	347
	Review Questions	347
	Answers and Explanations	355
Chapter 11	Access Control Methods and Models	361
	Foundation Topic	361
	Access Control Models Defined	361
	Discretionary Access Control	361
	Mandatory Access Control	363
	Role-Based Access Control (RBAC)	364
	Attribute-based Access Control (ABAC)	365
	Access Control Wise Practices	366
	Rights, Permissions, and Policies	369
	Users, Groups, and Permissions	369
	Permission Inheritance and Propagation	374
	Moving and Copying Folders and Files	376
	Usernames and Passwords	376
	Policies	379
	User Account Control (UAC)	383
	Chapter Summary	384
	Chapter Review Activities	385
	Review Key Topics	385
	Define Key Terms	386
	Complete the Real-World Scenarios	386
	Review Questions	386
	Answers and Explanations	392
Chapter 12	Vulnerability and Risk Assessment	397
	Foundation Topics	397
	Conducting Risk Assessments	397

Qualitative Risk Assessment	399
Quantitative Risk Assessment	400
Security Analysis Methodologies	402
Security Controls	404
Vulnerability Management	405
<i>Penetration Testing</i>	407
<i>OVAL</i>	408
<i>Additional Vulnerabilities</i>	409
Assessing Vulnerability with Security Tools	410
Network Mapping	411
Vulnerability Scanning	412
Network Sniffing	415
Password Analysis	417
Chapter Summary	420
Chapter Review Activities	421
Review Key Topics	421
Define Key Terms	422
Complete the Real-World Scenarios	422
Review Questions	422
Answers and Explanations	428
Chapter 13 Monitoring and Auditing	435
Foundation Topics	435
Monitoring Methodologies	435
Signature-Based Monitoring	435
Anomaly-Based Monitoring	436
Behavior-Based Monitoring	436
Using Tools to Monitor Systems and Networks	437
Performance Baselineing	438
Protocol Analyzers	440
<i>Wireshark</i>	441
SNMP	443
Analytical Tools	445
Use Static <i>and</i> Dynamic Tools	447
Conducting Audits	448
Auditing Files	448

Logging	451
Log File Maintenance and Security	455
Auditing System Security Settings	457
SIEM	460
Chapter Summary	461
Chapter Review Activities	462
Review Key Topics	462
Define Key Terms	463
Complete the Real-World Scenarios	463
Review Questions	463
Answers and Explanations	470
Chapter 14 Encryption and Hashing Concepts	477
Foundation Topics	477
Cryptography Concepts	477
Symmetric Versus Asymmetric Key Algorithms	481
<i>Symmetric Key Algorithms</i>	481
Asymmetric Key Algorithms	483
Public Key Cryptography	483
Key Management	484
Steganography	485
Encryption Algorithms	486
DES and 3DES	486
AES	487
RC	488
Blowfish and Twofish	489
Summary of Symmetric Algorithms	489
RSA	490
Diffie-Hellman	491
Elliptic Curve	492
More Encryption Types	493
<i>One-Time Pad</i>	493
PGP	494
<i>Pseudorandom Number Generators</i>	495
Hashing Basics	496

Cryptographic Hash Functions	498
MD5	498
SHA	498
RIPEMD and HMAC	499
LANMAN, NTLM, and NTLMv2	500
LANMAN	500
NTLM and NTLMv2	501
Hashing Attacks	502
Pass the Hash	502
Happy Birthday!	503
Additional Password Hashing Concepts	503
Chapter Summary	505
Chapter Review Activities	507
Review Key Topics	507
Define Key Terms	507
Complete the Real-World Scenarios	508
Review Questions	508
Answers and Explanations	515
Chapter 15 PKI and Encryption Protocols	521
Foundation Topics	521
Public Key Infrastructure	521
Certificates	522
SSL Certificate Types	522
Single-Sided and Dual-Sided Certificates	523
Certificate Chain of Trust	523
Certificate Formats	523
Certificate Authorities	525
Web of Trust	529
Security Protocols	529
S/MIME	530
SSL/TLS	531
SSH	532
PPTP, L2TP, and IPsec	533
PPTP	533

<i>L2TP</i>	534
<i>IPsec</i>	534
Chapter Summary	535
Chapter Review Activities	536
Review Key Topics	536
Define Key Terms	536
Complete the Real-World Scenarios	537
Review Questions	537
Answers and Explanations	542
Chapter 16 Redundancy and Disaster Recovery	547
Foundation Topics	547
Redundancy Planning	547
Redundant Power	549
Redundant Power Supplies	551
Uninterruptible Power Supplies	551
Backup Generators	553
Redundant Data	555
Redundant Networking	558
Redundant Servers	560
Redundant Sites	561
Redundant People	562
Disaster Recovery Planning and Procedures	562
Data Backup	562
DR Planning	567
Chapter Summary	571
Chapter Review Activities	572
Review Key Topics	572
Define Key Terms	572
Complete the Real-World Scenarios	573
Review Questions	573
Answers and Explanations	577
Chapter 17 Social Engineering, User Education, and Facilities Security	583
Foundation Topics	583
Social Engineering	583

Pretexting	584
Malicious Insider	585
Diversion Theft	586
Phishing	586
Hoaxes	587
Shoulder Surfing	588
Eavesdropping	588
Dumpster Diving	588
Baiting	589
Piggybacking/Tailgating	589
Watering Hole Attack	589
Summary of Social Engineering Types	590
User Education	591
Facilities Security	593
Fire Suppression	594
<i>Fire Extinguishers</i>	594
<i>Sprinkler Systems</i>	595
<i>Special Hazard Protection Systems</i>	596
HVAC	597
Shielding	598
Vehicles	600
Chapter Summary	602
Chapter Review Activities	603
Review Key Topics	603
Define Key Terms	603
Complete the Real-World Scenarios	603
Review Questions	604
Answers and Explanations	608
Chapter 18 Policies and Procedures	613
Foundation Topics	614
Legislative and Organizational Policies	614
Data Sensitivity and Classification of Information	615
Personnel Security Policies	617
<i>Privacy Policies</i>	618

<i>Acceptable Use</i>	618
<i>Change Management</i>	619
<i>Separation of Duties/Job Rotation</i>	619
<i>Mandatory Vacations</i>	620
<i>Onboarding and Offboarding</i>	620
<i>Due Diligence</i>	621
<i>Due Care</i>	621
<i>Due Process</i>	621
<i>User Education and Awareness Training</i>	621
<i>Summary of Personnel Security Policies</i>	622
How to Deal with Vendors	623
How to Dispose of Computers and Other IT Equipment Securely	625
Incident Response Procedures	627
IT Security Frameworks	633
Chapter Summary	635
Chapter Review Activities	636
Review Key Topics	636
Define Key Terms	636
Complete the Real-World Scenarios	637
Review Questions	637
Answers and Explanations	641
Chapter 19 Taking the Real Exam	647
Getting Ready and the Exam Preparation Checklist	647
Tips for Taking the Real Exam	651
Beyond the CompTIA Security+ Certification	655
Practice Exam 1: SY0-501	657
Answers to Practice Exam 1	679
Answers with Explanations	680
Glossary	718
Index	749
Elements Available Online	
View Recommended Resources	
Real-World Scenarios	

About the Author

David L. Prowse is an author, technologist, and technical trainer. He has penned a dozen books for Pearson Education, including the well-received *CompTIA A+ Exam Cram*. He also develops video content, including the *CompTIA A+ LiveLessons* video course. Over the past two decades he has taught CompTIA A+, Network+, and Security+ certification courses, both in the classroom and via the Internet. David has 20 years of experience in the IT field and loves to share that experience with his readers, watchers, and students.

He runs the website www.davidlprowse.com in support of his books and videos.

Acknowledgments

It takes a lot of amazing people to publish a book. Special thanks go to Eleanor Bru, Chris Crayton, Michelle Newcomb, and all the other people at Pearson (and beyond) who helped make this book a reality. I appreciate everything you do!

About the Technical Reviewer

Chris Crayton (MCSE) is an author, technical consultant, and trainer. In the past, he has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several leading publishing companies. Chris holds numerous industry certifications, has been recognized with many professional teaching awards, and has served as a state-level SkillsUSA competition judge.

We Want to Hear from You!

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

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

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

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

Email: feedback@pearsonitcertification.com

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

Reader Services

Register your copy of *CompTIA Security+ SY0-501 Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account.* Enter the product ISBN 9780789758996 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

Introduction

Welcome to the *CompTIA Security+ SY0-501 Cert Guide*. The CompTIA Security+ Certification is widely accepted as the first security certification you should attempt to attain in your information technology (IT) career. The CompTIA Security+ Certification is designed to be a vendor-neutral exam that measures your knowledge of industry-standard technologies and methodologies. It acts as a great stepping stone to other vendor-specific certifications and careers. I developed this book to be something you can study from for the exam and keep on your bookshelf for later use as a security resource.

I'd like to note that it's unfeasible to cover all security concepts in depth in a single book. However, the Security+ exam objectives are looking for a basic level of computer, networking, and organizational security knowledge. Keep this in mind while reading through this text, and remember that the main goal of this text is to help you pass the Security+ exam, not to be the master of all security. Not just yet at least!

Good luck as you prepare to take the CompTIA Security+ exam. As you read through this book, you will be building an impenetrable castle of knowledge, culminating in hands-on familiarity and the know-how to pass the exam.

IMPORTANT NOTE The first thing you should do before you start reading Chapter 1, "Introduction to Security," is check my website for errata and updated information, and mark those new items in the book. Go to www.davidlprowse.com and then the Security+ section. On my site you will also find videos, bonus test questions, and other additional content. And, of course, you can contact me directly at my website to ask me questions about the book.

Goals and Methods

The number one goal of this book is to help you pass the SY0-501 version of the CompTIA Security+ Certification Exam. To that effect, I have filled this book and practice exams with more than 600 questions/answers and explanations in total, including three 80-question practice exams. One of the exams is printed at the end of the book, and all exams are located in Pearson Test Prep practice test software in a custom test environment. These tests are geared to check your knowledge and ready you for the real exam.

The CompTIA Security+ Certification exam involves familiarity with computer security theory and hands-on know-how. To aid you in mastering and understanding the Security+ Certification objectives, this book uses the following methods:

- **Opening topics list:** This defines the topics to be covered in the chapter.
- **Topical coverage:** The heart of the chapter. Explains the topics from a theory-based standpoint, as well as from a hands-on perspective. This includes in-depth descriptions, tables, and figures that are geared to build your knowledge so that you can pass the exam. The chapters are broken down into two to three topics each.
- **Key Topics:** The Key Topic icons indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in table format at the end of the chapter.
- **Key Terms:** Key terms without definitions are listed at the end of each chapter. See whether you can define them, and then check your work against the complete key term definitions in the glossary.
- **Real-World Scenarios:** Included in the supplemental online material are real-world scenarios for each chapter. These offer the reader insightful questions and problems to solve. The questions are often open-ended, and can have several different solutions. The online material gives one or more possible solutions and then points to video-based solutions and simulation exercises online to further reinforce the concepts. Refer to these real-world scenarios at the end of each chapter.
- **Review Questions:** These quizzes, and answers with explanations, are meant to gauge your knowledge of the subjects. If an answer to a question doesn't come readily to you, be sure to review that portion of the chapter. The review questions are also available online.
- **Practice Exams:** There is one practice exam printed at the end of the book, and additional exams included in the Pearson Test Prep practice test software. These test your knowledge and skills in a realistic testing environment. Take these after you have read through the entire book. Master one, then move on to the next. Take any available bonus exams last.

Another goal of this book is to offer support for you, the reader. Again, if you have questions or suggestions, please contact me through my website: www.davidlprowse.com. I try my best to answer your queries as soon as possible.

Who Should Read This Book?

This book is for anyone who wants to start or advance a career in computer security. Readers of this book can range from persons taking a Security+ course to individuals already in the field who want to keep their skills sharp, or perhaps retain their job due to a company policy mandating they take the Security+ exam. Some information

assurance professionals who work for the Department of Defense or have privileged access to DoD systems are required to become Security+ certified as per DoD directive 8570.1.

This book is also designed for people who plan on taking additional security-related certifications after the CompTIA Security+ exam. The book is designed in such a way to offer an easy transition to future certification studies.

Although not a prerequisite, it is recommended that CompTIA Security+ candidates have at least two years of IT administration experience with an emphasis on security. The CompTIA Network+ certification is also recommended as a prerequisite. Before you begin your Security+ studies, it is expected that you understand computer topics such as how to install operating systems and applications, and networking topics such as how to configure IP, what a VLAN is, and so on. The focus of this book is to show how to secure these technologies and protect against possible exploits and attacks. Generally, for people looking to enter the IT field, the CompTIA Security+ certification is attained after the A+ and Network+ certifications.

CompTIA Security+ Exam Topics

If you haven't downloaded the Security+ certification exam objectives, do it now from CompTIA's website: <https://certification.comptia.org/>. Save the PDF file and print it out as well. It's a big document—review it carefully. Use the exam objectives list and acronyms list to aid in your studies while you use this book.

The following two tables are excerpts from the exam objectives document. Table I-1 lists the CompTIA Security+ domains and each domain's percentage of the exam.

Table I-1 CompTIA Security+ Exam Domains

Domain	Exam Topic	% of Exam
1.0	Threats, Attacks and Vulnerabilities	21%
2.0	Technologies and Tools	22%
3.0	Architecture and Design	15%
4.0	Identity and Access Management	16%
5.0	Risk Management	14%
6.0	Cryptography and PKI	12%

The Security+ domains are then further broken down into individual objectives. To achieve better flow and to present the topics in more of a building-block approach, I rearranged the concepts defined in the objectives. This approach is designed especially for people who are new to the computer security field.

Table I-2 lists the CompTIA Security+ exam objectives and their related chapters in this book. It does not list the bullets and sub-bullets for each objective.

NOTE Chapter 19 gives strategies for taking the exam and therefore does not map to any specific objectives.

Table I-2 CompTIA Security+ Exam Objectives

Objective	Chapter(s)
1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.	2, 13
1.2 Compare and contrast types of attacks.	7, 9, 14, 17
1.3 Explain threat actor types and attributes.	1, 17
1.4 Explain penetration testing concepts.	12
1.5 Explain vulnerability scanning concepts.	12
1.6 Explain the impact associated with types of vulnerabilities.	5, 12
2.1 Install and configure network components, both hardware- and software-based, to support organizational security.	6, 8, 10, 13, 15
2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.	13, 14, 18
2.3 Given a scenario, troubleshoot common security issues.	10, 11, 17
2.4 Given a scenario, analyze and interpret output from security technologies.	3, 4, 8
2.5 Given a scenario, deploy mobile devices securely.	3, 6, 9
2.6 Given a scenario, implement secure protocols.	6, 7, 13
3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.	12, 18
3.2 Given a scenario, implement secure network architecture concepts.	6, 7, 9, 10, 13
3.3 Given a scenario, implement secure systems design.	3, 4
3.4 Explain the importance of secure staging deployment concepts.	5, 12
3.5 Explain the security implications of embedded systems.	3, 4, 18
3.6 Summarize secure application development and deployment concepts.	5
3.7 Summarize cloud and virtualization concepts.	4, 6
3.8 Explain how resiliency and automation strategies reduce risk.	12, 16
3.9 Explain the importance of physical security controls.	10

Objective	Chapter(s)
4.1 Compare and contrast identity and access management concepts.	10
4.2 Given a scenario, install and configure identity and access services.	10
4.3 Given a scenario, implement identity and access management controls.	10, 11
4.4 Given a scenario, differentiate common account management practices.	11
5.1 Explain the importance of policies, plans and procedures related to organizational security.	18
5.2 Summarize business impact analysis concepts.	16
5.3 Explain risk management processes and concepts.	12, 18
5.4 Given a scenario, follow incident response procedures.	18
5.5 Summarize basic concepts of forensics.	18
5.6 Explain disaster recovery and continuity of operation concepts.	16
5.7 Compare and contrast various types of controls.	1, 12
5.8 Given a scenario, carry out data security and privacy practices.	18
6.1 Compare and contrast basic concepts of cryptography.	14
6.2 Explain cryptography algorithms and their basic characteristics.	14
6.3 Given a scenario, install and configure wireless security settings.	9, 10
6.4 Given a scenario, implement public key infrastructure.	15

Companion Website

Register this book to get access to the Pearson Test Prep practice test software and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

1. Go to www.pearsonitcertification.com/register and log in or create a new account.
2. On your Account page, tap or click the **Registered Products** tab, and then tap or click the **Register Another Product** link.
3. Enter this book's ISBN (9780789758996).

4. Answer the challenge question as proof of book ownership.
5. Tap or click the **Access Bonus Content** link for this book to go to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the preceding steps, please visit <http://www.pearsonitcertification.com/contact> and select the “Site Problems/Comments” option. Our customer service representatives will assist you.

Pearson Test Prep Practice Test Software

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

NOTE The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exams associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Accessing the Pearson Test Prep Software Online

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

1. Go to www.PearsonTestPrep.com and select **Pearson IT Certification** as your product group.
2. Enter your email/password for your account. If you do not have an account on PearsonITCertification.com or CiscoPress.com, you will need to establish one by going to PearsonITCertification.com/join.
3. On the My Products tab, tap or click the **Activate New Product** button.

4. Enter this book's activation code and click **Activate**.
5. The product will now be listed on your My Products tab. Tap or click the **Exams** button to launch the exam settings screen and start your exam.

Accessing the Pearson Test Prep Software Offline

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

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

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

1. Register your book by going to <http://www.pearsonitcertification.com/register> and entering the ISBN: **9780789758996**.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. Once the software finishes downloading, unzip all the files on your computer.
7. Double-click the application file to start the installation, and follow the onscreen instructions to complete the registration.
8. Once the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.
11. Click **Next** and then the **Finish** button to download the exam data to your application.
12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

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

Customizing Your Exams

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

- Study Mode
- Practice Exam Mode
- Flash Card Mode

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

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

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The exam printed in the book is available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all banks or just from one individual bank by selecting the desired banks in the exam bank area.

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

Updating Your Exams

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

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

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

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

Premium Edition eBook and Practice Tests

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



This chapter covers the following subjects:

- **Firewalls and Network Security:** In this section, you find out about one of the most important strategic pieces in your network security design—the firewall. Then we discuss other network security concepts such as packet filtering, access control lists, proxy servers, and honeypots.
- **NIDS Versus NIPS:** This section delves into the characteristics, advantages, disadvantages, and differences of network intrusion *detection* systems and network intrusion *prevention* systems.

This chapter is all about the network border, also known as the **network perimeter**. This should be a network security administrator's primary focus when it comes to securing the network because it contains the entrances that many attackers attempt to use.

Network Perimeter Security

Allow me to analogize for a few moments. I've said it before; as you read this book, you are building yourself an impenetrable castle of knowledge, culminating in hands-on familiarity and the know-how to pass the exam. But we can use the castle analogy for your network as well. Imagine a big stone castle with tall walls, an expanse of clear land around the castle, or perhaps a moat surrounding it (with alligators, of course), and one or more drawbridges. The tall walls are meant to keep the average person out, sort of like a firewall in a computer network—not perfect, but necessary. The open area around the castle makes it difficult for people to sneak up on your castle; they would quickly be *detected*, just like malicious packets detected by a network intrusion detection system. Or better yet, if you had a moat, people trying to cross it would have a difficult time, would be easy targets for your bowmen, and would probably be gobbled up by your pet alligators. This would represent a network intrusion *prevention* system, which not only detects threats, but also eliminates those threats to the network.

The drawbridge, or drawbridges, could be seen as network ports open to the network. As drawbridges are part of the castle wall, so network ports are part of the firewall. You, as the network security administrator, have the ability and the right to close these ports at any time. At the risk of taking this analogy even further, you might decide to set traps for people; like a pool of quicksand that has an open netted bag of pyrite suspended above it, or maybe a false entry to the castle that, after a long corridor, is walled off on the inside, ultimately trapping the unwary. In a network environment, these would be known as honeypots. Of course, every once in a while, legitimate traffic needs to enter and exit your network, too! To do this in a more secure fashion, you can set up proxy servers to act as go-betweens for the computers inside your network and the servers they talk to on the Internet: kind of like a sentry in the tower of the castle that would relay an outsider's messages to someone inside the castle.

The network perimeter is less tangible in an actual network environment (thus the previous use of superfluous metaphor). Networking devices are commonly located in a single server room or data center, or perhaps are located in a hybrid

of in-house and cloud-based locations. Either way, they can be difficult to visualize. To better envision your network, one of the best tips I can give you is to map out your network on paper, or create network documentation using programs such as Microsoft Visio and by utilizing network mapping tools (more on these tools in Chapter 12, “Vulnerability and Risk Assessment”).

So, before we end up playing *Dungeons & Dragons*, let’s talk about one of the most important parts of your strategic defense—the firewall.

Foundation Topics

Firewalls and Network Security

Nowadays, firewalls are everywhere. Businesses large and small use them, and many households have simpler versions of these protective devices as well. You need to be aware of several types of firewalls, and you definitely want to spend some time configuring hardware and software firewalls. There are many free software-based firewalls and firmware-based emulators that you can download. A quick search on the Internet will give you several options.

The firewall is there to protect the entire network, but other tools are often implemented as well; for example, proxy servers that help protect users and computers by keeping them anonymous; honeypots meant to attract hackers, crackers, and other types of attackers into a false computer or network; and data loss prevention (DLP) devices to keep confidential data from leaving the network. But by far, the most important element in your network will be the firewall, so let’s begin with that.

Firewalls

In Chapter 3, “Computer Systems Security Part II,” we discussed personal firewalls—you remember, the kind installed to an individual computer. Now let’s broaden the scope of your knowledge with network-based firewalls. Network-based firewalls are primarily used to section off and protect one network from another. They are a primary line of defense and are *extremely* important in network security. There are several types of firewalls; some run as software on server computers, some as standalone dedicated appliances, and some work as just one function of many on a single device. They are commonly represented as a sort of “brick wall” between a LAN and the Internet, as shown in Figure 8-1.

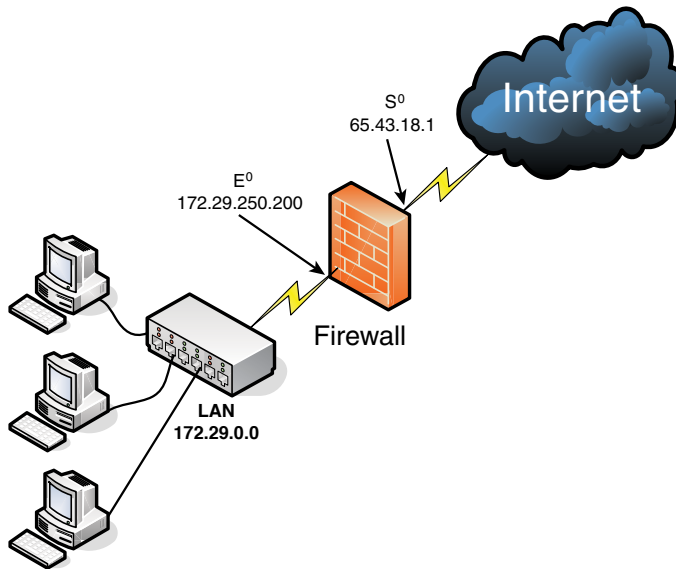
**Key
Topic**

Figure 8-1 Diagram of a Basic Firewall Implementation

Just as a firewall in a physical building is there to slow the spread of a fire and contain it until the fire department arrives, a firewall in a computer network is there to keep fire at bay in the form of malicious attacks. Often, a firewall (or the device the firewall resides on) has NAT in operation as well. In Figure 8-1, note that the firewall has a local address of 172.29.250.200; this connects it to the LAN. It also has an Internet address of 65.43.18.1, enabling connectivity for the entire LAN to the Internet, while hiding the LAN IP addresses. By default, the IP address 65.43.18.1 is completely shielded. This means that all inbound ports are effectively closed and will not enable incoming traffic, unless a LAN computer initiates a session with another system on the Internet. However, a good security administrator always checks this to make sure; first, by accessing the firewall's firmware (or software application, as the case may be) and verifying that the firewall is on, and next by scanning the firewall with third-party applications such as Nmap (<https://nmap.org>) or with a web-based port scanning utility, as was shown in a Chapter 7 Real-world Scenario. If any ports are open, or unshielded, they should be dealt with immediately. Then the firewall should be rescanned for vulnerabilities. You can find more information on port scanning and vulnerability assessments in Chapter 12.

Important point: Firewalls should be used only as they were intended. The company firewall should not handle any other extraneous services—for example, acting as a web server or SMTP server. By using a firewall as it was intended, its vulnerability is reduced.

Generally, a firewall inspects traffic that passes through it and permits or denies that traffic based on rules set by an administrator. These rules are stored within **access control lists** (ACLs). In regards to firewalls, an ACL is a set of rules that applies to a list of network names, IP addresses, and port numbers. These rules can be configured to control inbound and outbound traffic. This is a bit different than ACLs with respect to operating systems, which we cover in Chapter 11, “Access Control Methods and Models,” but the same basic principles apply: Basically, one entity is granted or denied permission to another entity. If you decide that a specific type of traffic should be granted access to your network, you would **explicitly allow** that traffic as a rule within an ACL. If on the other hand you decide that a specific type of traffic should *not* be granted access, you would **explicitly deny** that traffic within an ACL. And finally, if a type of network traffic is not defined in the firewall’s rule set, it should be stopped by default. This is the concept of **implicit deny** and is usually a default rule found in a firewall’s ACL. It is often added automatically to the end of a firewall’s rule set (ACLs) and is also known as “block all.”

Firewall rules should be specific. Here’s an example of a firewall rule:

```
deny TCP any any port 53
```

This rule can be used to restrict DNS zone transfers (as they run on top of TCP and use port 53), but other DNS traffic will still function properly. The rule is specific; it gives the transport layer protocol to be filtered, and the exact port, and also states that it applies to *any* computer’s IP address on the inbound and outbound side. Be careful with firewall rules and ACLs; they need to be written very cautiously so as not to filter required traffic.

NOTE Traffic can also be passed to other computers and servers, or to specific ports. For a quick tutorial on setting up virtual servers and port forwarding on a typical SOHO router/firewall, see the following link: <http://www.davidprowse.com/articles/?p=916>.

A lot of today’s firewalls have two types of firewall technologies built into them: SPI and NAT. However, you also should be aware of a couple other types of firewall methodologies:

**Key
Topic**

- **Packet filtering:** Inspects each packet passing through the firewall and accepts or rejects it based on rules. However, there are two types: stateless packet inspection and **stateful packet inspection** (also known as SPI or a stateful firewall). A stateless packet filter, also known as pure packet filtering, does not

retain memory of packets that have passed through the firewall; due to this, a stateless packet filter can be vulnerable to IP spoofing attacks. But a firewall running stateful packet inspection is normally not vulnerable to this because it keeps track of the state of network connections by examining the header in each packet. It can distinguish between legitimate and illegitimate packets. This function operates at the network layer of the OSI model.

- **NAT filtering:** Also known as NAT endpoint filtering, filters traffic according to ports (TCP or UDP). This can be done in three ways: by way of basic endpoint connections, by matching incoming traffic to the corresponding outbound IP address connection, or by matching incoming traffic to the corresponding IP address and port.
- **Application-level gateway (ALG):** Applies security mechanisms to specific applications, such as FTP or BitTorrent. It supports address and port translation and checks whether the type of application traffic is allowed. For example, your company might allow FTP traffic through the firewall, but might decide to disable Telnet traffic (probably a wise choice). The ALG checks each type of packet coming in and discards Telnet packets. Although this adds a powerful layer of security, the price is that it is resource-intensive, which could lead to performance degradation.
- **Circuit-level gateway:** Works at the session layer of the OSI model, and applies security mechanisms when a TCP or UDP connection is established; it acts as a go-between for the transport and application layers in TCP/IP. After the connection has been made, packets can flow between the hosts without further checking. Circuit-level gateways hide information about the private network, but they do not filter individual packets.

A firewall can be set up in several different physical configurations. For example, in Chapter 6, “Network Design Elements,” we discussed implementing a DMZ. This could be done in a back-to-back configuration (two firewalls surrounding the DMZ), as shown in Figure 8-2, or as a 3-leg perimeter configuration.

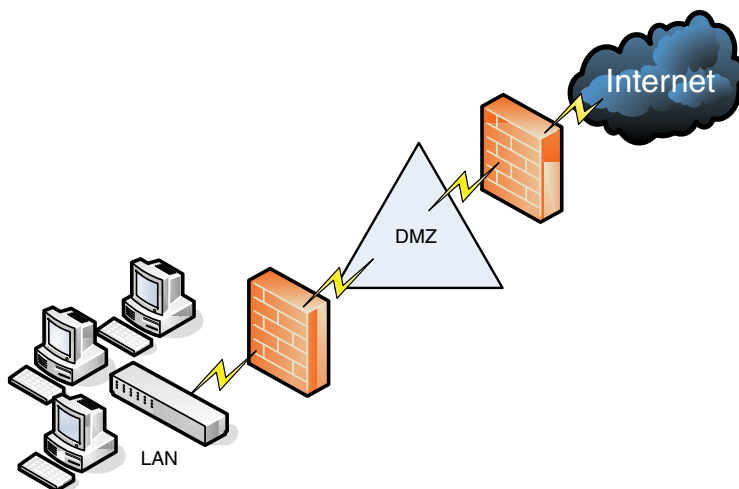
**Key
Topic**

Figure 8-2 Back-to-Back Firewall/DMZ Configuration

Generally, there will be one firewall with the network and all devices and computers residing “behind” it. By the way, if a device is “behind” the firewall, it is also considered to be “after” the firewall, and if the device is “in front of” the firewall, it is also known as being “before” the firewall. Think of the firewall as the drawbridge of a castle. When you are trying to gain admittance to the castle, the drawbridge will probably be closed. You would be in front of the drawbridge, and the people inside the castle would be behind the drawbridge. This is a basic analogy but should help you to understand the whole “in front of” and “behind” business as it relates to data attempting to enter the network and devices that reside on your network.

Logging is also important when it comes to a firewall. Firewall logs should be the first thing you check when an intrusion has been detected. You should know how to access the logs and how to read them. For example, Figure 8-3 shows two screen captures: The first displays the Internet sessions on a basic SOHO router/firewall, and the second shows log events such as blocked packets. Look at the blocked Gnutella packet that is pointed out. I know it is a Gnutella packet because the inbound port on my firewall that the external computer is trying to connect to shows as port 6346; this associates with Gnutella. Gnutella is an older P2P file-sharing network. None of the computers on this particular network use or are in any way connected to the Gnutella service. These external computers are just random clients of the Gnutella P2P network trying to connect to anyone possible.

DIR-655	SETUP	ADVANCED	TOOLS	STATUS
DEVICE INFO	INTERNET SESSIONS			
LOGS	This page displays the full details of active internet sessions to your router.			
STATISTICS				
INTERNET SESSIONS				
WIRELESS				
WISH SESSIONS				
	Local	NAT	Internet	Protocol State Dir Priority Time Out
	216.164.145.27:39533	216.164.145.27:39533	208.59.247.45:53	UDP - Out 128 27
	10.254.254.205:64278	216.164.145.27:64278	74.125.162.95:80	TCP EST Out 176 7794
	10.254.254.205:49405	216.164.145.27:49405	208.59.247.45:53	UDP - Out 128 23
	10.254.254.205:64277	216.164.145.27:64277	72.14.204.100:80	TCP EST Out 133 7793
	10.254.254.205:52885	216.164.145.27:52885	208.59.247.45:53	UDP - Out 128 23
	10.254.254.205:64276	216.164.145.27:64276	65.54.51.27:443	TCP LA Out 128 233
	10.254.254.205:64275	216.164.145.27:64275	65.54.51.27:443	TCP LA Out 128 233
	10.254.254.117:37560	216.164.145.27:37560	204.176.49.2:80	TCP LA Out 128 220
	10.254.254.205:64221	216.164.145.27:64221	216.97.236.245:80	TCP TW Out 128 128
	10.254.254.205:64220	216.164.145.27:64220	216.97.236.245:80	TCP LA Out 128 128
	10.254.254.205:64213	216.164.145.27:64213	216.97.236.245:80	TCP TW Out 128 118
	10.254.254.205:64212	216.164.145.27:64212	216.97.236.245:80	TCP CL Out 182 128
	10.254.254.205:64211	216.164.145.27:64211	216.97.236.245:80	TCP LA Out 128 117
	10.254.254.205:64207	216.164.145.27:64207	216.97.236.245:80	TCP TW Out 128 116
	10.254.254.205:64206	216.164.145.27:64206	216.97.236.245:80	TCP LA Out 128 116
	10.254.254.205:64205	216.164.145.27:64205	216.97.236.245:80	TCP TW Out 128 116
	10.254.254.205:64204	216.164.145.27:64204	216.97.236.245:80	TCP LA Out 128 116
	10.254.254.205:64203	216.164.145.27:64203	216.97.236.245:80	TCP LA Out 128 115
	10.254.254.205:64202	216.164.145.27:64202	216.97.236.245:80	TCP LA Out 128 115

DIR-655	SETUP	ADVANCED	TOOLS	STATUS
DEVICE INFO	LOGS			
LOGS	Use this option to view the router logs. You can define what types of events you want to view and the event levels to view. This router also has internal syslog server support so you can send the log files to a computer on your network that is running a syslog utility.			
STATISTICS				
INTERNET SESSIONS				
WIRELESS	LOG OPTIONS			
WISH SESSIONS	What to View : <input checked="" type="checkbox"/> Firewall & Security <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> Router Status View Levels : <input checked="" type="checkbox"/> Critical <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Informational <input type="button" value="Apply Log Settings Now"/>			
	LOG DETAILS			
	<input type="button" value="Refresh"/> <input type="button" value="Clear"/> <input type="button" value="Email Now"/> <input type="button" value="Save Log"/>			
	1999 Log Entries:			
	Priority	Time	Message	
	[INFO]	Fri Apr 30 12:41:04 2010	Blocked incoming TCP connection request from 24.253.3.20:4770 to 216.164.145.27:6346	
	[INFO]	Fri Apr 30 12:41:01 2010	Above message repeated 1 times	
	[INFO]	Fri Apr 30 12:41:01 2010	Blocked incoming TCP packet from 24.253.3.20:4361 to 216.164.145.27:6346 as RST received but there is no active connection	
	[INFO]	Fri Apr 30 12:40:44 2010	Blocked incoming UDP packet from 24.253.3.20:46376 to 216.164.145.27:6346	
	[INFO]	Fri Apr 30 12:39:05 2010	Blocked incoming TCP connection request from 24.253.3.20:4689 to 216.164.145.27:6346	

Blocked Gnutella packet

Figure 8-3 SOHO Router/Firewall Internet Sessions

It's good that these packets have been blocked, but maybe you don't want the IP address shown (24.253.3.20) to have any capability to connect to your network at all. To eliminate that IP, you could add it to an inbound filter or to an ACL.

So far, we have discussed host-based firewalls (in Chapter 3) and, just now, network-based firewalls. However, both of these firewalls can also fall into the category of **application firewall**. If either type runs protocols that operate on the application layer of the OSI model, then it can be classified as an application firewall. That means that it can control the traffic associated with specific applications. This is

something a stateful network firewall cannot do, as this function operates at the application layer of the OSI model. Many host-based firewalls fall into this category, but when it comes to network-based firewalls, it varies. A basic SOHO router with built-in firewalling capabilities would usually not fall into the application firewall category. However, more advanced network appliances from companies such as Barracuda, Citrix, Fortinet, and Smoothwall do fall into this category. This means that they allow for more in-depth monitoring of the network by controlling the input, output, and access to applications and services all the way up through the application layer of the OSI model. These appliances might also be referred to as *network-based application layer firewalls*. Now that's a mouthful—just be ready for multiple terms used by companies and technicians.

Going a step further, some of the aforementioned network appliances have tools that are designed to specifically protect HTTP sessions from XSS attacks and SQL injection. These types of tools are known as **web application firewalls**. WAFs can help to protect the servers in your environment.

NOTE A firewall appliance needs more than one network adapter so that it can connect to more than one network; this is known as a *multihomed connection*. It might be dual-homed (two adapters), or perhaps it has more, maybe three network adapters, in case you want to implement a DMZ or another perimeter security technique.

Firewalls are often considered to be all-in-one devices, but actually they provide specific functionality as discussed in this section. Still, it is common to hear people refer to a firewall when they are really talking about another technology, or even another device. For example, many SOHO users have an all-in-one multifunction network device. This device has four ports for wired connections, plus a wireless antenna; it connects all the computers to the Internet, and finally has a firewall built-in. Because some users consider this to be simply a firewall, you should teach them about the benefits of disabling SSID broadcasting, and enabling MAC filtering. By disabling Service Set Identifier (SSID) broadcasting, the average user cannot connect wirelessly to the device. An attacker knows how to bypass this, but it is an important element of security that you should implement after all trusted computers have been connected wirelessly. MAC filtering denies access to any computer that does not have one of the MAC addresses you list, another powerful tool that we will cover more in Chapter 9, “Securing Network Media and Devices.”

To make matters a bit more confusing, a firewall can also act as, or in combination with, a proxy server, which we discuss in the following section.

Proxy Servers

A **proxy server** acts as an intermediary for clients, usually located on a LAN, and the servers that they want to access, usually located on the Internet. By definition, *proxy* means go-between, or mediator, acting as such a mediator in between a private network and a public network. The proxy server evaluates requests from clients and, if they meet certain criteria, forwards them to the appropriate server. There are several types of proxies, including a couple you should know for the exam:

Key Topic

- **IP proxy:** Secures a network by keeping machines behind it anonymous; it does this through the use of NAT. For example, a basic four-port router can act as an IP proxy for the clients on the LAN it protects. An IP proxy can be the victim of many of the network attacks mentioned in Chapter 6, especially DoS attacks. Regardless of whether the IP proxy is an appliance or a computer, it should be updated regularly, and its log files should be monitored periodically and audited according to organization policies.
- **Caching proxy:** Attempts to serve client requests without actually contacting the remote server. Although there are FTP and SMTP proxies, among others, the most common caching proxy is the **HTTP proxy**, also known as a **web proxy**, which caches web pages from servers on the Internet for a set amount of time. Examples of caching proxies include WinGate (for Windows systems) and Squid (commonly used on Linux-based systems). An example of a caching proxy is illustrated in Figure 8-4. For example, let's say a co-worker of yours (Client A) accessed www.google.com, and that she was the first person to do so on the network. This client request will go through the HTTP proxy and be redirected to Google's web server. As the data for Google's home page comes in, the HTTP proxy will store or cache that information. When another person on your network (Client B) makes a subsequent request for www.google.com, the bulk of that information will come from the HTTP proxy instead of from Google's web server. This is done to save bandwidth on the company's Internet connection and to increase the speed at which client requests are carried out. Most HTTP proxies check websites to verify that nothing has changed since the last request. Because information changes quickly on the Internet, a time limit of 24 hours is common for storing cached information before it is deleted. Web browsers make use of a **proxy auto-configuration (PAC)** file, which defines how the browser can automatically choose a proxy server. The file itself and the embedded JavaScript function pose a security risk in that the file can be exploited and modified, ultimately redirecting the user to unwanted (and potentially malicious) websites. Consider disabling PAC files and auto-configuration in general within client web browsers.

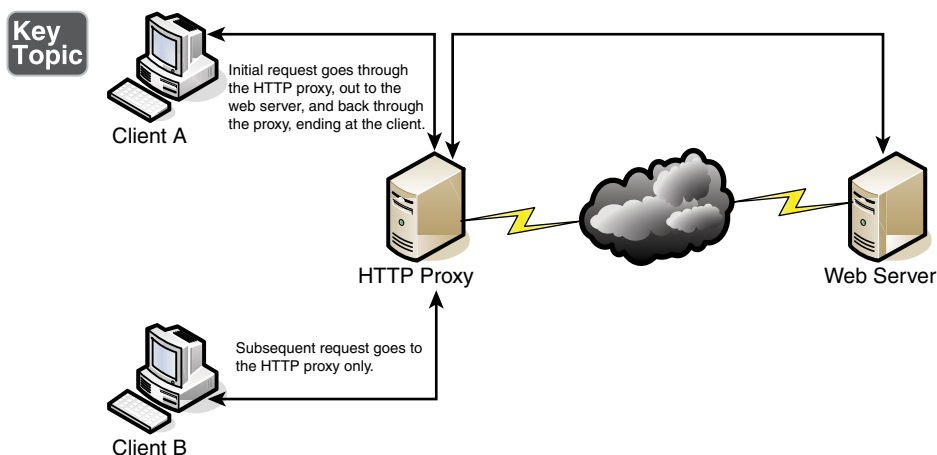


Figure 8-4 Illustration of an HTTP Proxy in Action

Other types of proxies are available to apply policies, block undesirable websites, audit employee usage, and scan for malware. One device or computer might do all these things or just one or two. It depends on the software used or appliance installed. Reverse proxies can also be implemented to protect a DMZ server's identity or to provide authentication and other secure tasks. This is done when users on the Internet are accessing server resources on your network. Generally, a proxy server has more than one network adapter so that it can connect to the various networks it is acting as a mediator for. Each of the network adapters in a proxy should be periodically monitored for improper traffic and for possible network attacks and other vulnerabilities. A proxy server might be the same device as a firewall, or it could be separate. Because of this, a multitude of network configurations are possible. Proxy servers, especially HTTP proxies, can be used maliciously to record traffic sent through them; because most of the traffic is sent in unencrypted form, this could be a security risk. A possible mitigation for this is to chain multiple proxies together in an attempt to confuse any onlookers and potential attackers.

Most often, a proxy server is implemented as a *forward proxy*. This means that clients looking for websites, or files via an FTP connection, pass their requests through to the proxy. However, there is also a *reverse proxy*, where *multiple* HTTP or FTP servers use a proxy server and send out content to one or more clients. These HTTP and FTP servers could be located in a server farm or similar grouping, and the reverse proxy might also undertake the role of load balancer in this situation. A reverse proxy can act as another layer of defense for an organization's FTP or HTTP servers. An *application proxy* might be used as a reverse proxy; for example, Microsoft's Web Application Proxy, which enables remote users to connect to the organization's internal network to access multiple servers. These are often multipurpose by design, allowing for HTTP, FTP, e-mail, and other types of data

connections. However, it could be that you have a single application stored on several servers. Those servers can work together utilizing clustering technology. The clustering might be controlled by the servers themselves or, more commonly, a load balancer can be installed in front of the servers that distributes the network load among them. That load balancer in effect acts as a reverse proxy.

Regardless of the type of proxy used, it will often modify the requests of the “client computer,” whatever that client is, providing for a level of anonymity. But in some cases, you might need a proxy that does not modify requests. This is known as a *transparent proxy*. While it allows for increased efficiency, there is less protection for the client system.

Another example of a proxy in action is Internet content filtering. An **Internet content filter**, or simply a content filter, is usually applied as software at the application layer and can filter out various types of Internet activities such as websites accessed, e-mail, instant messaging, and more. It often functions as a content inspection device, and disallows access to inappropriate web material (estimated to be a big percentage of the Internet!) or websites that take up far too much of an organization’s Internet bandwidth. Internet content filters can be installed on individual clients, but by far the more efficient implementation is as an individual proxy that acts as a mediator between all the clients and the Internet. These proxy versions of content filters secure the network in two ways: one, by forbidding access to potentially malicious websites, and two, by blocking access to objectionable material that employees might feel is offensive. It can also act as a URL filter; even if employees inadvertently type an incorrect URL, they can rest assured that any objectionable material will not show up on their display.

Internet filtering appliances analyze just about all the data that comes through them, including Internet content, URLs, HTML tags, metadata, and security certificates such as the kind you would automatically receive when going to a secure site that starts with https. (However, revoked certificates and certificate revocation lists, or CRLs, will not be filtered because they are only published periodically. More on certificates and CRLs is provided in Chapter 15, “PKI and Encryption Protocols.”) Some of these appliances are even capable of malware inspection. Another similar appliance is the web security gateway. **Web security gateways** (such as Forcepoint, previously known as Websense) act as go-between devices that scan for viruses, filter content, and act as data loss prevention (DLP) devices. This type of content inspection/content filtering is accomplished by actively monitoring the users’ data streams in search of malicious code, bad behavior, or confidential data that should not be leaked outside the network.

As you can see, many, many options for security devices are available for your network, and many vendors offer them. Based on price, you can purchase all kinds of devices, from ones that do an individual task, to ones that are combinations of

everything we spoke about so far, which are also known as *all-in-one security appliances* or unified threat management (UTM) devices (discussed in the upcoming “NIDS Versus NIPS” section).

NOTE Proxies, content filters, and web security gateways are examples of servers that probably face the Internet directly. These “Internet-facing servers” require security controls before they are installed. The two most important security controls are to keep the application up to date, and to review and apply vendor-provided hardening documentation. Remember to do these things before putting the proxy server (or other Internet-facing servers) in a live environment.

Honeypots and Honeynets

Honeypots and honeynets attract and trap potential attackers to counteract any attempts at unauthorized access of the network. This isolates the potential attacker in a monitored area and contains dummy resources that look to be of value to the perpetrator. While an attacker is trapped in one of these, their methods can be studied and analyzed, and the results of those analyses can be applied to the general security of the functional network.

A **honeypot** is generally a single computer but could also be a file, group of files, or an area of unused IP address space, whereas a **honeynet** is one or more computers, servers, or an area of a network; a honeynet is used when a single honeypot is not sufficient. Either way, the individual computer, or group of servers, will *usually* not house any important company information. Various analysis tools are implemented to study the attacker; these tools, along with a centralized group of honeypots (or a honeynet), are known collectively as a honeyfarm.

One example of a honeypot in action is the spam honeypot. Spam e-mail is one of the worst banes known to a network administrator; a spam honeypot can lure spammers in, enabling the network administrators to study the spammers’ techniques and habits, thus allowing the network admins to better protect their actual e-mail servers, SMTP relays, SMTP proxies, and so on, over the long term. It might ultimately keep the spammers away from the real e-mail addresses, because the spammers are occupied elsewhere. Some of the information gained by studying spammers is often shared with other network admins or organizations’ websites dedicated to reducing spam. A spam honeypot could be as simple as a single e-mail address or as complex as an entire e-mail domain with multiple SMTP servers.

Of course, as with any technology that studies attackers, honeypots also bear risks to the legitimate network. The honeypot or honeynet should be carefully firewalled off from the legitimate network to ensure that the attacker can’t break through.

Often, honeypots and honeynets are used as part of a more complex solution known as a network intrusion detection system, discussed following a short review of data loss prevention.

Data Loss Prevention (DLP)

We mentioned DLP in Chapter 3. Let's discuss it briefly now as it relates to networks. **Data loss prevention (DLP)** systems are designed to protect data by way of content inspection. They are meant to stop the leakage of confidential data, often concentrating on communications. As such, they are also referred to as data leak prevention (DLP) devices, information leak prevention (ILP) devices, and extrusion prevention systems. Regardless, they are intended to be used to keep data from leaking past a computer system or network and into unwanted hands.

In network-based DLP, systems deal with data in motion and are usually located on the perimeter of the network. If data is classified in an organization's policy as confidential and not to be read by outsiders, the DLP system detects it and prevents it from leaving the network. Network-based DLP systems can be hardware-based or software-based. An example of a network-based DLP system would be one that detects and prevents the transfer of confidential e-mail information outside the network. Organizations such as Check Point offer DLP solutions, and there are some free open source applications as well. Going further, there are cloud-based DLP solutions available. But it all depends on where you store your data. If you store some or all of your data on the cloud, or if you have a large bring your own device (BYOD) or choose your own device (CYOD) population, then cloud-based DLP becomes an important part of your security strategy. Because the data—and the security of that data—is now external from the company, planning becomes even more vital. Some key elements of the security mindset include: 1) planning for the mitigation of security risks; 2) adequate understanding of the cloud-based provider, where and how data is stored, and their service-level agreement (SLA); 3) in-depth analysis of code and the types of data that will be stored in the cloud; and 4) strong authentication, auditing, and logging. If all this is planned for and implemented properly, it can build the organization's confidence in the cloud, which can lead to a smoother transition, and ultimately reduce risk. However, all this becomes a bigger conversation: We'll talk more about general mindsets when dealing with cloud-based companies in Chapter 16, "Redundancy and Disaster Recovery," and Chapter 18, "Policies and Procedures."

As for DLP, the monitoring of possible leaked information could become a privacy concern. Before implementing a system of this nature, it is important to review your organization's privacy policies. Leaks can still occur due to poor implementation of DLP systems, so it is essential to plan what type of DLP solution your organization needs, exactly how it will be installed, and how it will be monitored.

NIDS Versus NIPS

It's not a battle royale, but you should be able to differentiate between a network intrusion *detection* system (NIDS) and a network intrusion *prevention* system (NIPS) for the exam. Previously, in Chapter 4, "OS Hardening and Virtualization," we discussed host-based intrusion detection systems (or HIDSs). Although a great many attacks can hamper an individual computer, just as many network attacks could possibly take down a server, switch, router, or even an entire network. Network-based IDSs were developed to detect these malicious network attacks, and network-based IPSs were developed in an attempt to prevent them.

NIDS

A **network intrusion detection system (NIDS)** by definition is a type of IDS that attempts to detect malicious network activities, for example, port scans and DoS attacks, by constantly monitoring network traffic. It can also be instrumental in rogue machine detection, including rogue desktops, laptops, and mobile devices, as well as rogue access points, DHCP servers, and network sniffers. Examples of NIDS solutions include open-source products such as Snort (<https://www.snort.org/>), Bro (<https://www.bro.org/>), and many other commercial hardware and software-based products. A NIDS should be situated at the entrance or gateway to your network. It is not a firewall but should be used with a firewall. Because the NIDS inspects every packet that traverses your network, it needs to be fast; basically, the slower the NIDS, the slower the network. So, the solution itself, the computer/device it is installed on, and the network connections of that computer/device all need to be planned out accordingly to ensure that the NIDS does not cause network performance degradation.

Figure 8-5 illustrates how a NIDS might be implemented on a network. Often it is placed in front of a firewall. The NIDS detects attacks and anomalies and alerts the administrator if they occur, whereas the firewall does its best to prevent those attacks from entering the network. However, a NIDS could be placed behind the firewall, or you might have multiple NIDS points strategically placed around the network. If the NIDS is placed in front of the firewall, it generates a lot more administrator alerts, but these can usually be whittled down within the firmware or software of the device running the NIDS. Regardless of where the NIDS is located, a network administrator should monitor traffic from time to time; to do so, the computer, server, or appliance that has the NIDS installed should have a network adapter configured to work in **promiscuous mode**. This passes all traffic to the CPU, not just the frames addressed to it.

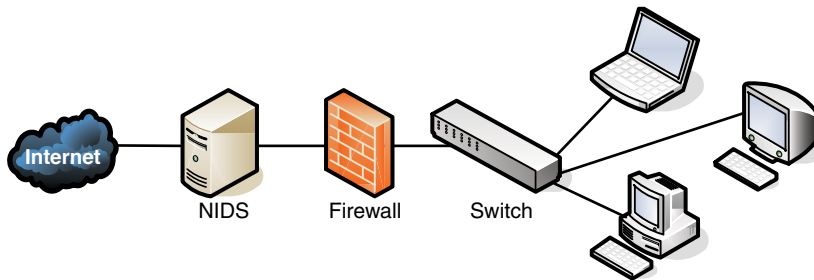
**Key
Topic**

Figure 8-5 Illustration of NIDS Placement in a Network

The beauty of a NIDS is that you might get away with one or two NIDS points on the network, and do away with some or all the HIDS installed on individual computers, effectively lowering the bottom line while still doing a decent job of mitigating risk. A couple of disadvantages of a NIDS, aside from possible network performance issues, are that it might not be able to read encrypted packets of information and will not detect problems that occur on an individual computer. Therefore, to secure a network and its hosts, many organizations implement a mixture of NIDS and HIDS. If a NIDS is placed in front of the firewall, it is subject to attack; therefore, it should be monitored and updated regularly. Some NIDS solutions will auto-update. Finally, the biggest disadvantage of a NIDS is that it is passive, meaning it only *detects* attacks; to protect against, or *prevent*, these attacks, you need something active, you need a NIPS.

NIPS

A **network intrusion prevention system (NIPS)** is designed to inspect traffic and, based on its configuration or security policy, either remove, detain, or redirect malicious traffic that it becomes aware of. The NIPS (as well as the NIDS) is considered to be an *application-aware device*, meaning it can divine different types of packets, define what application they are based on, and ultimately permit or disallow that traffic on the network. More and more companies are offering NIPS solutions in addition to, or instead of, NIDS solutions. Examples of NIPS solutions include Check Point security appliances (<https://www.checkpoint.com>), and the aforementioned Snort, which is actually a NIDS/NIPS software package that should be installed on a dual-homed or multihomed server. Not only can a NIPS go above and beyond a NIDS by removing or redirecting malicious traffic, it can also redirect a recognized attacker to a single computer known as a padded cell, which contains no information of value and has no way out.

Like a NIDS, a NIPS should sit inline on the network, often in front of the firewall, although it could be placed elsewhere, depending on the network segment it protects and the network architecture. Whereas many NIPS solutions have two

connections only and are known as perimeter solutions, other NIPS appliances have up to 16 ports enabling many points of detection on the network—these would be known as network “core” devices. Regardless of the solution you select, as packets pass through the device, they are inspected for possible attacks. These devices need to be accurate and updated often (hopefully automatically) to avoid the misidentification of legitimate traffic, or worse, the misidentification of attacks. If the NIPS blocks legitimate traffic, it would be known as a **false positive**, and effectively could deny service to legitimate customers, creating a self-inflicted denial-of-service of sorts.

If the IPS does not have a particular attack’s signature in its database, and lets that attack through thinking it is legitimate traffic, it is known as a **false negative**, also bad for obvious reasons! Many IPS systems can monitor for attack signatures and anomalies. More information on signatures can be found in Chapter 4 and Chapter 13, “Monitoring and Auditing.” Another type of error that can occur with NIDS and NIPS is a subversion error; this is when the NIDS/NIPS has been altered by an attacker to allow for false negatives, ultimately leading to attacks creeping into the network. This can be deadly because the NIDS/NIPS often is the first point of resistance in the network. To protect against this, some devices have the capability to hide or mask their IP address. They might also come with an internal firewall. It is also important to select an IPS solution that has a secure channel for the management console interface.

One advantage of newer NIPS solutions is that some of them can act as protocol analyzers by reading encrypted traffic and stopping encrypted attacks. In general, the beauty of a NIPS compared to a host-based IPS (HIPS) is that it can protect non-computer-based network devices such as switches, routers, and firewalls. However, the NIPS is considered a single point of failure because it sits inline on the network. Due to this, some organizations opt to install a bypass switch, which also enables the NIPS to be taken offline when maintenance needs to be done.

A vital NIPS consideration is whether to implement a fail-close or fail-open policy—in essence, deciding what will happen if the NIPS fails. Fail-close means that all data transfer is stopped, while fail-open means that data transfer (including potential attacks) are passed through. Let’s consider an example. Say that the NIPS was protecting an individual server (or router), and had a certain level of control over that system. Now let’s say that the NIPS failed. In a fail-close scenario, it would disconnect the system that it is protecting, stopping all data transfer. This is unacceptable to some organizations that require near 100 percent uptime. These organizations are willing to accept additional risk, and therefore are more receptive to a fail-open scenario. However, in this case, if the NIPS fails, it continues to pass all traffic to the “protected” system, which could include possible attacks. Sometimes, fail-open scenarios are necessary. In these cases, defense in depth is the

best strategy. For instance, you might opt to have a firewall filter the bulk of traffic coming into the network, but have the IPS filter only specific traffic, reducing the chances of IPS failure. This layered approach can offer greater security with less chance of attacks passing through, but often comes with increased cost and administration.

Summary of NIDS Versus NIPS

Table 8-1 summarizes NIDS versus NIPS.

Key Topic

Table 8-1 Summary of NIDS Versus NIPS

Type of System	Summary	Disadvantage/Advantage	Example
NIDS	Detects malicious network activities	Pro: Only a limited number of NIDSs are necessary on a network. Con: Only detects malicious activities.	Snort Bro IDS
NIPS	Detects, removes, detains, and redirects traffic	Pro: Detects and mitigates malicious activity. Pro: Can act as a protocol analyzer. Con: Uses more resources. Con: Possibility of false positives and false negatives.	Check Point Systems solutions

The Protocol Analyzer's Role in NIDS and NIPS

You might be familiar already with protocol analyzers such as Wireshark (previously Ethereal) or Network Monitor. These are loaded on a computer and are controlled by the user in a GUI environment; they capture packets, enabling the user to analyze them and view their contents. However, some NIDS/NIPS solutions are considered to be full protocol analyzers with no user intervention required. The protocol analyzer is built into the NIDS/NIPS appliance. It decodes application layer protocols, such as HTTP, FTP, or SMTP, and forwards the results to the IDS or IPS analysis engine. Then the analysis engine studies the information for anomalous or behavioral exploits. This type of analysis can block many exploits based on a single signature. This is superior to basic signature pattern recognition (without protocol analysis), because with signature-based IDS/IPS solutions, many signatures have to be constantly downloaded and stored in the device's database, and they don't enable dynamic understanding of new attacks. However, as with any powerful analysis, like protocol analysis, a premium is placed on processing power, and the price of these types of IDS/IPS solutions will undoubtedly be higher.

NOTE There are also wireless versions of IDS: WIDS and WIPS. They monitor the radio spectrum for unauthorized access and rogue access points. However, these names might be incorporated into the concept of NIDS and NIPS by some organizations. Regardless, be sure to use an IDS (or IPS) for your wired and wireless connections!

Unified Threat Management

A relatively newer concept, **unified threat management (UTM)** is the culmination of everything we discussed in this chapter so far. As early as the year 2000, it was realized that the firewall was no longer enough to protect an organization's network. Other devices and technologies such as NIDS/NIPS systems, content filters, anti-malware gateways, data leak prevention, and virtual private networks were added to the network in order to better protect it. However, with all these extra devices and technologies come added cost and more administration. And so, UTM providers simplify the whole situation by offering all-in-one devices that combine the various levels of defense into one solution. The all-in-one device might also be referred to as a next-generation firewall (NGFW). Companies such as Cisco, Fortinet, and Sophos (to name a few) offer UTM and NGFW solutions; often this is a single device that sits last on the network before the Internet connection. They usually come with a straightforward web-based GUI, which is good news for the beleaguered security administrator who might be burning the midnight oil researching the latest attacks and prevention methods. There's a caveat to all this, and it is a common theme in network security: a single point of defense is a single point of failure. Get past the UTM, and your job as an attacker is done. Secondary and backup UTM devices, as well as server-based HIDSs, strike a balance and create a certain level of defense in depth, while still retaining a level of simplicity. Another consideration is that UTMs should be quick. If they are to take the place of several other devices, then their data processing and traffic flow requirements will be steep. The smart network administrator/security administrator will consider a device that exceeds their current needs and then some.

It was important to discuss each of the tools and technologies separately in this chapter so that you understand how to work with each. But keep in mind that many of these technologies are consolidated into a single solution, a trend that will likely continue as we move forward.

Chapter Summary

Well, it goes without saying that there are many potential attackers who would “storm the castle.” The question presents itself: Have you performed your due diligence in securing your computer networking kingdom?

If you answered yes, then it most likely means you have implemented some kind of unified threat management solution; one that includes a firewall, content filter, anti-malware technology, IDS/IPS, and possibly other network security technologies. This collaborative effort makes for a strong network perimeter. The firewall is at the frontlines, whether it is part of a UTM or running as a separate device. Its importance can’t be stressed enough, and you can’t just implement a firewall; it has to be configured properly with your organization’s policies in mind. ACLs, stateful packet inspection, and network address translation should be employed to solidify your firewall solution.

If you answered no, then prepare ye for more metaphorical expression. Remember that enemy forces are everywhere. They are lying in wait just outside your network, and they can even reside within your network—for example, the malicious insider, that dragon who has usurped the mountain and is perhaps in control of your precious treasure...your data. Analogies aside, this is all clear and present danger—it is *real*, and should be enough to convince you to take strong measures to protect your network.

Often, the act of securing the network can also provide increased efficiency and productivity. For example, a proxy server can act to filter content, and can provide anonymity, but also saves time and bandwidth for commonly accessed data. A honeypot can trap an attacker, thus securing the network, but the secondary result is that network bandwidth is not gobbled up by the powerful attacker. However, the same act can have the opposite effect. For example, a NIDS that is installed to detect anomalies in packets can slow down the network if it is not a powerful enough model. For increased efficiency (and lower all-around cost), consider an all-in-one device such as a UTM, which includes functionality such as firewalling, IDS/IPS, AV, VPN, and DLP. Just make sure it has the core processing and memory required to keep up with the amount of data that will flow through your network.

If you can find the right balance of security and performance while employing your network security solution, it will be analogous to your network donning the aegis, acting as a powerful shield against network attacks from within and without.

Chapter Review Activities

Use the features in this section to study and review the topics in this chapter.

Review Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 8-2 lists a reference of these key topics and the page number on which each is found.



Table 8-2 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
Figure 8-1	Diagram of a basic firewall	257
Bulleted list	Types of firewalls	258
Figure 8-2	Back-to-back firewall/DMZ configuration	260
Bulleted list	Types of proxies	263
Figure 8-4	Illustration of an HTTP proxy in action	264
Figure 8-5	Illustration of NIDS placement in a network	269
Table 8-1	Summary of NIDS versus NIPS	271

Define Key Terms

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

network perimeter, access control list, explicit allow, explicit deny, implicit deny, packet filtering, stateful packet inspection, application-level gateway, circuit-level gateway, application firewall, web application firewall, proxy server, IP proxy, HTTP proxy (web proxy), proxy auto-configuration (PAC), Internet content filter, web security gateway, honeypot, honeynet, data loss prevention (DLP), network intrusion detection system (NIDS), promiscuous mode, network intrusion prevention system (NIPS), false positive, false negative, unified threat management (UTM)

Complete the Real-World Scenarios

Complete the Real-World Scenarios found on the companion website (www.pearsonitcertification.com/title/9780789758996). You will find a PDF containing the scenario and questions, and also supporting videos and simulations.

Review Questions

Answer the following review questions. Check your answers with the correct answers that follow.

1. Which tool would you use if you want to view the contents of a packet?
 - A. TDR
 - B. Port scanner
 - C. Protocol analyzer
 - D. Loopback adapter
2. The honeypot concept is enticing to administrators because
 - A. It enables them to observe attacks.
 - B. It traps an attacker in a network.
 - C. It bounces attacks back at the attacker.
 - D. It traps a person physically between two locked doors.
3. James has detected an intrusion in his company network. What should he check first?
 - A. DNS logs
 - B. Firewall logs
 - C. The Event Viewer
 - D. Performance logs
4. Which of the following devices should you employ to protect your network? (Select the best answer.)
 - A. Protocol analyzer
 - B. Firewall
 - C. DMZ
 - D. Proxy server
5. Which device's log file will show access control lists and who was allowed access and who wasn't?
 - A. Firewall
 - B. Smartphone
 - C. Performance Monitor
 - D. IP proxy

6. Where are software firewalls usually located?
 - A. On routers
 - B. On servers
 - C. On clients
 - D. On every computer
7. Where is the optimal place to have a proxy server?
 - A. In between two private networks
 - B. In between a private network and a public network
 - C. In between two public networks
 - D. On all of the servers
8. A coworker has installed an SMTP server on the company firewall. What security principle does this violate?
 - A. Chain of custody
 - B. Use of a device as it was intended
 - C. Man trap
 - D. Use of multifunction network devices
9. You are working on a server and are busy implementing a network intrusion detection system on the network. You need to monitor the network traffic from the server. What mode should you configure the network adapter to work in?
 - A. Half-duplex mode
 - B. Full-duplex mode
 - C. Auto-configuration mode
 - D. Promiscuous mode
10. Which of the following displays a single public IP address to the Internet while hiding a group of internal private IP addresses?
 - A. HTTP proxy
 - B. Protocol analyzer
 - C. IP proxy
 - D. SMTP proxy
 - E. PAC

- 11.** If your ISP blocks objectionable material, what device would you guess has been implemented?

 - A.** Proxy server
 - B.** Firewall
 - C.** Internet content filter
 - D.** NIDS
- 12.** Of the following, which is a collection of servers that was set up to attract attackers?

 - A.** DMZ
 - B.** Honeypot
 - C.** Honeynet
 - D.** VLAN
- 13.** Which of the following will detect malicious packets and discard them?

 - A.** Proxy server
 - B.** NIDS
 - C.** NIPS
 - D.** PAT
- 14.** Which of the following will an Internet filtering appliance analyze? (Select the three best answers.)

 - A.** Content
 - B.** Certificates
 - C.** Certificate revocation lists
 - D.** URLs
- 15.** Which of the following devices would detect but not react to suspicious behavior on the network? (Select the most accurate answer.)

 - A.** NIPS
 - B.** Firewall
 - C.** NIDS
 - D.** HIDS
 - E.** UTM

- 16.** One of the programmers in your organization complains that he can no longer transfer files to the FTP server. You check the network firewall and see that the proper FTP ports are open. What should you check next?
- A.** ACLs
 - B.** NIDS
 - C.** AV definitions
 - D.** FTP permissions
- 17.** Which of the following is likely to be the last rule contained within the ACLs of a firewall?
- A.** Time of day restrictions
 - B.** Explicit allow
 - C.** IP allow any
 - D.** Implicit deny
- 18.** Which of the following best describes an IPS?
- A.** A system that identifies attacks
 - B.** A system that stops attacks in progress
 - C.** A system that is designed to attract and trap attackers
 - D.** A system that logs attacks for later analysis
- 19.** What is a device doing when it actively monitors data streams for malicious code?
- A.** Content inspection
 - B.** URL filtering
 - C.** Load balancing
 - D.** NAT
- 20.** Allowing or denying traffic based on ports, protocols, addresses, or direction of data is an example of what?
- A.** Port security
 - B.** Content inspection
 - C.** Firewall rules
 - D.** Honeynet

- 21.** Which of the following should a security administrator implement to limit web-based traffic that is based on the country of origin? (Select the three best answers.)
- A.** AV software
 - B.** Proxy server
 - C.** Spam filter
 - D.** Load balancer
 - E.** Firewall
 - F.** URL filter
 - G.** NIDS
- 22.** You have implemented a technology that enables you to review logs from computers located on the Internet. The information gathered is used to find out about new malware attacks. What have you implemented?
- A.** Honeynet
 - B.** Protocol analyzer
 - C.** Firewall
 - D.** Proxy
- 23.** Which of the following is a layer 7 device used to prevent specific types of HTML tags from passing through to the client computer?
- A.** Router
 - B.** Firewall
 - C.** Content filter
 - D.** NIDS
- 24.** Your boss has asked you to implement a solution that will monitor users and limit their access to external websites. Which of the following is the best solution?
- A.** NIDS
 - B.** Proxy server
 - C.** Block all traffic on port 80
 - D.** Honeypot

25. Which of the following firewall rules only denies DNS zone transfers?

- A.** deny IP any any
- B.** deny TCP any any port 53
- C.** deny UDP any any port 53
- D.** deny all dns packets

Answers and Explanations

- 1. C.** A protocol analyzer has the capability to “drill” down through a packet and show the contents of that packet as they correspond to the OSI model. A TDR is a time-domain reflectometer, a tool used to locate faults in cabling. (I threw that one in for fun. It is a Network+ level concept, so you security people should know it!) A port scanner identifies open network ports on a computer or device; we’ll discuss that more in Chapters 12 and 13. A loopback adapter is a device that can test a switch port or network adapter (depending on how it is used).
- 2. A.** By creating a honeypot, the administrator can monitor attacks without sustaining damage to a server or other computer. Don’t confuse this with a honeynet (answer B), which is meant to attract and trap malicious attackers in an entirely false network. Answer C is not something that an administrator would normally do, and answer D is defining a man trap.
- 3. B.** If there was an intrusion, James should check the firewall logs first. DNS logs in the Event Viewer and the performance logs will most likely not show intrusions to the company network. The best place to look first is the firewall logs.
- 4. B.** Install a firewall to protect the network. Protocol analyzers do not help to protect a network but are valuable as vulnerability assessment and monitoring tools. Although a DMZ and a proxy server could possibly help to protect a portion of the network to a certain extent, the best answer is firewall.
- 5. A.** A firewall contains one or more access control lists (ACLs) defining who is enabled to access the network. The firewall can also show attempts at access and whether they succeeded or failed. A smartphone might list who called or e-mailed, but as of the writing of this book does not use ACLs. Performance Monitor analyzes the performance of a computer, and an IP proxy deals with network address translation, hiding many private IP addresses behind one public address. Although the function of an IP proxy is often built into a firewall, the best answer would be firewall.

6. **C.** Software-based firewalls, such as Windows Firewall, are normally running on the client computers. Although a software-based firewall could also be run on a server, it is not as common. Also, a SOHO router might have a built-in firewall, but not all routers have firewalls.
7. **B.** Proxy servers should normally be between the private network and the public network. This way they can act as a go-between for all the computers located on the private network. This applies especially to IP proxy servers but might also include HTTP proxy servers.
8. **B.** SMTP servers should not be installed on a company firewall. This is not the intention of a firewall device. The SMTP server should most likely be installed within a DMZ.
9. **D.** To monitor the implementation of NIDS on the network, you should configure the network adapter to work in promiscuous mode; this forces the network adapter to pass all the traffic it receives to the processor, not just the frames that were addressed to that particular network adapter. The other three answers have to do with duplexing—whether the network adapter can send and receive simultaneously.
10. **C.** An IP proxy displays a single public IP address to the Internet while hiding a group of internal private IP addresses. It sends data back and forth between the IP addresses by using network address translation (NAT). This functionality is usually built into SOHO routers and is one of the main functions of those routers. HTTP proxies store commonly accessed Internet information. Protocol analyzers enable the capture and viewing of network data. SMTP proxies act as a go-between for e-mail. PAC stands for proxy auto-config, a file built into web browsers that allows the browser to automatically connect to a proxy server.
11. **C.** An Internet content filter, usually implemented as content-control software, can block objectionable material before it ever gets to the user. This is common in schools, government agencies, and many companies.
12. **C.** A honeynet is a collection of servers set up to attract attackers. A honeypot is usually one computer or one server that has the same purpose. A DMZ is the demilitarized zone that is in between the LAN and the Internet. A VLAN is a virtual LAN.
13. **C.** A NIPS, or network intrusion prevention system, detects and discards malicious packets. A NIDS only detects them and alerts the administrator. A proxy server acts as a go-between for clients sending data to systems on the Internet. PAT is port-based address translation.

- 14. A, B, and D.** Internet filtering appliances will analyze content, certificates, and URLs. However, certificate revocation lists will most likely not be analyzed. Remember that CRLs are published only periodically.
- 15. C.** A NIDS, or network intrusion detection system, will detect suspicious behavior but most likely will not react to it. To prevent it and react to it, you would want a NIPS. Firewalls block certain types of traffic but by default do not check for suspicious behavior. HIDS is the host-based version of an IDS; it checks only the local computer, not the network. A UTM is an all-inclusive security product that will probably include an IDS or IPS—but you don't know which, so you can't assume that a UTM will function in the same manner as a NIDS.
- 16. A.** Access control lists can stop specific network traffic (such as FTP transfers) even if the appropriate ports are open. A NIDS will detect traffic and report on it but not prevent it. Antivirus definitions have no bearing on this scenario. If the programmer was able to connect to the FTP server, the password should not be an issue. FTP permissions might be an issue, but since you are working in the firewall, you should check the ACL first; then later you can check on the FTP permissions, passwords, and so on.
- 17. D.** Implicit deny (block all) is often the last rule in a firewall; it is added automatically by the firewall, not by the user. Any rules that allow traffic will be before the implicit deny/block all on the list. Time of day restrictions will probably be stored elsewhere but otherwise would be before the implicit deny as well.
- 18. B.** An IPS (intrusion prevention system) is a system that prevents or stops attacks in progress. A system that only identifies attacks would be an IDS. A system designed to attract and trap attackers would be a honeypot. A system that logs attacks would also be an IDS or one of several other devices or servers.
- 19. A.** A device that is actively monitoring data streams for malicious code is inspecting the content. URL filtering is the inspection of the URL only (for example, <https://www.comptia.org>). Load balancing is the act of dividing up workload between multiple computers; we'll discuss that more in Chapter 16, "Redundancy and Disaster Recovery." NAT is network address translation, which is often accomplished by a firewall or IP proxy.
- 20. C.** Firewall rules (ACLs) are generated to allow or deny traffic. They can be based on ports, protocols, IP addresses, or which way the data is headed. Port security deals more with switches and the restriction of MAC addresses that

are allowed to access particular physical ports. Content inspection is the filtering of web content, checking for inappropriate or malicious material. A honeynet is a group of computers or other systems designed to attract and trap an attacker.

21. **B, E, and F.** The security administrator should implement a proxy server, a firewall, and/or a URL filter. These can all act as tools to reduce or limit the amount of traffic based on a specific country. AV software checks for, and quarantines, malware. Spam filters will reduce the amount of spam that an e-mail address or entire e-mail server receives. A load balancer spreads out the network load to various switches, routers, and servers. A NIDS is used to detect anomalies in network traffic.
22. **A.** A honeynet has been employed. This is a group of computers on the Internet, or on a DMZ (and sometimes on the LAN), that is used to trap attackers and analyze their attack methods, whether they are network attacks or malware attempts. A protocol analyzer captures packets on a specific computer in order to analyze them but doesn't capture logs per se. A firewall is used to block network attacks but not malware. A proxy is used to cache websites and act as a filter for clients.
23. **C.** A content filter is an application layer (layer 7) device that is used to prevent undesired HTML tags, URLs, certificates, and so on, from passing through to the client computers. A router is used to connect IP networks. A firewall blocks network attacks. A NIDS is used to detect anomalous traffic.
24. **B.** You should implement a proxy server. This can limit access to specific websites, and monitor who goes to which websites. Also, it can often filter various HTML and website content. A NIDS is used to report potentially unwanted data traffic that is found on the network. Blocking all traffic on port 80 is something you would accomplish at a firewall, but that would stop all users from accessing any websites that use inbound port 80 (the great majority of them!). A honeypot is a group of computers used to lure attackers in and trap them for later analysis.
25. **B.** The firewall rule listed that only denies DNS zone transfers is `deny TCP any any port 53`. As mentioned in Chapter 7, "Networking Protocols and Threats," DNS uses port 53, and DNS zone transfers specifically use TCP. This rule will apply to any computer's IP address initiating zone transfers on the inbound and outbound sides. If you configured the rule for UDP, other desired DNS functionality would be lost. Denying IP in general would have additional unwanted results. When creating a firewall rule (or ACL), you need to be very specific so that you do not filter out desired traffic.



Index

Numbers

- 3-leg perimeter DMZ (Demilitarized Zones), 183
- 3DES (Data Encryption Standard), 486, 489
- 10 tape rotation backup scheme, 565
- 802.1X, 344
 - authentication procedure, 331
 - connection components, 331
 - EAP, 330-332

A

AAA (Accounting, Authentication, Authorization)

- accounting, 6, 221
- authentication, 5-7, 327
 - captive portals*, 337
 - CHAP*, 338-339, 345
 - cloud security*, 195
 - context-aware authentication*, 328
 - deauthentication attacks*. See *Wi-Fi, disassociation attacks*
 - definition*, 321
 - Diameter port associations*, 221
 - EAP*, 330-332
 - extranets*, 185
 - HMAC*, 499
 - identification*, 321
 - inherence factors*, 322
 - intranets*, 185
 - Kerberos*, 220, 334-336, 344

- knowledge factors*, 322
- LDAP*, 333, 344
- LEAP*, 332
- localized authentication*, 329-337, 344
- MFA*, 327
- MS-CHAP*, 338
- multifactor authentication*, 337, 589
- mutual authentication*, 334
- networks*, 72
- nonces*, 235
- PAM*, *Kerberos*, 336
- PEAP*, 330-332
- physical security*, 321
- possession factors*, 322
- RADIUS*, 221, 343-345
- reduced sign-ons*, 328
- remote authentication*, 337-345
- Remote Desktop Services*, 336-337
- servers*, 72, 331
- SSO*, 328-329
- TACACS+*, 220, 343-345
- web of trust*, 529

authorization, 5

- biometric readers*, 326-327, 345
- definition*, 321
- Diameter port associations*, 221
- FIM*, 328
- fingerprint readers/scanners*, 326
- RADIUS port associations*, 221

ABAC (Attribute-Based Access Control), 365-366

accepting

- cookies, 136
- risk, 398

access (unauthorized), 6**access control**

- ABAC, 365-366
- ACL, permissions, 371
- Administrator accounts, 378
- Bell-LaPadula, 364
- Biba, 364
- CAPTCHA, 383
- centralized access control, 366
- Clark-Wilson, 364
- Ctrl+Alt+Del at logon, 379
- DAC, 361-365
- DACL, 372
- decentralized access control, 366
- files/folders
 - copying*, 376
 - moving*, 376
- groups, 371
- guest accounts, 378
- implicit deny, 366
- job rotation, 368
- least privilege, 367
- MAC, 366
 - data labeling*, 363
 - lattice-based access control*, 364
 - rule-based access control*, 364
- mobile devices, 75
- passwords, 376-378
- permissions
 - ACL*, 371
 - DACL*, 372
 - inheritance*, 374-375
 - Linux file permissions*, 373
 - NTFS permissions*, 372, 376
 - privilege creep*, 374
 - propagating*, 375

SACL, 372

user access recertification, 374

policies

Account Lockout Threshold Policy, 382

Default Domain Policy, 379

passwords, 379-383

RBAC, 364-366

SACL, 372

separation of duties, 368

UAC, 383-384

users, 369

access recertification, 374

Account Expiration dates, 370

ADUC, 369

multiple user accounts, 371

passwords, 376-377

time-of-day restrictions, 370

usernames, 376-377

Account Expiration dates, 370**Account Lockout Threshold Policy, 382****accounting**

AAA, 6

Diameter, port associations with, 221

RADIUS, port associations with, 221

ACK packets

SYN floods, 227

TCP/IP hijacking, 232

ACL (Access Control Lists)

DACL, 372

firewall rules, 258

permissions, 371

routers, 179

SACL, 372

active interception, malware delivery, 28**active reconnaissance (security analysis), 403****ActiveX controls, 137****acts (legislative policies), 616-617****ad blocking, browser security, 135**

- ad filtering, 58**
- ad hoc networks, WAP, 299-300**
- adapters (network)**
 - multiple network adapters, 559
 - redundancy planning, 558-559
- adaptive frequency hopping, 306**
- add-ons**
 - ActiveX controls, 137
 - malicious add-ons, 138
 - managing, 138
- addresses (email), preventing/**
troubleshooting spam, 40
- administration**
 - account passwords, 378
 - centrally administered management systems, 92
 - CVE, 200-201
 - guest accounts, passwords, 378
 - HIDS, 57
 - offboarding, 76
 - onboarding, 76
 - removable media controls, 63
 - rootkits, 24
 - Alureon rootkits, 26*
 - definition of, 26*
 - Evil Maid Attack, 26*
 - preventing/troubleshooting, 41*
 - security plans, 7
- administration interface (WAP), 295-296**
- ADUC (Active Directory Users and Computers), 369**
- adware, 23**
- AES (Advanced Encryption Standard), 64, 298, 482, 487-489**
- agents, SNMP, 444**
- aggregation switches, 177**
- agile model (SDLC), 146**
- agreements, copies of (DRP), 570**
- AH (Authentication Headers), IPsec, 534**
- air gaps, 600-601**
- aisles (HVAC), facilities security, 597**
- ALE (Annualized Loss Expectancy), quantitative risk assessment, 400-401**
- alerts, performance baselining, 440**
- ALG (Application-Level Gateways), 259**
- algorithms**
 - 3DES, 486, 489
 - AES, 482, 487-489
 - asymmetric algorithms, 483
 - Diffie-Hellman key exchange, 491*
 - RSA, 490*
 - Blowfish, 489
 - CBC, 482
 - ciphers, 480
 - DEA, 486
 - defining, 480
 - DES, 486, 489
 - ECC, 492-493
 - ECDHE, 492
 - genetic algorithms, 496
 - HMAC, 499
 - IDEA, 486
 - MD5, 498
 - password hashing
 - birthday attacks, 503*
 - key stretching, 504*
 - LANMAN hashing, 500-501*
 - NTLM hashing, 501-502*
 - NTLMv2 hashing, 502*
 - pass the hash attacks, 502-503*
- RC**
 - RC4, 488-489*
 - RC5, 489*
 - RC6, 489*
- RIPEMD, 499**
- RSA, 490**
- SHA, 498-499**
- symmetric algorithms, 481-482**

- 3DES*, 486
- AES*, 487-489
- Blowfish*, 489
- DEA*, 486
- DES*, 486, 489
- IDEA*, 486
- RC*, 488-489
- Threefish*, 489
- Twofish*, 489
- Threefish, 489
- Twofish, 489
- all-in-one security appliances**, 266
- altered host files**, 237, 241
- alternative controls**. *See* **compensating controls**
- Alureon rootkits**, 24-26
- always-on VPN (Virtual Private Network)**, 342
- analytical monitoring tools**
 - Computer Management, 445
 - keyloggers, 447
 - net file command, 446
 - netstat command, 446
 - openfiles command, 445
 - static and dynamic analytical tools, 447
- analyzing**
 - data, incident response procedures, 631
 - passwords, 417-420
 - protocols, 415
 - risk, IT security frameworks, 635
 - security, active/passive reconnaissance, 402-403
- Angry IP Scanner**, 414
- anomaly-based monitoring**, 436-437
- ANT sensors (HVAC)**, facilities security, 598
- anti-malware**
 - software, 8
 - updates, 108
- anti-spyware**, 35-37
- antivirus software**
 - preventing/troubleshooting
 - Trojans*, 35
 - viruses*, 31, 34
 - worms*, 35
 - Safe Mode, 34
- anycast IPv6 addresses**, 181
- AP (Access Points)**
 - Bluetooth AP, 306
 - evil twins, 297
 - isolating, WAP, 303
 - Rogue AP, 296
 - WAP, wireless network security
 - ad hoc networks*, 299-300
 - administration interface*, 295-296
 - AP isolation*, 303
 - brute-force attacks*, 299, 305
 - encryption*, 297-299, 303
 - evil twins*, 297
 - firewalls*, 302
 - MAC filtering*, 302
 - placement of*, 300
 - PSK*, 298
 - rogue AP*, 296
 - SSID*, 296
 - VPN*, 300
 - wireless point-to-multipoint layouts*, 301
 - WLAN controllers*, 303
 - WPS*, 299
 - WLAN AP, 306
- Apache servers**, 201
- application-aware devices**, 269
- Application layer (OSI model)**, 174
- applications (apps)**
 - arbitrary code execution, 155
 - back office applications, securing, 143
 - backdoor attacks, 22, 29, 153, 159
 - backdoors, 288-289

- backward compatibility, 91
- blacklisting, 73, 92
- buffer overflows, 153, 159
- code injections, 156-159
- containerization, 112
- directory traversals, 158-159
- DLL injections, 158
- encryption, 71, 78
- Excel, securing, 143
- firewalls, 261
- geotagging, 74
- HTTPS connection, 71-72
- immutable systems, 146
- input validation, 150-151
- integer overflows, 154
- key management, 72
- LDAP injections, 157
- logs, 452
- memory leaks, 154
- MMS attacks, 73
- mobile apps, security, 143
- network authentication, 72
- NoSQL injections, 157
- null pointer dereferences, 154
- OS hardening, 90-92
- Outlook, securing, 143
- patch management, 142
- privilege escalation, 287-288
- programming
 - ASLR*, 155
 - authenticity*, 148
 - CIA triad*, 146
 - code checking*, 148
 - code signing*, 148
 - DevOps*, 146-148
 - error-handling*, 148
 - integrity*, 148
 - minimizing attack surface area*, 147
 - obfuscation*, 148
 - passwords*, 147
 - patches*, 148
 - permissions*, 147
 - principle of defense in depth*, 147
 - principle of least privilege*, 147
 - quality assurance policies*, 147
 - SDLC*, 145-148
 - secure code review*, 146
 - secure coding concepts*, 144
 - testing methods*, 149-152
 - threat modeling*, 147
 - trusting user input*, 147
 - vulnerabilities/attacks*, 153-159
- proxies, 264
- RCE, 155, 159
- removing, 90-91
- security
 - back office applications*, 143
 - DevOps*, 146-148
 - encryption*, 71, 78
 - Excel*, 143
 - firewalls*, 261
 - mobile apps*, 143
 - network authentication*, 72
 - Outlook*, 143
 - patch management*, 142
 - policy implementation*, 140
 - SDLC*, 145-148
 - secure coding concepts*, 144
 - server authentication*, 72
 - UAC*, 140
 - Word*, 143
- server authentication, 72
- service ports, 219
- SMS attacks, 73
- SQL injections, 156
- transitive trust, 72
- uninstalling, preventing/troubleshooting
 - spyware, 36

- unnecessary applications, removing, 90-91
- user input, 147
- whitelisting, 73, 92
- Word, securing, 143
- XML injections, 157
- XSRF, 156, 159
- XSS, 156, 159
- zero day attacks, 158-159

APT (Advanced Persistent Threats), 11, 22

arbitrary code execution, 155

archive.org, 202

armored viruses, 21

ARO (Annualized Rate of Occurrence),
quantitative risk assessment, 400-401

ARP poisoning, 238, 241

ARP spoofing, 177

ASLR (Address Space Layout
Randomization), 155

assessing

- impact, 399

- risk

- definition, 397-398*

- impact assessment, 399*

- qualitative risk management, 399, 402*

- qualitative risk mitigation, 400*

- quantitative risk management, 400-402*

- residual risk, 398*

- risk acceptance, 398*

- risk avoidance, 398*

- risk management, 397-399*

- risk reduction, 398*

- risk registers, 399*

- risk transference, 398*

- security analysis, 402-403*

- security controls, 404-405*

- vulnerabilities, 406, 410

- defining vulnerabilities, 396*

- general vulnerabilities/basic prevention*
methods table, 409-410

- IT security frameworks, 635*

- managing vulnerabilities, 405-410*

- network mapping, 411-412*

- network sniffers, 415-417*

- OVAL, 408-409*

- password analysis, 417-420*

- penetration testing, 407-408*

- vulnerability scanning, 412-414*

asymmetric algorithms, 483

- Diffie-Hellman key exchange, 491

- RSA, 490

attack guards, 227

attack surface, reducing, 94, 147

attack vectors, malware delivery, 26

attacks/vulnerabilities, programming

- arbitrary code execution, 155

- backdoor attacks, 22, 29, 153, 159

- buffer overflows, 153, 159

- code injections, 156-159

- directory traversals, 158-159

- DLL injections, 158

- integer overflows, 154

- LDAP injections, 157

- memory leaks, 154

- NoSQL injections, 157

- null pointer dereferences, 154

- RCE, 155, 159

- SQL injections, 156

- XML injections, 157

- XSRF, 156, 159

- XSS, 156, 159

- zero day attacks, 158-159

attestation, BIOS, 62

auditing

- audit trails, 451

- computer security audits, 448

- files, 448-450

- independent security auditors, 448

logging

- application logs*, 452
- audit trails*, 451
- DFS Replication logs*, 452
- DNS Server logs*, 452
- file maintenance/security*, 455-457
- firewall logs*, 453
- Syslog*, 454-455
- system logs*, 452
- viewing security events*, 450

manual auditing, 448

monitoring and, 434

SIEM, 460

system security settings, 457-460

AUP (Acceptable Use Policies), 618, 622**authentication, 7, 327**

AAA, 5

captive portals, 337

CHAP, 345

- MS-CHAP*, 338

- RAS authentication*, 338-339

cloud security, 195

context-aware authentication, 328

deauthentication attacks. *See* Wi-Fi,
disassociation attacks

definition, 321

Diameter, port associations with, 221

EAP

- EAP-FAST*, 332

- EAP-MD5*, 332

- EAP-TLS*, 332

- EAP-TTLS*, 332

- LEAP*, 332

- PEAP*, 330-332

extranets, 185

HMAC, 499

identification, 321

inherence factors, 322

intranets, 185

Kerberos, 220, 334-336, 344

knowledge factors, 322

LDAP, 333-344

LEAP, 332

localized authentication, 329

- 802.1X*, 330-332, 344

- Kerberos*, 334-336, 344

- LDAP*, 333, 344

- mutual authentication*, 334

- Remote Desktop Services*, 336-337

MFA, 327

MS-CHAP, 338

multifactor authentication, 337, 589

mutual authentication, 334

networks, 72

nonces, 235

PAM, Kerberos, 336

PEAP, 330-332

physical security, 321

possession factors, 322

RADIUS

- port associations with*, 221

- RADIUS federation*, 343-345

reduced sign-ons, 328

remote authentication

- RADIUS*, 343-345

- RAS*, 337-340, 344

- TACACS+*, 343-345

- VPN*, 340-342

Remote Desktop Services, 336-337

servers, 72, 331

SSO, 328-329

TACACS+, 220, 343-345

web of trust, 529

authenticators (802.1X), 331**authenticity, programming security, 148****authorization**

AAA, 5

biometric readers, 326-327, 345

definition, 321

- Diameter, port associations with, 221
- FIM, 328
- fingerprint readers/scanners, 326
- RADIUS, port associations with, 221
- automated monitoring, 435**
- automated systems, war-dialing, 587**
- automatically updating browsers, 128**
- automating cyber-crime. *See* crimeware**
- availability**
 - CIA triad, 5, 146
 - VoIP, 191
- avoiding risk, 398**
- awareness training, 7, 621-622**

B

- back office applications, securing, 143**
- Back Orifice backdoor attacks, 22, 29**
- back-to-back firewall/DMZ configurations, 259**
- back-to-back perimeter networks, 184**
- backdoors**
 - backdoor attacks, 22, 29, 153, 159
 - malware delivery, 29
 - RAT, 29
 - wired network/device security, 288-289
- backups, 8**
 - battery backups, 552
 - data, 557
 - 10 tape rotation backup scheme, 565*
 - differential data backups, 563-565*
 - disaster recovery, 562-566*
 - full data backups, 563*
 - grandfather-father-son backup scheme, 565*
 - incremental data backups, 563-564*
 - snapshot backups, 566*
 - Towers of Hanoi backup scheme, 566*
 - disaster recovery
 - data backups, 562-566*
 - drills/exercises, 570*

- DRP, 569-570*
- fire, 567*
- flood, 568*
- loss of building, 568*
- power loss (long-term), 568*
- theft/malicious attacks, 568*
- generators
 - considerations for selecting, 554*
 - types of, 553*
- hard disks, 107
- redundancy planning
 - backup generators, 553-554*
 - battery backups, 552*
 - data, 555-558*
 - employees, 562*
 - fail-closed, 549*
 - fail-open, 549*
 - failover redundancy, 548*
 - networks, 558-561*
 - power supplies, 549-551*
 - single points of failure, 547-548*
 - standby generators, 553*
 - succession planning, 562*
 - websites, 561*
- unsavable computers, malware, 40
- backward compatibility, 91**
- badware, 37**
- baiting, social engineering attacks, 589-591**
- banner grabbing, 414**
- baselining, 105**
 - alerts, 440
 - baseline reporting, 438
 - Performance Monitor, 439
 - standard loads, 438
 - System Monitor, 440
- battery backups, 552**
- battery-inverter generators, 554**
- BCC (Blind Carbon Copy), preventing/troubleshooting spam, 40**

BCP (Business Continuity Plans), 569
behavior-based monitoring, 436-437
Bell-LaPadula access control model, 364
BER (Basic Encoding Rules) format, certificates, 524
BIA (Business Impact Analysis), BCP, 569
Biba access control model, 364
biometric readers, physical security, 326-327, 345
BIOS (Basic Input/Output System)
 attestation, 62
 boot order, 61
 external ports, disabling, 61
 flashing, 60
 measured boot option, 62
 passwords, 60
 root of trust, 62
 secure boot option, 61
 updates, 108
birthday attacks, 503
bit torrents, malware delivery, 27
BitLocker, disk encryption, 64-65
black book phone number encryption, 477-480
black-box testing, 149
black hats, 9
Blackhole exploit kits, 27
blackhole lists, 230
blackholes, 230
blacklists
 applications, 92
 OS hardening, 92
 preventing/troubleshooting spam, 40
blackouts (power supplies), 550
blind hijacking, 233
block ciphers, 482, 489
blocking cookies, 136
Blowfish, 489
blue hats, 10

Bluetooth
 adaptive frequency hopping, 306
 AP, 306
 bluejacking, 69, 306
 bluesnarfing, 69, 306-307
 frequency hopping, 306
 NFC, 306
boot order, BIOS, 61
boot sector viruses, 20, 34
botnets
 malware delivery, 28
 mobile devices, 68, 77
 ZeroAccess botnet, 28
bots, 22
BPA (Business Partner Agreements), 623-624
bridges, 178
broadcast storms, 441
brownouts (power supplies), 550
browsers
 automatically updating, 128
 choosing, 127-128
 company requirements, 128
 functionality, 129
 HTTP connections, 71
 HTTPS connections, 71-72
 MITB attacks, 233-234, 240
 OS, determining, 128
 PAC files, 263
 pop-up blockers, 53, 57-59
 preventing/troubleshooting spyware, 35
 recommendations, 127-128
 security, 129
 ad-blocking, 135
 add-ons, 137-138
 advanced security settings, 138-139
 content filtering, 133-134
 cookies, 136-137
 LSO, 137

- mobile devices*, 135
- passwords*, 139
- policy implementation*, 129, 131
- pop-up blocking*, 135
- proxy servers*, 133-134
- security zones*, 135
- temporary files*, 138
- updates*, 135
- user training*, 133

- updates, 128, 135
- vulnerabilities/fixes, 128

brute-force attacks

- password cracking, 419
- WAP, 299, 305

buffer overflows, 153, 159**buildings**

- loss of (disaster recovery), 568
- security
 - fire suppression*, 594-596
 - HVAC*, 597-600
 - shielding*, 598-600
 - vehicles*, 600-601

butt sets, wiretapping, 293**BYOD (Bring Your Own Device), mobile device security**, 74-78**C****CA (Certificate Authorities)**

- chain of trust, 528
- CRL, 527
- CSR, 525
- horizontal organization, 528
- key escrow, 528
- key recovery agents, 528
- mapping certificates, 527
- pinning certificates, 526-527
- revoking certificates
 - CRL*, 527
 - OCSP*, 528

- social engineering and, 527
- validating certificates, 525
- verifying certificates with RA, 527
- VeriSign certificates, 72, 525
- web of trust, 529

cable loops, switches, 177**cabling**

- coaxial cabling, 290-292
- data emanation, 292-294
- fiber-optic cabling, 290, 294
- interference
 - crosstalk*, 291-292
 - EMI*, 290
 - RFI*, 291
- PDS, 295
- STP cabling, 292, 599
- twisted-pair cabling, 290
 - crosstalk*, 291-292
 - wiretapping*, 293
- UTP cabling, 292
- wired network/device security, 290-295
- wiretapping, 293-294
- wiring closets, 294

CAC (Common Access Cards). *See* smart cards**caching proxies**, 263-264**Caesar Cipher**, 478**Cain & Abel**, password cracking, 417-418**California SB 1386**, 617**CallManager**, privilege escalation, 288**CAM (Content Addressable Memory)**

- tables, MAC flooding, 176

Camtasia 9, 91**Camtasia Studio 8**, 91**CAN (Controller Area Networks), vehicles and facilities security**, 600**CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)**, 383

captive portals, 337**capturing**

- network traffic, incident response procedures, 631
- packets, 415, 440
- screenshots, incident response procedures, 631
- system images, incident response procedures, 630
- video, incident response procedures, 631

cardkey systems, 324**carrier unlocking, mobile devices, 69****CASB (Cloud Access Security Brokers), 197****CBC (Cipher Block Chaining), 482****CBC-MAC (Cipher Block Chaining Message Authentication Code) protocol, 298****CCI (Co-Channel Interference). *See* cross-talk****CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), 298****CCTV (Closed-Circuit Television), 323****cell phones. *See* mobile devices****cellular networks, 308****centralized access control, 366****centrally administered management systems, 92****CER (Canonical Encoding Rules) format, certificates, 524****CER (Crossover Error Rates), biometric readers, 326****certificates**

- digital certificates
 - CA*, 525
 - chain of trust*, 523, 528
 - CRL*, 527
 - CSR*, 525
 - key escrow*, 528
 - key recovery agents*, 528

mapping, 527*pinning*, 526-527*PKI*, 522-525, 528*revoking*, 527-528*validation*, 525*verifying with RA*, 527*VeriSign certificates*, 72, 525*web of trust*, 529

post-certification process, 655

public key cryptography, 484

chain of custody (evidence collection), 629**change management policies, 619, 622****CHAP (Challenge-Handshake Authentication Protocol), 345**

MS-CHAP, 338

PPTP and, 533

RAS authentication, 338-339

session theft, 232

cheat sheets, exam preparation, 649-650**checkpoints, VM disk files, 114****Christmas Tree attacks, 228****chromatic dispersion, 294****CIA triad, 4**

availability, 5

confidentiality, 5

integrity, 5

secure code review, 146

CIDR (Classless Interdomain Routing), 187**cipher locks, 324****ciphers**

algorithms as, 480

block ciphers, 482, 489

Caesar Cipher, 478

defining, 480

RC

RC4, 488-489*RC5*, 489*RC6*, 489

stream ciphers, 482

one-time pads, 493-494

RC4, 488-489

Vernam ciphers. *See* one-time pads

circuit-level gateways, 259

Cisco routers, 178

Clark-Wilson access control model, 364

clean desk policy, 592

clearing (data removal), 626

clear-text passwords, 443

CLI (Command-Line Interface), closing
open ports, 224

clickjacking, 233

client-side attacks, 236

closets (wiring), 294

cloud computing

community clouds, 194

CSP, 194

definition, 192

DLP systems, 59

hybrid clouds, 194

IaaS, 193

MaaS, 194

P2P networks and, 198

PaaS, 193

private clouds, 194

public clouds, 194

SaaS, 193

SECaaS, 193

security

authentication, 195

CASB, 197

data access security, 196

encryption, 196

passwords, 195

programming standardization, 196

server defense

email servers, 199-200

file servers, 198-199

FTP servers, 202-203

network controllers, 199

web servers, 200-202

services, 197

social media and, 197

XaaS, 194

clusters, 561

cluster tips, 626

data remanence, 626

failover clusters, 560

load-balancing clusters, 560

coaxial cabling, 290-292

code checking, programming security, 148

code injections, 159

DLL injections, 158

LDAP injections, 157

NoSQL injections, 157

SQL injections, 156

XML injections, 157

XSRE, 156

XSS, 156

code signing, programming security, 148

coding

ASLR, 155

authenticity, 148

CIA triad, 146

code checking, 148

code signing, 148

DevOps, 146-148

error-handling, 148

integrity, 148

minimizing attack surface area, 147

obfuscation, 148

passwords, 147

patches, 148

permissions, 147

principle of defense in depth, 147

principle of least privilege, 147

quality assurance policies, 147

SDLC

agile model, 146
principles of, 146-148
V-shaped model, 145
waterfall model, 145

secure code review, 146

secure coding concepts, 144

testing methods

black-box testing, 149
compile-time errors, 150
dynamic code analysis, 152
fuzz testing, 152
gray-box testing, 149
input validation, 150-151
penetration tests, 149
runtime errors, 150
sandboxes, 149
SEH, 150
static code analysis, 151-152
stress testing, 149
white-box testing, 149

threat modeling, 147

trusting user input, 147

vulnerabilities/attacks

arbitrary code execution, 155
backdoor attacks, 22, 29, 153, 159
buffer overflows, 153, 159
code injections, 156-159
directory traversals, 158-159
DLL injections, 158
integer overflows, 154
LDAP injections, 157
memory leaks, 154
NoSQL injections, 157
null pointer dereferences, 154
RCE, 155, 159
SQL injections, 156
XML injections, 157
XSRF, 156, 159

XSS, 156, 159

zero day attacks, 158-159

cold and hot aisles (HVAC), facilities security, 597

cold sites, 561

collecting/preserving evidence (incident response procedures), 629, 632-633

collisions, MD5, 498

command-line scripting, network attacks, 235

community clouds, 194

company policies

data sensitivity

classifying data, 615
DHE, 616
legislative policies, 616-617

equipment recycling/donation policies, ISA, 625

example of, 614-615

personal security policies, 617

AUP, 618, 622
awareness training, 621-622
change management policies, 619, 622
due care policies, 621-623
due diligence, infrastructure security, 621-623
due process policies, 621-623
mandatory vacations, 620-622
offboarding, 620
onboarding, 620, 623
privacy policies, 618
separation of duties/job rotation policies, 619, 622
user education, 621-622

vendor policies, 623

BPA, 623-624
ISA, 624
MoU, 624
SLA, 623-624

compatibility (backward), 91

compensating controls, 405

compile-time errors, 150

compliance

GRC, 617

licensing compliance violations, 632

CompTIA exams

exam preparation checklist, 647-650

grading scale, 647

post-certification process, 655

registration, 650

taking exams, 651-654

Computer Management, 445

computers

maintaining, 108-109

security audits, 448

confidence tricks (cons), social engineering, 588

confidential information, classifying (data sensitivity), 615

confidentiality (CIA triad), 5, 146

configuration baselines, 105

configuring

managing configurations, 102

PAC files, 263

routers, secure configurations, 178

conserving hard disk space, 91

console (WAP). *See* administration interface

consolidating services, 144

contacts, DRP, 569

containerization (applications), 112

containment phase (incident response procedures), 628

content filtering, 58

browsers, 133-134

Internet, 265

routers, 179

context-aware authentication, 328

contingency planning. *See* BCP; ITCP

contracts

BPA, 623-624

ISA, 624

MoU, 624

SLA, 623-624

cookies

accepting/blocking, 136

definition of, 136

Flash cookies. *See* LSO

persistent cookies, 136

privacy alerts, 136

session hijacking, 137

session theft, 232

tracking cookies, 137

XSS, 137

COOP (Continuity of Operations Plan).

See BCP

COPE (Corporate Owned, Personally

Enabled) mobile devices, security, 74

copying files/folders, 376

corrective controls, 405

cracking passwords, 417-420

crashes. *See* system failure

crimeware, 27. *See also* malware

critical systems/data, hierarchical lists of (DRP), 570

critical updates, 98

CRL (Certificate Revocation Lists), 527

cross-site scripting. *See* XSS

crosstalk, cabling, 291-292

cryptanalysis attacks (password cracking method), 419

cryptography. *See also* encryption

asymmetric key algorithms, 483

black book phone number encryption, 477-480

Caesar Cipher, 478

ciphers

algorithms as, 480

block ciphers, 482, 489

- defining*, 480
- stream ciphers*, 482
- defining, 477, 480
- ECC, 492-493
- ECDHE, 492
- hash functions
 - HMAC*, 499
 - MD5*, 498
 - RIPEMD*, 499
 - SHA*, 498-499
- keys
 - defining*, 480-481
 - DEK*, 488
 - Diffie-Hellman key exchange*, 484, 491
 - KEK*, 488
 - key stretching*, 504
 - managing*, 484-485
 - MEK*, 488
 - PKI*, 521-528
 - private key cryptography*, 481
 - public key cryptography*, 481-484
- quantum cryptography, 493
- steganography, defining, 485
- symmetric key algorithms, 481-482
- CryptoLocker**, 23, 26
- cryptoprocessors**. *See* **HSM**
- CSO (Chief Security Officers)**, disaster recovery planning, 570
- CSP (Cloud Service Providers)**, 194
- CSR (Certificate Signing Requests)**, 525
- CSU (Channel Service Units)**, 179
- Ctrl+Alt+Del at login**, 379
- custody, chain of (evidence collection)**, 629
- CVE (Common Vulnerabilities and Exposures)**, 200-201
- cyber-crime, automating**. *See* **crimeware**
- cyber-criminals**, 11
- CYOD (Choose Your Own Device)**, mobile device security, 74

D

- DAC (Discretionary Access Control)**, 361-365
- DACL (Discretionary Access Control Lists)**, 372
- damage/loss control (incident response procedures)**, 630
- Darkleech**, 201
- darknet**, 198
- data access security, cloud security**, 196
- data analysis, incident response procedures**, 631
- data at rest, defining**, 477
- data backups**, 8, 557
 - 10 tape rotation backup scheme, 565
 - differential data backups, 563-565
 - disaster recovery, 562
 - 10 tape rotation backup scheme*, 565
 - differential data backups*, 563-565
 - full data backups*, 563
 - grandfather-father-son backup scheme*, 565
 - incremental data backups*, 563-564
 - snapshot backups*, 566
 - Towers of Hanoi backup scheme*, 566
 - full data backups, 563
 - grandfather-father-son backup scheme, 565
 - incremental data backups, 563-564
 - snapshot backups, 566
 - Towers of Hanoi backup scheme, 566
- data centers, mantraps**, 589
- data disclosure acts**, 616-617
- data emanation**, 292-294
- data encryption**, 8, 476
 - 3DES, 486, 489
 - AES, 482, 487-489
 - asymmetric algorithms, 483
 - Blowfish, 489
 - CBC, 482

ciphers

- algorithms as*, 480
- block ciphers*, 482, 489
- defining*, 480
- stream ciphers*, 482

cryptography

- black book phone number encryption*, 477-480
- Caesar Cipher*, 478
- defining*, 477, 480
- hash functions*, 498-499
- quantum cryptography*, 493

- data at rest, defining, 477

- data in transit, defining, 477

- data in use, defining, 477

- DEA, 486

- defining, 480

- DES, 486, 489

- Diffie-Hellman key exchange, 484, 491-492

- ECB, block ciphers, 482

- ECC, 492-493

- ECDHE, 492

- IDEA, 486

keys

- defining*, 480-481
- DEK*, 488
- Diffie-Hellman key exchange*, 484, 491
- KEK*, 488
- key stretching*, 504
- managing*, 484-485
- MEK*, 488
- PKI*, 521-528
- private key cryptography*, 481
- public key cryptography*, 481-484

- one-time pads, 493-494

password hashing

- birthday attacks*, 503
- key stretching*, 504
- LANMAN hashing*, 500-501
- NTLM hashing*, 501-502

- NTLMv2 hashing*, 502

- pass the hash attacks*, 502-503

- PGP, 494-495

PKI

- CA*, 525-528

- certificates*, 522-524, 528

- defining*, 521

- IPsec*, 534-535

- L2TP*, 534

- PPTP*, 533

- S/MIME*, 530-531

- SSH*, 532-533

- SSL/TLS*, 531-532

- PRNG, 495

RC

- RC4*, 488-489

- RC5*, 489

- RC6*, 489

- RSA, 490

- steganography, defining, 485

- symmetric algorithms, 481-482

- Threefish, 489

- Twofish, 489

- web of trust, 529

- data exfiltration**, 378

- data handling (DHE)**, sensitive data, 616

- data in transit**, defining, 477

- data in use**, defining, 477

- data labeling**, MAC, 363

- Data Link layer (OSI model)**, 174

- data redundancy**, RAID

- RAID 0, 555

- RAID 0+1, 556

- RAID 1, 556-557

- RAID 5, 556-557

- RAID 6, 556-558

- RAID 10, 556

- data remanence**, 8, 626

- data removal**, 8

- clearing, 626
- destroying storage media (physical data removal), 627
- purging, 626
- data sensitivity**
 - classifying data, 615
 - data handling (DHE), 616
 - legislative policies, 616-617
- data storage segmentation, mobile devices, 75**
- data validation. *See* input validation**
- databases (relational)**
 - normalization, 157
 - RDBMS, 156-157
- DDoS (Distributed Denial-of-Service) attacks, 229-230, 240**
- DEA (Data Encryption Algorithm), 486**
- deauthentication attacks (Wi-Fi).**
 - See* disassociation attacks (Wi-Fi)
- decentralized access control, 366**
- default accounts, wired network/device security, 286**
- Default Domain Policy, 379**
- defense in depth, 9, 147**
- defragmenting hard disks, 107**
- DEK (Data Encryption Keys), 488**
- deleting data**
 - clearing, 626
 - destroying storage media (physical data removal), 627
 - purging, 626
- delivery systems (malware)**
 - active interception, 28
 - attack vectors, 26
 - backdoors, 29
 - bit torrents, 27
 - botnets, 28
 - Easter eggs, 30
 - email, 26
 - exploit kits, 27
 - FTP servers, 26
 - instant messaging, 26
 - keyloggers, 27
 - logic bombs, 29
 - media-based delivery, 27
 - memory cards, 27
 - optical discs, 27
 - P2P networks, 27
 - privilege escalation, 29
 - smartphones, 27
 - software, 26
 - threat vectors, 26
 - time bombs, 29
 - typosquatting, 27
 - URL hijacking, 27
 - USB flash drives, 27
 - user error, 27
 - websites, 27
 - zip files, 26
 - zombies, 28
- DER (Distinguished Encoding Rules)**
 - format, certificates, 524
- DES (Data Encryption Standard), 486, 489**
- designing networks**
 - back-to-back perimeter networks, 184
 - bridges, 178
 - cellular networks, 308
 - cloud computing
 - community clouds, 194*
 - CSP, 194*
 - definition, 192*
 - hybrid clouds, 194*
 - IaaS, 193*
 - MaaS, 194*
 - P2P networks and, 198*
 - PaaS, 193*
 - private clouds, 194*
 - public clouds, 194*
 - SaaS, 193*

- SECaaS*, 193
- security*, 195-203
- services*, 197
- social media and*, 197
- XaaS*, 194
- CSU, 179
- DMZ
 - 3-leg perimeter DMZ*, 183
 - back-to-back perimeter networks*, 184
- documenting network design, 309
- DSU, 179
- extranets, 184-185
- firewalls, back-to-back perimeter networks, 184
- Internet, 183
- intranets, 184-185
- IP addresses, ports and, 222
- LAN
 - routers*, 178
 - VLAN*, 188-189
 - WAN versus*, 182
- modems, 190-191
- NAC, 185-186
- NAT
 - firewall effect*, 180
 - IPv4 addresses*, 180-182
 - IPv6 addresses*, 181-182
 - private IPv4 addresses*, 180
 - private IPv6 addresses*, 181-182
 - public IPv4 addresses*, 180
 - static NAT*, 180
- OSI model, 173
 - layers of*, 174
 - TCP/IP model versus*, 175
- PAT, IPv4 addresses, 180
- PBX equipment, 191
- ports
 - application service ports*, 219
 - associated protocols table*, 219-221
 - closing open ports*, 224
 - dynamic ports*, 218
 - FTP servers*, 223
 - inbound ports*, 219
 - IP addresses and*, 222
 - outbound ports*, 219
 - port zero security*, 224
 - private ports*, 218
 - ranges*, 218
 - registered ports*, 218
 - scanning for open ports*, 223
 - TCP*, 217-221
 - TCP reset attacks*, 225
 - UDP*, 217-221
 - unnecessary ports*, 224
 - well-known ports*, 218
- protocols and port associations
 - associated protocols table*, 219-221
 - Diameter*, 221
 - DNS*, 220
 - FCIP*, 221
 - FTP*, 219, 225
 - HTTP*, 220
 - IMAP*, 220
 - iSCSI*, 221
 - Kerberos*, 220
 - L2TP*, 221
 - LDAP*, 221
 - Ms-sql-s*, 221
 - NetBIOS*, 220
 - NNTP*, 220
 - POP3*, 220
 - PPTP*, 221
 - RADIUS*, 221
 - RDP*, 221
 - RPC*, 220
 - RTP*, 222
 - SMB*, 221

- SMTP, 220
- SNMP, 220
- SNMPTRAP, 220
- SSH, 219
- Syslog, 221
- TACACS+, 220
- Telnet, 220
- TFTP, 220
- routers
 - ACL, 179
 - Cisco routers, 178
 - content filtering, 179
 - firewalls, 178
 - IPS, 179
 - secure configurations, 178
 - secure VPN connectivity, 179
 - SOHO routers, 178-179
- SATCOM, 308
- subnetting, 186-187
- switches, 175
 - aggregation switches, 177
 - ARP spoofing, 177
 - DHCP starvation attacks, 177
 - fail-open mode, 176
 - looping, 177
 - MAC flooding, 176, 189
 - MAC spoofing, 176-177
 - physical tampering, 177
 - port security, 176-177
 - STP, 177
- TCP/IP model versus OSI model, 175
- telephony
 - modems, 190-191
 - PBX equipment, 191
 - VoIP, 191
- VLAN, 188-189
- VoIP, 191
- VPN, WAP, 300
- WAN
 - LAN versus, 183
 - routers, 178
- wired network/device security, 285
 - backdoors, 288-289
 - cabling, 290-295
 - default accounts, 286
 - network attacks, 289
 - passwords, 286-287
 - privilege escalation, 287-288
 - remote ports, 289
 - Telnet, 289
- wireless network security
 - Bluetooth, 306-307
 - cellular networks, 308
 - documenting network design, 309
 - geofences, 308
 - GPS, 308
 - NFC, 306-307
 - RFID, 307
 - SATCOM, 308
 - third-party wireless adapter connections, 296
 - VPN, 300
 - WAP, 295-305
 - wireless protocols, 298
 - wireless transmission vulnerabilities, 304-305
- destroying storage media (data removal), 627
- detecting rootkits, 24
- detective controls, 405
- device drivers, updates, 99
- DevOps, 146-148
- DFS (Distributed File System) Replication logs, 452
- DHCP snooping, 177
- DHCP starvation attacks, 177
- DHE (Data-Handling Electronics), sensitive data, 616
- DHTML (Dynamic HTML), hover ads, 59

Diameter, port associations with, 221

dictionary attacks (password cracking method), 419

differential data backups, 563-565

Diffie-Hellman key exchange, 484, 491-492

digital certificates

CA, 525

CRL, 527

CSR, 525

key escrow, 528

key recovery agents, 528

mapping, 527

pinning, 526-527

PKI

BER format, 524

CA, 525

CER format, 524

chain of trust, 523, 528

DER format, 524

dual-sided certificates, 523

DV certificates, 522

EV certificates, 522

multidomain certificates, 523

OV certificates, 522

P12/PFX format, 524

PEM format, 524

SAN field, 523

single-sided certificates, 523

wildcard certificates, 523

X.509 standard, 522

revoking

CRL, 527

OCSP, 528

validation, 525

verifying with RA, 527

VeriSign certificates, 72, 525

web of trust, 529

digital signatures, public key cryptography, 484

directory traversals, 158-159

disabling

default accounts, 286

external ports, 61

guest accounts, 286

hardware, virtualization, 115

LSO, 137

services, 95-97

SSID broadcasting, 262

disassociation attacks (Wi-Fi), 305

disaster recovery

data backups, 562

10 tape rotation backup scheme, 565

differential data backups, 563-565

full data backups, 563

grandfather-father-son backup scheme, 565

incremental data backups, 563-564

snapshot backups, 566

Towers of Hanoi backup scheme, 566

drills/exercises, 570

DRP

agreements, copies of, 570

BCP, 569

contacts, 569

critical systems/data, hierarchical lists of, 570

drills/exercises, 570

impact determination, 569

fire, 567

flood, 568

loss of building, 568

power loss (long-term), 568

theft/malicious attacks, 568

disaster-tolerant disk systems, RAID, 558

disk duplexing, 556

disk encryption

BitLocker, 64-65

FDE, 64

SED, 64

diversion theft, social engineering attacks,
586, 590

DLL injections, 158

DLP (Data Loss Prevention), 59, 267

DMZ (Demilitarized Zones)

- 3-leg perimeter DMZ, 183
- back-to-back configurations, 259
- back-to-back perimeter networks, 184
- firewalls, 259

DNS (Domain Name Servers)

- amplification attacks, 230, 240
- blackholes, 230
- domain name kiting, 238, 241
- logs, 452
- pharming, 237
- poisoning, 236, 241
- port associations with, 220
- sinkholes, 230
- unauthorized zone transfers, 237, 241
- zone transfers, 258

DNSBL (DNS Blackhole Lists), 230

documentation (file network), 309

domain controllers

- IE domain controller-managed policies,
131-132
- KDC, tickets, 334

domains

- Default Domain Policy, 379
- name kiting, 238, 241

donating/recycling equipment policies, 625

door access, physical security

- cardkey systems, 324
- cipher locks, 324
- mantraps, 326
- proximity sensors, 325
- security tokens, 325
- smart cards, 325

DoS (Denial-of-Service) attacks

- flood attacks, 226

Fraggle, 227, 239

ping floods, 226, 239

Smurf attacks, 226, 239

SYN floods, 227, 239

UDP flood attacks, 227

Xmas attacks, 228

fork bombs, 229

permanent DoS attacks, 229

POD, 228, 239

spoofed MAC addresses, 305

teardrop attacks, 229, 239

**dot dot slash attacks. See directory
traversals**

double-tagging attacks, 189

downgrade attacks, 532

drive lock passwords, 61

driver updates, 99

**DRM (Digital Rights Management),
jailbreaking, 288**

drones, facilities security, 601

DRP (Disaster Recovery Plans)

- agreements, copies of, 570
- BCP, 569
- contacts, 569
- critical systems/data, hierarchical lists of,
570
- drills/exercises, 570
- impact determination, 569

DSU (Data Service Units), 179

dual-sided certificates, 523

due care policies, 621-623

**due diligence, infrastructure security,
621-623**

due process policies, 621-623

**dumpster diving, social engineering
attacks, 588-590**

duties

- segregation of, 405
- separation of, 619, 622

DV (Domain Validation) certificates, 522

DyFuCA (Internet Optimizer), 26
 dynamic and static analytical monitoring tools, 447
 dynamic code analysis, 152
 dynamic ports, 218

E

EAP (Extensible Authentication Protocol), 330-332
Easter eggs, malware delivery, 30
eavesdropping, social engineering attacks, 588-590
ECB (Electronic Codebook), block ciphers, 482
ECC (Elliptic Curve Cryptography), 492-493
ECDHE (Elliptic Curve Diffie-Hellman Ephemeral), 492
educating users, 591-593, 621-622
elite hackers, 10
email
 address links, preventing/troubleshooting spam, 40
 BCC, preventing/troubleshooting spam, 40
 blacklists, preventing/troubleshooting spam, 40
 identity theft emails, 26
 lottery scam emails, 26
 malware delivery, 26
 open mail relays, preventing/troubleshooting spam, 39
 S/MIME, 530-531
 spam, 25
 definition of, 26
 preventing/troubleshooting, 41
 spam honeypots, 266
 SSL/TLS, 531-532
 whitelists, preventing/troubleshooting spam, 40

email servers, security, 199-200
emergency response detail (incident response procedures), 629
EMI (Electromagnetic Interference), cabling, 290
EMP (Electromagnetic Pulses), 599
employees
 awareness training, 621-622
 clean desk policy, 592
 educating, 591-593, 621-622
 first responders (incident response procedures), 629
 offboarding, 620
 onboarding, 620, 623
 personal security policies, 617
 AUP, 618, 622
 awareness training, 621-622
 change management policies, 619, 622
 due care policies, 621-623
 due diligence, infrastructure security, 621-623
 due process policies, 621-623
 mandatory vacations, 620-622
 offboarding, 620
 onboarding, 620, 623
 privacy policies, 618
 separation of duties/job rotation policies, 619, 622
 user education, 621-622
 PII, 616-617, 622
 succession planning, 562
 vacations, 620-622
 vetting, 592
emulators, 111
encryption, 8, 476
 3DES, 486, 489
 AES, 64, 487, 482, 489
 applications (apps), 71, 78
 asymmetric key algorithms, 483
 Blowfish, 489

- CBC, 482
- ciphers
 - algorithms as*, 480
 - block ciphers*, 482, 489
 - defining*, 480
 - stream ciphers*, 482
- cloud security, 196
- cryptography
 - black book phone number encryption*, 477-480
 - Caesar Cipher*, 478
 - defining*, 477, 480
 - hash functions*, 498-499
 - quantum cryptography*, 493
- data at rest, defining, 477
- data in transit, defining, 477
- data in use, defining, 477
- DEA, 486
- defining, 480
- DES, 486, 489
- Diffie-Hellman key exchange, 484, 491-492
- ECB, block ciphers, 482
- ECC, 492-493
- ECDHE, 492
- encrypted viruses, 20
- FTP servers, 202
- full device encryption, mobile devices, 70
- hard drives
 - BitLocker*, 64-65
 - FDE*, 64
 - SED*, 64
- IDEA, 486
- keys
 - defining*, 480-481
 - DEK*, 488
 - Diffie-Hellman key exchange*, 484, 491
 - KEK*, 488
 - key stretching*, 504
 - managing*, 484-485
 - MEK*, 488
 - PKI*, 521-528
 - private key cryptography*, 481
 - public key cryptography*, 481-484
- mobile devices, 67
- one-time pads, 493-494
- password hashing, 500
 - birthday attacks*, 503
 - key stretching*, 504
 - LANMAN hashing*, 500-501
 - NTLM hashing*, 501-502
 - NTLMv2 hashing*, 502
 - pass the hash attacks*, 502-503
- PGP, 494-495
- PKI
 - CA*, 525-528
 - certificates*, 522-524, 528-530
 - defining*, 521
 - IPsec*, 534-535
 - L2TP*, 534
 - PPTP*, 533
 - S/MIME*, 531
 - SSH*, 532-533
 - SSL/TLS*, 531-532
- PRNG, 495
- RC
 - RC4*, 488-489
 - RC5*, 489
 - RC6*, 489
- RSA, 490
- steganography, defining, 485
- symmetric key algorithms, 481-482
- Threefish, 489
- Twofish, 489
- USB devices, 63
- viruses, preventing/troubleshooting, 33
- WAP, 297-299, 303
- web of trust, 529
- whole disk encryption, 108

- end-of-chapter questions, exam preparation, 648**
- endpoint DLP systems, 59**
- enumeration, 414**
- ephemeral mode**
 - Diffie-Hellman key exchange, 492
 - ECDHE, 492
- equipment recycling/donation policies, 625**
- eradication phase (incident response procedures), 628**
- ERP (Enterprise Resource Planning), IT security frameworks, 635**
- error-handling**
 - compile-time errors, 150
 - programming security, 148
 - runtime errors, 150
 - SEH, 150
- escrow, certificate keys, 528**
- ESP (Encapsulating Security Payloads), IPsec, 535**
- Ethernet**
 - ARP poisoning, 238, 241
 - FCoE, 221
 - NAS, 63-64
- Ethernet switching. *See* switches**
- ethical hackers, 9**
- EV (Extended Validation) certificates, 522**
- events (security)**
 - audit trails, 451
 - failure to *see* events in security logs, 450
 - incidents versus, 627
 - SIEM, 460
- evidence, collecting/preserving (incident response procedures), 629, 632-633**
- Evil Maid Attacks, 26**
- evil twins, WAP, 297**
- exams**
 - preparing for
 - exam preparation checklist, 647-650*
 - grading scale, 647*

- post-certification process, 655*

- taking exams, 651-654*

- registering for, 650

- Excel (MS), securing, 143

- exception-handling, SEH, 150

- expenses/man hours, tracking (incident response procedures), 632

- explicit allow firewall rule (ACL), 258

- explicit deny firewall rule (ACL), 258

- exploit kits, malware delivery, 27

- exposing sensitive data, 151

- external ports, disabling, 61

- extranets, 184-185

F

- F2F (Friend-to-Friend) networks, 198**

- facilities**

- loss of (disaster recovery), 568

- security

- fire suppression, 594-596*

- HVAC, 597-600*

- shielding, 598-600*

- vehicles, 600-601*

- fail-closed, redundancy planning, 549**

- fail-open, redundancy planning, 549**

- fail-open mode, switches, 176**

- failover clusters, 560**

- failover redundancy, 548**

- failure-resistant disk systems, RAID, 557**

- failure-tolerant disk systems, RAID, 558**

- failures**

- single points of (redundancy planning), 547-548

- system failure, 6

- false acceptances, biometric readers, 326, 345**

- false negatives**

- IDS, 56

- IPS, 270

false positives

IDS, 56

NIPS, 270

false rejection, biometric readers, 326, 345

Faraday cages, 292, 303, 599

fault tolerance, 557**FCIP (Fiber Channel over IP), port associations with, 221****FCoE (Fibre Channel over Ethernet), 221****FDE (Full Disk Encryption), 64****FEXT (Far End Crosstalk), 292****fiber-optic cabling, 290, 294****file servers, security, 198-199****file systems, OS hardening, 105-106****fileless malware, 24****files/folders**

auditing, 448-450

copying, 376

IT folder

*advanced security settings, 459-460**permissions, 458*

log file maintenance/security, 455-457

moving, 376

net file command, analytical monitoring,
446openfiles command, analytical monitoring,
445**filters**

ad filtering, 58

content filters, 58, 179

Internet content filtering, 265

NAT filtering, 259

packet filtering, 258

Spam filters, 38

stateless packet filters, spoofing attacks, 259

web security gateways, 265

**FIM (Federated Identity Management),
328****final network documentation, 309****fingerprint readers/scanners, physical security, 326****fingerprinting, 403****fire**

disaster recovery, 567

suppression

*fire extinguishers, 594-595**special hazard protection systems, 596**sprinkler systems, 595-596***Firefox, secure connections, 525****firewalls**

back-to-back perimeter networks, 184

closing open ports, 224

firewall effect, NAT, 180

flood guards, 227

IPFW, 54

iptables, 54

logs, 453

network perimeter security

*ACL firewall rules, 258**ALG, 259**application firewalls, 261**back-to-back firewall/DMZ configurations,
259**basic implementation diagram, 256**circuit-level gateways, 259**firewall logs, 260**multihomed connections, 262**NAT filtering, 259**packet filtering, 258**SOHO router/firewall Internet sessions,
260**SPI, 258**web application firewalls, 262*

NGFW, 532

personal firewalls, 53

*IPFW, 54**iptables, 54**PF, 54*

SOHO router/firewall configuration, 55

Windows Firewall, 54

ZoneAlarm, 54

PF, 54

routers, 178

SOHO routers, 178

spam firewalls, 38

updates, 108

WAP, 302

Windows Firewall, 31, 54

ZoneAlarm, 54

first responders (incident response procedures), 629

FIT (Failure In Time), quantitative risk assessment, 402

Flash

cookies. *See* LSO

malicious add-ons, 138

pop-up ads, 59

flash drives, encryption, 63

Flash Player Settings Manager, disabling LSO, 137

flashing, BIOS, 60

flood attacks

Fraggle, 227, 239

MAC flooding, 176, 189

ping floods, 226, 239

Smurf attacks, 226, 239

SYN floods, 227, 239

UDP flood attacks, 227

Xmas attacks, 228

flood guards, 227

floods, disaster recovery, 568

Fluke, 417

folders/files

auditing, 448-450

copying, 376

IT folder

advanced security settings, 459-460

permissions, 458

log file maintenance/security, 455-457

moving, 376

net file command, analytical monitoring, 446

openfiles command, analytical monitoring, 445

forensics, incident response procedures

data analysis, 631

licensing reviews, 632

network traffic, 631

OOV, 630-631

screenshots, 631

system images, 630

tracking man hours/expenses, 632

video, 631

witness statements, 631

fork bombs, 229

forward proxies, 264

Fraggle, 227, 239

frequency hopping, 306

FTP (File Transfer Protocol), 225

port associations with, 219

servers

malware delivery, 26

ports and, 223

protocol analysis, 443

security, 202-203

FTPS (FTP Secure), 225

full data backups, 563

full device encryption, mobile devices, 70

fuzz testing, 152

G

gas-engine generators, 553

Gates, Bill, 588

gateways

ALG, 259

circuit-level gateways, 259

web security gateways, 265

generators

- backup generators
 - considerations for selecting, 554*
 - types of, 553*
- battery-inverter generators, 554
- fuel sources, 554
- gas-powered generators, 553
- permanently installed generators, 553
- portable generators, 553
- power output, 554
- standby generators, 553
- starting, 554
- uptime, 554

genetic algorithms, 496**geofences, 308****geotagging, 74, 308****GinMaster Trojan, 67****glass-box testing. *See* white-box testing****GLB (Gramm-Leach-Bliley) act, 617****Gnutella, firewall logs, 260****Google, name change hoax, 588****GPG (GNU Privacy Guard) and PGP, 495****GPMC (Group Policy Management Console), 133****GPS (Global Positioning Systems)**

- geofences, 308
- geotagging, 74, 308
- mobile devices, 70
- wireless network security, 308

GPT rootkits, preventing/troubleshooting, 38**grading scale, CompTIA exams, 647****grandfather-father-son backup scheme, 565****gray-box testing, 149****gray hats, 10****grayware, 23****GRC (Governance, Risk and Compliance), 617****GRE (Generic Routing Encapsulation), 342****Group Policies**

- GPMC, 133
- Import Policy From window (Windows Server), 104
- Local Group Policy Editor, 103
- OS hardening, 102-104

groups, access control, 371**guessing (password cracking method), 418****guest accounts, disabling, 286**

H

hackers. *See also* threat actors

- black hats, 9
- blue hats, 10
- elite hackers, 10
- ethical hackers, 9
- gray hats, 10
- thinking like a hacker, 9
- white hats, 9

Hackers, 361**hacktivists, 11****Hanoi backup scheme, Towers of, 566****happy birthday attacks, 503****hard disks**

- backups, 107
- conserving disk space, 91
- data removal
 - clearing, 626*
 - destroying storage media (physical data removal), 627*
 - purging, 626*
- defragmenting, 107
- drive lock passwords, 61
- encryption
 - BitLocker, 64-65*
 - FDE, 64*

- SED*, 64
- whole disk encryption*, 108
- fault tolerance, 557
- maintaining, 109
- OS hardening, 106-108
- restore points, 107
- hardening OS, 89**
 - applications
 - backward compatibility*, 91
 - blacklisting*, 92
 - removing*, 90-91
 - whitelisting*, 92
 - attack surface, reducing, 94
 - baselining, 105
 - centrally administered management systems, 92
 - configuration management, 102
 - file systems, 105-106
 - Group Policies, 102-104
 - hard disks, 91, 106-108
 - hotfixes, 99-100
 - least functionality, 90
 - Linux, starting/stopping services, 95-97
 - macOS/OS X, starting/stopping services, 96-97
 - messaging, 90
 - patches, 99-102
 - remote control programs, 90
 - Remote Desktop Connection, 90
 - Remote Desktop Services, 93
 - security templates, 103-104
 - services
 - disabling*, 95-97
 - Remote Desktop Services*, 93
 - removing*, 90-91
 - TOS, 97
 - updates, 98-99
 - whitelisting applications, 92

Windows

- Programs and Features window*, 91
- starting/stopping services*, 95-97
- Windows Update*, 98-99
- Windows XP*, 94

hashing

- defining, 496-497
- hash functions
 - cryptographic hash functions*, 498-499
 - defining*, 497
- HMAC, 499
- MD5, 498
- one-way function, 498
- password hashing
 - birthday attacks*, 503
 - key stretching*, 504
 - LANMAN hashing*, 500-501
 - NTLM hashing*, 501-502
 - NTLMv2 hashing*, 502
 - pass the hash attacks*, 502-503
- process of, 497
- RIPEMD, 499
- SHA, 498-499
- system images, incident response procedures, 630

HAVA (Help America Vote Act of 2002), 617

hazard protection systems, 596

headers

- AH, IPsec, 534
- manipulation, 441

heuristic analysis, 437

HIDS (Host-based Intrusion Detection Systems), 53-55

- Trend Micro OSSEC, 56
- Tripwire, 57
- Verisys, 57

hierarchical CA organization, 528
 hierarchical lists of critical systems/data,
 DRP, 570
 high availability, RAID arrays, 63
 high-energy EMP (Electromagnetic
 Pulses), 599
 hijacking sessions, XSS, 137
 HIPAA (Health Insurance Portability and
 Accountability Act), 616
 HIPS (Host Intrusion Prevention Systems),
 270
 HMAC (Hash-based Message
 Authentication Code), 499
 hoaxes, social engineering attacks, 587, 590
 honeynets, 266
 honeypots, 266
 horizontal privilege escalation, 288
 host files, DNS servers, 237, 241
 hosted hypervisors, 112
 HOSTS files, preventing/troubleshooting
 spyware, 37
 hot and cold aisles (HVAC), facilities secu-
 rity, 597
 hot sites, 561
 hotfixes, OS hardening, 99-100
 hover ads (DHTML), 59
 HSM (Hardware Security Modules), 65-66
 HTTP (Hypertext Transfer Protocol)
 connections, 71
 port associations with, 220
 proxies. *See* proxy servers
 response packets, header manipulation, 441
 HTTPS (HTTP Secure), 71-72, 532
 HVAC (Heating, Ventilation, Air
 Conditioning), facilities security, 597
 ANT sensors, 598
 SCADA, 598-600
 shielding, 599
 hybrid clouds, 194
 Hyper-V, 114
 hypervisors, 111-112

I
 IA (Information Assurance). *See* risk,
 assessment; risk, management
 IaaS (Infrastructure as a Service), 193
 ICMP flood attacks. *See* ping floods
 IDEA (International Data Encryption
 Algorithm), 486
 identification
 authentication schemes, 321
 biometric readers, 326-327, 345
 cardkey systems, 324
 definition, 321
 FIM, 328
 fingerprint readers/scanners, 326
 identity proofing, 322
 identity theft emails, 26
 photo ID, 324
 security tokens, 325
 smart cards, 325
 verifying. *See* authentication
 identification phase (incident response pro-
 cedures), 628
 IDF (Intermediate Distribution Frame)
 rooms, wire closets, 294
 IDPS (Intrusion Detection and Prevention
 Systems), 57
 IDS (Intrusion Detection Systems)
 false negatives, 56
 false positives, 56
 HIDS, 53-55
 Trend Micro OSSEC, 56
 Tripwire, 57
 Verisys, 57
 NIDS, 55
 placement within networks, 269
 promiscuous mode, 268
 protocol analyzers, 271
 signature-based detection, 56
 statistical anomaly detection, 56
 WIDS, 272

IE (Internet Explorer)

domain controller-managed policies,
131-132

Internet Explorer Maintenance Security,
130-131

security settings, 130

IF-THEN statements, genetic algorithms, 496**imaging**

OOV, 630-631

systems, 109, 630

**IMAP (Internet Message Access Protocol),
port associations with, 220****immutable systems, 146****impact analysis (business), BCP, 569****impact assessment, 399****impact determination, DRP, 569****implicit deny (access control), 366****implicit deny firewall rule (ACL), 258****Import Policy From window (Windows
Server), 104****in-band management, 444****inbound ports, 219****incident management, 627****incident response procedures**

chain of custody (evidence collection), 629

collecting/preserving evidence, 629, 632-633

containment phase, 628

damage/loss control, 630

emergency response detail, 629

eradication phase, 628

events versus incidents, 627

forensics

data analysis, 631

licensing reviews, 632

network traffic, 631

OOV, 630-631

screenshots, 631

system images, 630

tracking man hours/expenses, 632

video, 631

witness statements, 631

identification phase, 628

initial incident management process, 629

lessons learned phase, 628

need-to-know, 633

preparation phase, 628

recovery phase, 628

incremental data backups, 563-564**information security**

anti-malware, 8, 108

authentication, 7

backups, 8

data removal, 8

defense in depth, 9

encryption, 8

malware, 6

security plans, 7

social engineering, 6

system failure, 6

unauthorized access, 6

user awareness, 7

**infrastructure security, due diligence,
621-623****inherence factors (authentication), 322****inheritance (permissions), 374-375****initial incident management process
(incident response procedures), 629****input validation, 150-151****installing, 36****instant messaging**

malware delivery, 26

OS hardening, 90

spim, 25

integer overflows, 154**integrity (CIA triad), 5, 146-148**

interference

- cabling
 - crosstalk*, 291-292
 - EMI*, 290
 - RFI*, 291
- surveys, 302

internal information, classifying (data sensitivity), 615**Internet**

- content filtering, 265
- messaging, 73
- network design, 183

Internet Explorer

- Internet Optimizer, 23-26
- Maintenance Security, 130-131

Internet protocol suite. *See* TCP/IP**intranets, 184-185****IP addresses**

- ports and, 222
- spoofing attacks, 231

IP proxies, 263**IP spoofing attacks, 179****IPFW (IP Firewall), 54****IPS (Intrusion Prevention Systems), 57**

- false negatives, 270
- HIPS, 270
- NIPS, 268-269
 - false positives*, 270
 - protocol analyzers*, 271
- routers, 179
- WIPS, 272

IPsec (Internet Protocol Security)

- AH, 534
- ESP, 535
- SA, 534
- transport mode, 535
- tunneling mode, 535

iptables, 54**IPv4**

- addresses, 180-182
- firewall effect, 180

IPv6 addresses, 181-182**IronKey, 63****ISA (Interconnection Security Agreements), 624****iSCSI (Internet Small Computer Systems Interface), port associations with, 221****ISP (Internet Service Providers), redundancy planning, 559****ISSO (Information Systems Security Officers), disaster recovery planning, 570****IT folder**

- advanced security settings, 459-460
- permissions, 458

IT security frameworks

- ERP, 635
- reference frameworks, 634
- risk analysis, 635
- vulnerability assessments, 635

ITCP (IT Contingency Planning), 569**IV attacks, 304**

J - K

jailbreaking, 135. *See also* privilege, escalation

- DRM, 288
- mobile devices, 75

jamming surveys, 302**job rotation**

- access control, 368
- separation of duties policies, 619, 622

KDC (Key Distribution Center), tickets, 334**KEK (Key Encryption Keys), 488****Kerberos, 334-336, 344, 482, 502**

- LDAP injections, 199
- Microsoft Security Bulletins, 199

port associations with, 220

vulnerabilities, 199

keyloggers, 27, 447

keys

certificate keys, 528

cryptography

asymmetric key algorithms, 483

defining, 480-481

DEK, 488

Diffie-Hellman key exchange, 484, 491-492

KEK, 488

key stretching, 504

managing, 484-485

MEK, 488

PKI, 521-535

private key cryptography, 481, 490

public key cryptography, 481-484, 490-493

QKD, 493

symmetric algorithms, 481-482

web of trust, 529

managing, 72, 484-485

Knoppix, 35-37

knowledge factors (authentication), 322

L

L2TP (Layer 2 Tunneling Protocol), 534

port associations with, 221

VPN connections, 340-342

LAN (Local Area Networks)

bridges, 178

broadcast storms, 441

routers, 178

split tunneling, 342

VLAN, 188

MAC flooding, 189

VLAN hopping, 189

WAN versus, 182

LANMAN hashing, 500-501

LDAP (Lightweight Directory Access Protocol), 333-344

injections, 157, 199

port associations with, 221

LEAP (Lightweight Extensible Authentication Protocol), 332

least functionality, 90

least privilege

access control, 367

principle of, 147

legislative policies, 616-617

lessons learned phase (incident response procedures), 628

licensing

compliance violations, 632

reviewing, incident response procedures, 632

lineman's handsets. See butt sets

links (email), preventing/troubleshooting spam, 40

Linux

file permissions, 373

netstat command, analytical monitoring, 447

OS hardening, starting/stopping services, 95-97

patch management, 102

SELinux, 57

System Monitor, 440

tcpdump packet analyzer, 443

virus prevention/troubleshooting tools, 35

vulnerability scanning, 414

LM hashes. See LANMAN hashing

load-balancing clusters, 560

Local Group Policy

browser security, 129

LANMAN hashing, 501

Local Group Policy Editor, 103

localized authentication, 329

802.1X, 344

- authentication procedure, 331*
- connection components, 331*
- EAP, 330-332*
- Kerberos, 334-336, 344
- LDAP, 333, 344
- mutual authentication, 334
- Remote Desktop Services, 336-337
- locking systems, vehicles and facilities security, 601**
- lockout programs, mobile devices, 70**
- logic bombs, malware delivery, 29**
- logins**
 - Ctrl+Alt+Del at logon, 379
 - SSO, 328-329
- logs**
 - application logs, 452
 - audit trails, 451
 - DFS Replication logs, 452
 - DNS Server logs, 452
 - file maintenance/security, 455-457
 - firewall logs, 260, 453
 - network traffic logs, incident response procedures, 631
 - non-repudiation, 450
 - security events, failure to *see* events, 450
 - Syslog, 454-455
 - system logs, 452
- long-term power loss, disaster recovery, 568**
- looping switches, 177**
- loss/damage control (incident response procedures), 630**
- loss of building, disaster recovery, 568**
- lottery scam emails, 26**
- Love Bug viruses, 25**
- LSO (Locally Shared Objects), 137**

M

- MaaS (Monitoring as a Service), 194**
- MAC (Mandatory Access Control), 366**

- data labeling, 363
- filtering, WAP, 302
- flooding, 176, 189
- lattice-based access control, 364
- rule-based access control, 364
- spoofing, 176-177, 305
- macOS/OS X**
 - OS hardening, starting/stopping services, 96-97
 - patches, 101-102
- macro viruses, 20**
- maintenance**
 - computers, 108-109
 - hard disks, 109
 - Internet Explorer Maintenance Security, 130-131
- malicious add-ons, 138**
- malicious attacks/theft, disaster recovery, 568**
- malicious insiders, social engineering attacks, 585, 590**
- malvertising, 23**
- malware, 6, 19. *See also* crimeware**
 - adware, 23
 - anti-malware
 - software, 8*
 - updates, 108*
 - APT, 22
 - badware, 37
 - delivery systems
 - active interception, 28*
 - attack vectors, 26*
 - backdoors, 29*
 - bit torrents, 27*
 - botnets, 28*
 - Easter eggs, 30*
 - email, 26*
 - exploit kits, 27*
 - FTP servers, 26*
 - instant messaging, 26*

- keyloggers*, 27
- logic bombs*, 29
- media-based delivery*, 27
- memory cards*, 27
- optical discs*, 27
- P2P networks*, 27
- privilege escalation*, 29
- smartphones*, 27
- software*, 26
- threat vectors*, 26
- time bombs*, 29
- typosquatting*, 27
- URL hijacking*, 27
- USB flash drives*, 27
- user error*, 27
- websites*, 27
- zip files*, 26
- zombies*, 28
- grayware, 23
- malvertising, 23
- mobile devices, 67, 77
- non-malware, 24
- ransomware, 22
 - CryptoLocker*, 23, 26
 - definition of, 26
 - preventing/troubleshooting, 35
- rootkits
 - Alureon rootkits*, 24-26
 - definition of, 26
 - detecting, 24
 - Evil Maid Attacks*, 26
 - preventing/troubleshooting, 38, 41
- spam, 25
 - definition of, 26
 - filters, 38
 - firewalls, 38
 - identity theft emails, 26
 - lottery scam emails, 26
 - preventing/troubleshooting, 38-41
- spim, 25
- spyware, 23-24
 - definition of, 26
 - Internet Optimizer*, 26
 - preventing/troubleshooting, 35-37, 41
 - symptoms of, 36
 - tracking cookies, 137
- Trojans
 - definition of, 25
 - GinMaster Trojan*, 67
 - MITB attacks*, 233-234, 240
 - PlugX Trojans*, 25
 - preventing/troubleshooting, 35, 41
 - RAT*, 22, 29
 - time bombs*, 29
 - ZeroAccess botnet*, 28
- unsavable computers, 40
- viruses
 - armored viruses*, 21
 - boot sector viruses*, 20, 34
 - definition of, 25
 - encrypted viruses*, 20
 - Love Bug virus*, 25
 - macro viruses*, 20
 - metamorphic viruses*, 21
 - multipartite viruses*, 21
 - polymorphic viruses*, 20
 - preventing/troubleshooting, 31-35, 41
 - program viruses*, 20
 - stealth viruses*, 21
 - symptoms of, 33-34
 - virus hoaxes*, 21
- worms
 - definition of, 25
 - Nimda*, 21
 - Nimda worm*, 25
 - preventing/troubleshooting, 35, 41
- man hours/expenses, tracking (incident response procedures), 632**

management controls, 404**managing**

- add-ons, 138
- application patches, 142
- change management policies, 619, 622
- configurations, 102
- group policies, GPMC, 133
- in-band management, 444
- incidents, 627
- keys (cryptography), 484-485
- out-of-band management, 444
- patches, 101-102
- risk, 397-399
- vulnerabilities
 - general vulnerabilities/basic prevention methods table, 409-410*
 - OVAL, 408-409*
 - penetration testing, 407-408*
 - process of, 405-406*

Mandatory Security Policy. See MAC**mandatory vacations, 620-622****mantraps**

- multifactor authentication, 589
- physical security, 326

manual auditing, 448**manual monitoring, 435****many-to-one mapping (certificates), 527****mapping**

- certificates, 527
- networks, 411-412

MBR (Master Boot Records) rootkits, preventing/troubleshooting, 38**MBSA (Microsoft Baseline Security Analyzer), 101****MD5 (Message-Digest algorithm 5), 498****MDF (Main Distribution Frame) rooms, wire closets, 294****MDM (Mobile Device Management), 75****measured boot option, BIOS, 62****media gateways, 191****media-based malware delivery, 27****MEK (Master Encryption Keys), 488****memory**

- ASLR, 155
- buffer overflows, 153, 159
- CAM tables, MAC flooding, 176
- integer overflows, 154
- memory leaks, 154
- null pointer dereferences, 154
- RDBMS, stored procedures, 156-157

memory cards, malware delivery, 27**messaging (instant)**

- malware delivery, 26
- MMS attacks, 73
- OS hardening, 90
- SMS attacks, 73
- spim, 25

metamorphic viruses, 21**MFA (Multifactor Authentication), 327****Microsoft domains, KDC tickets, 334****Microsoft Edge, policy settings, 130****Microsoft Security Bulletins, Kerberos vulnerabilities, 199****minimizing attack surface, 94, 147****mirroring ports, 442****MITB (Man-in-the-Browser) attacks, 233-234, 240****mitigating risk, 400****MITM (Man-in-the-Middle) attacks, 28, 233, 240****mobile apps, security, 143****mobile devices, 66**

- access control, 75
- application security, 78
 - application blacklisting, 73*
 - application whitelisting, 73*
 - geotagging, 74*
 - HTTPS connections, 71-72*

- key management*, 72
 - MMS attacks*, 73
 - server/network authentication*, 72
 - SMS attacks*, 73
 - transitive trust*, 72
- bluejacking, 69
- bluesnarfing, 69
- botnets, 68, 77
- browser security, 135
- BYOD, 74-78
- carrier unlocking, 69
- COPE, 74
- crosstalk, 291
- CYOD, 74
- encryption, 67
- full device encryption, 70
- GPS tracking, 70, 74
- jailbreaking, 75, 135
- lockout programs, 70
- malware, 67, 77
- MDM, 75
- offboarding, 76
- onboarding, 76
- passwords, 67, 71
- rooting, 75, 135
- sanitizing, 70
- screen locks, 71
- sideloading, 75
- SIM cloning, 68, 77
- social engineering attacks, 68
- storage segmentation, 75
- theft of, 70-71, 77
- wireless attacks, 69-70, 77
- modems**
 - network design, 190-191
 - war-dialing, 190
- monitoring**
 - analytical monitoring tools
 - Computer Management*, 445
 - keyloggers*, 447
 - net file command*, 446
 - netstat command*, 446
 - openfiles command*, 445
 - static and dynamic analytical tools*, 447
 - anomaly-based monitoring, 436-437
 - auditing and, 434
 - automated monitoring, 435
 - behavior-based monitoring, 436-437
 - manual monitoring, 435
 - performance baselining
 - alerts*, 440
 - baseline reporting*, 438
 - Performance Monitor*, 439
 - standard loads*, 438
 - System Monitor*, 440
 - protocol analyzers
 - broadcast storms*, 441
 - network adapters*, 440
 - packet capturing*, 440
 - TCP/IP handshakes*, 441
 - Wireshark*, 441-442
 - session monitoring, Computer Management, 445
 - signature-based monitoring, 435-437
 - SNMP, 443-445
- motion detectors, physical security**, 323
- MoU (Memorandums of Understanding)**, 624
- moving files/folders**, 376
- MPLS (Multiprotocol Label Switching)**, 342
- MS-CHAP (Microsoft-Challenge Handshake Authentication Protocol)**, RAS authentication, 338
- Ms-sql-s**, port associations with, 221
- MTBF (Mean Time Between Failures)**, quantitative risk assessment, 401-402
- MTTF (Mean Time To Failure)**, quantitative risk assessment, 402

MTTR (Mean Time To Repair), quantitative risk assessment, 402
 multicast IPv6 addresses, 181
 multidomain certificates, 523
 multifactor authentication, 337, 589
 multihomed connections, 262
 multipartite viruses, 21
 multiple user accounts, 371
 mutual authentication, 334

N

NAC (Network Access Control), 185-186
 NAS (Network Attached Storage), 63
 NAT (Network Address Translation), 180
 filtering, 259
 firewall effect, 180
 IPv4 addresses, 180-182
 IPv6 addresses, 181-182
 static NAT, 180
 native hypervisors, 112
 NCAS (National Cyber Awareness System), mobile device security, 67
 Ncat, 414
 need-to-know (incident response procedures), 633
 Nessus, 414
 net file command, analytical monitoring, 446
 NetBIOS, port associations with, 220
 NetBus, 22
 Netcat, 414-415
 netstat command, analytical monitoring, 446
 network controllers, security, 199
 Network layer (OSI model), 174
 networks
 adapters, 440, 558-559
 attacks
 ARP poisoning, 238, 241
 blackholes, 230
 client-side attacks, 236
 command-line scripting and, 235
 DDoS attacks, 229-230, 240
 DNS servers, 236-238, 241
 DoS attacks, 226-229, 239
 null sessions, 235, 241
 phishing attacks, 231
 replay attacks, 234-235, 241
 session hijacking, 232-234, 240
 sinkholes, 230
 spoofing attacks, 231-232, 240
 transitive access, 236, 241
 wired network/device security, 289
 authentication, 72
 back-to-back perimeter networks, 184
 bridges, 178
 cellular networks, 308
 cloud computing
 community clouds, 194
 CSP, 194
 definition, 192
 hybrid clouds, 194
 IaaS, 193
 MaaS, 194
 P2P networks and, 198
 PaaS, 193
 private clouds, 194
 public clouds, 194
 SaaS, 193
 SECaaS, 193
 security, 195-203
 services, 197
 social media and, 197
 XaaS, 194
 connections, redundancy planning, 558
 CSU, 179
 DLP systems, 59

DMZ

- 3-leg perimeter DMZ, 183*
- back-to-back perimeter networks, 184*

documenting network design, 309

DSU, 179

enumerators, 414

extranets, 184-185

firewalls, back-to-back perimeter networks, 184

Internet, 183

intranets, 184-185

IP addresses and ports, 222

LAN

- routers, 178*
- VLAN, 188-189*
- WAN versus, 182*

mapping, 411-412

modems, 190-191

NAC, 185-186

NAS, 63

NAT

- firewall effect, 180*
- IPv4 addresses, 180-182*
- IPv6 addresses, 181-182*
- private IPv4 addresses, 180*
- private IPv6 addresses, 181-182*
- public IPv4 addresses, 180*
- static NAT, 180*

OSI model, 173

- layers of, 174*
- TCP/IP model versus, 175*

PAT, IPv4 addresses, 180

PBX equipment, 191

perimeter security, 254-255

- DLP, 267*
- firewalls, 256-262*
- HIPS, 270*
- honeynets, 266*
- honeypots, 266*
- NIDS, 268-271*

NIPS, 268-271

proxy servers, 263-265

SSID broadcasting, disabling, 262

UTM, 272

web security gateways, 265

WIDS, 272

WIPS, 272

ports

- application service ports, 219*
- associated protocols table, 219-221*
- closing open ports, 224*
- dynamic ports, 218*
- FTP servers, 223*
- inbound ports, 219*
- IP addresses and, 222*
- outbound ports, 219*
- port zero security, 224*
- private ports, 218*
- protocol associations, 219-221*
- ranges, 218*
- registered ports, 218*
- scanning for open ports, 223*
- TCP, 217-221, 225*
- UDP, 217-221*
- unnecessary ports, 224*
- well-known ports, 218*

protocols and port associations

- associated protocols table, 219-221*
- Diameter, 221*
- DNS, 220*
- FCIP, 221*
- FTP, 219, 225*
- HTTP, 220*
- IMAP, 220*
- iSCSI, 221*
- Kerberos, 220*
- L2TP, 221*
- LDAP, 221*
- MS-sql-s, 221*

- NetBIOS*, 220
- NNTP*, 220
- POP3*, 220
- PPTP*, 221
- RADIUS*, 221
- RDP*, 221
- RPC*, 220
- RTP*, 222
- SMB*, 221
- SMTP*, 220
- SNMP*, 220
- SNMPTRAP*, 220
- SSH*, 219
- Syslog*, 221
- TACACS+*, 220
- Telnet*, 220
- TFTP*, 220
- redundancy planning
 - ISP*, 559
 - network adapters*, 558-559
 - network connections*, 558
 - servers*, 560-561
 - switches*, 559
- routers
 - ACL*, 179
 - Cisco routers*, 178
 - content filtering*, 179
 - firewalls*, 178
 - IPS*, 179
 - secure configurations*, 178
 - secure VPN connectivity*, 179
 - SOHO routers*, 178-179
- SAN*, NAS, 64
- SATCOM*, 308
- security, 254-255
 - air gaps*, 600-601
 - DLP*, 267
 - firewalls*, 256-262
 - HIPS*, 270
 - honeynets*, 266
 - honeypots*, 266
 - NIDS*, 268-271
 - NIPS*, 268-271
 - proxy servers*, 263-265
 - SSID broadcasting, disabling*, 262
 - UTM*, 272
 - web security gateways*, 265
 - WIDS*, 272
 - WIPS*, 272
- sniffers, 415-417
- subnetting, 186-187
- switches, 175
 - aggregation switches*, 177
 - ARP spoofing*, 177
 - DHCP starvation attacks*, 177
 - fail-open mode*, 176
 - looping*, 177
 - MAC flooding*, 176, 189
 - MAC spoofing*, 176-177
 - physical tampering*, 177
 - port security*, 176-177
 - STP*, 177
- TCP/IP model versus OSI model, 175
- telephony
 - modems*, 190-191
 - PBX equipment*, 191
 - VoIP*, 191
- traffic, incident response procedures, 631
- transitive trust, 72
- VLAN, 188-189
- VoIP, 191
- VPN, WAP, 300
- WAN
 - LAN versus*, 183
 - routers*, 178
- wired network/device security, 285
 - backdoors*, 288-289
 - cabling*, 290-295

- default accounts*, 286
 - network attacks*, 289
 - passwords*, 286-287
 - privilege escalation*, 287-288
 - remote ports*, 289
 - Telnet*, 289
 - wireless network security
 - Bluetooth*, 306-307
 - cellular networks*, 308
 - documenting network design*, 309
 - geofences*, 308
 - GPS*, 308
 - NFC*, 306-307
 - RFID*, 307
 - SATCOM*, 308
 - third-party wireless adapter connections*, 296
 - VPN*, 300
 - WAP*, 295-305
 - wireless protocols*, 298
 - wireless transmission vulnerabilities*, 304-305
 - NEXT (Near End Crosstalk)**, 292
 - NFC (Near Field Communication)**, 306-307
 - NGFW (Next Generation Firewalls)**, 532
 - NIDS (Network Intrusion Detection Systems)**, 55
 - placement within networks, 269
 - promiscuous mode, 268
 - protocol analyzers, 271
 - Nimda worm**, 21, 25
 - NIPS (Network Intrusion Prevention Systems)**, 268-269
 - false positives, 270
 - protocol analyzers, 271
 - NIST penetration testing**, 408
 - Nmap**, 413
 - NMS (Network Management System)**, SNMP, 444
 - NNTP (File Transfer Protocol)**, port associations with, 220
 - non-promiscuous mode**, network adapters, 440
 - non-repudiation**, 6, 450
 - nonces**, 235, 504
 - normalization**, relational databases, 157
 - NoSQL injections**, 157
 - NTFS (NT File System) permissions**, 372, 376
 - NTLM hashing**, 501-502
 - NTLMv2 hashing**, 502
 - null pointer dereferences**, 154
 - null sessions**, 235, 241
-
- ## O
-
- obfuscation**, programming security, 148
 - OCSP (Online Certificate Status Protocol)**, 528
 - offboarding**, 76, 620
 - on-demand VPN (Virtual Private Networks)**, 535
 - onboarding**, 76, 620, 623
 - one-time pads**, 493-494
 - one-to-one mapping**, 180, 527
 - one-way functions**, hashes as, 498
 - OOV (Order of Volatility)**
 - imaging media, 630-631
 - incident response procedures, 630-631
 - open mail relays**, preventing/troubleshooting spam, 39
 - open ports**
 - closing, 224
 - scanning for, 223
 - openfiles command**, analytical monitoring, 445
 - operational controls**, 404
 - optical discs**, malware delivery, 27
 - Orange Book**, 361, 364

organizational policies

data sensitivity

classifying data, 615*DHE*, 616*legislative policies*, 616-617

example of, 614-615

personal security policies, 617

AUP, 618, 622*awareness training*, 621-622*change management policies*, 619, 622*due care policies*, 621-623*due diligence, infrastructure security*,
621-623*due process policies*, 621-623*equipment recycling/donation policies*, 625*mandatory vacations*, 620-622*offboarding*, 620*onboarding*, 620, 623*privacy policies*, 618*separation of duties/job rotation policies*,
619, 622*user education*, 621-622*vendor policies*, 623-624**organized crime, 11****organizing CA horizontally, 528****OS**

fingerprinting, 403

hardening, 89

backward compatibility of applications, 91*baselining*, 105*blacklisting applications*, 92*centrally administered management
systems*, 92*configuration management*, 102*disabling services*, 95-97*file systems*, 105-106*Group Policies*, 102-104*hard disk space, conserving*, 91*hard disks*, 106-108*hotfixes*, 99-100*least functionality*, 90-91*Linux, starting/stopping services*, 95-97*macOS/OS X, starting/stopping services*,
96-97*messaging*, 90*patches*, 99-102*reducing attack surface*, 94*remote control programs*, 90*Remote Desktop Connection*, 90*Remote Desktop Services*, 93*removing applications*, 90-91*removing services*, 90-91*security templates*, 103-104*TOS*, 97*updates*, 98-99*whitelisting applications*, 92*Windows, starting/stopping services*, 95-97*Windows Programs and Features window*,
91*Windows Update*, 98-99*Windows XP*, 94

privilege escalation, 287-288

updates, 108

OS GUI, closing open ports, 224**OS X**OS hardening, starting/stopping services,
96-97

patch management, 102

patches, 101-102

OSI (Open Systems Interconnection)**model, network design**, 173

layers of, 174

TCP/IP model versus, 175

**OSINT (Open Source Intelligence), social
engineering, 584****OSSEC, 56****OSSTMM (Open Source Security Testing
Methodology Manual), penetration
testing, 408**

out-of-band management, 444
outbound ports, 219
Outlook, securing, 143
OV (Organizational Validation) certificates, 522
OVAL (Open Vulnerability and Assessment Language), 408-409

P

P2P networks

cloud computing and, 198
 malware delivery, 27

P12/PFX (P12 Personal Information Exchange) format, certificates, 524

PaaS (Platform as a Service), 193

PAC (Proxy Auto-Configuration) files, 263

packets

capturing, 415, 440
 filtering, 258
 headers
 manipulating, 441
 session theft, 232
 HTTP response packets, header manipulation, 441
 sniffers, 443
 SPI, 258

PAM (Pluggable Authentication Modules), Kerberos, 336

pass the hash attacks, 502-503

passive optical splitters, fiber-optic cabling, 294

passive reconnaissance (security analysis), 403

passwords, 376-377

Administrator accounts, 378
 analyzing, 417-40
 BIOS, 60
 browser security, 139
 clear-text passwords, 443

cloud security, 195
 complexity of, 381
 cracking, 417-420
 data exfiltration, 378
 default accounts, 286
 drive lock passwords, 61
 guest accounts, 378
 hashing
 birthday attacks, 503
 key stretching, 504
 LANMAN hashing, 500-501
 NTLM hashing, 501-502
 NTLMv2 hashing, 502
 pass the hash attacks, 502-503
 length of, 381
 mobile devices, 67, 71
 nonce, 504
 policies, 379-383
 programming security, 147
 strong passwords, 286-287
 wired network/device security, 286-287

PAT (Port Address Translation), IPv4 addresses, 180

patches

managing, 101-102, 142
 OS hardening, 99-102
 programming security, 148

PayPal, VeriSign certificates, 525

PBX (Private Branch Exchange) equipment, network design, 191

Pcap. *See* packets, capturing

PDS (Protected Distribution Systems), cabling, 295

PEAP (Protected Extensible Authentication Protocol), 330-332

PEM (Privacy-enhanced Electronic Mail) format, certificates, 524

penetration tests, 149, 407-408

people, succession planning, 562

performance baselining

- alerts, 440
- baseline reporting, 438
- Performance Monitor, 439
- standard loads, 438
- System Monitor, 440

Performance Monitor, 439, 445**peripherals (wireless), 66****permanent DoS attacks, 229****permanently installed generators, 553****permissions**

- ACL, 371
- DACL, 372
- inheritance, 374-375
- IT folder, 458
- Linux file permissions, 373
- NTFS permissions, 372, 376
- privilege creep, 374
- programming security, 147
- propagating, 375
- SACL, 372
- user access recertification, 374

persistence (penetration testing), 407**persistent cookies, 136****personal firewalls, 53**

- IPFW, 54
- iptables, 54
- PF, 54
- SOHO router/firewall configuration, 55
- Windows Firewall, 54
- ZoneAlarm, 54

personal security policies, 617

- AUP, 618, 622
- awareness training, 621-622
- change management policies, 619, 622
- due care policies, 621-623
- due diligence, infrastructure security, 621-623

- due process policies, 621-623
- mandatory vacations, 620-622
- offboarding, 620
- onboarding, 620, 623
- privacy policies, 618
- separation of duties/job rotation policies, 619, 622
- user education, 621-622

PF (Packet Filters), 54**PFS (Perfect Forward Secrecy), 492****PGP (Pretty Good Privacy), 494-495****pharming, 237****PHI (Protected Health Information), 616-617****phishing attacks, 231, 586, 590****phone number encryption, 477-480****phone phishing. *See* vishing****photo ID, 324****PHP scripts, exploit kits, 27****Physical layer (OSI model), 174****physical security, 7**

- authentication, 321
- biometric readers, 326-327, 345
- CCTV, 323
- door access
 - cardkey systems, 324*
 - cipher locks, 324*
 - mantraps, 326*
 - proximity sensors, 325*
 - security tokens, 325*
 - smart cards, 325*

fingerprint readers/scanners, 326**mantraps, 589****motion detectors, 323****server rooms, 323****user safety, 324****video surveillance, 323****piggybacking, social engineering attacks, 589-591**

PII (Personally Identifiable Information),
616-617, 622

ping floods, 226, 239

pinning certificates, 526-527

pivots (penetration testing), 407

PIV (Personal Identity Verification) cards.
See smart cards

PKI (Public Key Infrastructure)

CA

certificate mapping, 527

certificate pinning, 526-527

certificate validation, 525

certificate verification with RA, 527

chain of trust, 528

CRL, 527

CSR, 525

horizontal organization, 528

key escrow, 528

key recovery agents, 528

revoking certificates, 527-528

VeriSign certificates, 72, 525

web of trust, 529

certificates

BER format, 524

CA, 525

CER format, 524

chain of trust, 523, 528

DER format, 524

dual-sided certificates, 523

DV certificates, 522

EV certificates, 522

multidomain certificates, 523

OV certificates, 522

P12/PFX format, 524

PEM format, 524

SAN field, 523

single-sided certificates, 523

validation, 525

web of trust, 529

wildcard certificates, 523

X.509 standard, 522

defining, 521

IPsec

AH, 534

ESP, 535

SA, 534

transport mode, 535

tunneling mode, 535

L2TP, 534

PPTP, 533

S/MIME, 530-531

SSH, 532-533

SSL/TLS, 531-532

PlugX RAT, 22

PlugX Trojans, 25

PNAC (Port-based Network Access
Control), 802.1X, 330

POD (Ping of Death), 228, 239

Poirot, Hercule, 435

policies

access control

Account Lockout Threshold Policy, 382

Default Domain Policy, 379

passwords, 379-383

Account Lockout Threshold Policy, 382

Default Domain Policy, 379

equipment recycling/donation policies, 625

legislative policies, 616-617

organizational policies

data sensitivity, 615-617

equipment recycling/donation policies, 625

example of, 614-615

personal security policies, 617-623

vendor policies, 623-624

passwords, 379-383

personal security policies, 617

AUP, 618, 622

awareness training, 621-622

- change management policies, 619, 622*
- due care policies, 621-623*
- due diligence, infrastructure security, 621-623*
- due process policies, 621-623*
- mandatory vacations, 620-622*
- offboarding, 620*
- onboarding, 620, 623*
- privacy policies, 618*
- separation of duties/job rotation policies, 619, 622*
- user education, 621-622*
- privacy policies, 618
- procedures versus, 613
- vendor policies
 - BPA, 623-624*
 - ISA, 624*
 - MoU, 624*
 - SLA, 623-624*
- policy implementation, applications, 140**
- polymorphic viruses, 20**
- POP3, port associations with, 220**
- pop-under ads, 59**
- pop-up blockers, 53, 57-59, 135**
- portable generators, 553**
- ports**
 - application service ports, 219
 - associated protocols table, 219-221
 - dynamic ports, 218
 - external ports, disabling, 61
 - FTP servers, 223
 - inbound ports, 219
 - IP addresses and, 222
 - mirroring, 442
 - NAC, 186
 - open ports
 - closing, 224*
 - scanning for, 223*
 - unnecessary ports, 224*
 - outbound ports, 219
 - PAT, IPv4 addresses, 180
 - PNAC, 802.1X, 330
 - port zero security, 224
 - private ports, 218
 - registered ports, 218
 - remote ports, wired network/device security, 289
 - RTP and port associations, 222
 - scanning, 413
 - SNMP, 444
 - switch port security, 176-177
 - TCP, 217-221, 225
 - twisted-pair networks, wiretapping, 293
 - UDP, 217-221
 - well-known ports, 218
 - WinDump, 443
- possession factors (authentication), 322**
- post-certification process, 655**
- power supplies**
 - backup generators
 - considerations for selecting, 554*
 - types of, 553*
 - battery backups, 552
 - blackouts, 550
 - brownouts, 550
 - disaster recovery, 568
 - failures, 550
 - redundancy planning, 549-550
 - backup generators, 553-554*
 - battery backups, 552*
 - standby generators, 553*
 - UPS, 551-552*
 - sags, 550
 - spikes, 550
 - standby generators, 553
 - surges, 550
 - UPS, 551-552

PPTP (Point-to-Point Tunneling Protocol), 533

port associations with, 221

VPN connections, 340-342

practice exams, 649**pre-action sprinkler systems, 596****Premiere Pro, 91****preparation phase (incident response procedures), 628****preparing for exams**

exam preparation checklist, 647-650

grading scale, 647

post-certification process, 655

taking exams, 651-654

Presentation layer (OSI model), 174**preserving evidence (incident response procedures), 629, 632-633****pretexting, social engineering attacks, 584, 590****preventing/troubleshooting**

ransomware, 35

rootkits, 38, 41

spam, 38-41

spyware, 35-37, 41

Trojans, 35, 41

viruses, 41

antivirus software, 31, 34

encryption, 33

Linux-based tools, 35

Windows Firewall, 31

Windows Update, 31

worms, 35, 41

preventive controls, 404**principle of defense in depth, 147****principle of least privilege, 147****Privacy Act of 1974, 616-618****privacy policies, 618****private clouds, 194****private information, classifying (data sensitivity), 615****private IPv4 addresses, 180****private key cryptography, 481, 490****private ports, 218****privilege**

creep, 374

de-escalation, 288

escalation. *See also* jailbreaking

horizontal privilege escalation, 288

malware delivery, 29

SOHO routers, 288

vertical privilege escalation, 288

wired network/device security, 287-288

principle of least privilege, 147

PRNG (Pseudorandom Number Generator), 495**Pro Tools, 91****procedures**

incident response procedures, 627

chain of custody (evidence collection), 629

collecting/preserving evidence, 629, 632-633

containment phase, 628

damage/loss control, 630

emergency response detail, 629

eradication phase, 628

events versus incidents, 627

forensics, 630-632

identification phase, 628

initial incident management process, 629

lessons learned phase, 628

need-to-know, 633

preparation phase, 628

recovery phase, 628

witness statements, 631

policies versus, 613

process VM (Virtual Machines), 111**program viruses, 20****programming**

ASLR, 155

- authenticity, 148
- CIA triad, 146
- cloud security, 196
- code checking, 148
- code signing, 148
- DevOps, 146-148
- error-handling, 148
- integrity, 148
- minimizing attack surface area, 147
- obfuscation, 148
- passwords, 147
- patches, 148
- permissions, 147
- principle of least privilege, 147
- quality assurance policies, 147
- SDLC
 - agile model*, 146
 - principles of*, 146-148
 - V-shaped model*, 145
 - waterfall model*, 145
- secure code review, 146
- secure coding concepts, definition of, 144
- testing methods
 - black-box testing*, 149
 - compile-time errors*, 150
 - dynamic code analysis*, 152
 - fuzz testing*, 152
 - gray-box testing*, 149
 - input validation*, 150-151
 - penetration tests*, 149
 - runtime errors*, 150
 - sandboxes*, 149
 - SEH*, 150
 - static code analysis*, 151-152
 - stress testing*, 149
 - white-box testing*, 149
- threat modeling, 147
- trusting user input, 147

- vulnerabilities/attacks
 - arbitrary code execution*, 155
 - backdoor attacks*, 22, 29, 153, 159
 - buffer overflows*, 153, 159
 - code injections*, 156-159
 - directory traversals*, 158-159
 - DLL injections*, 158
 - integer overflows*, 154
 - LDAP injections*, 157
 - memory leaks*, 154
 - NoSQL injections*, 157
 - null pointer dereferences*, 154
 - RCE*, 155, 159
 - SQL injections*, 156
 - XML injections*, 157
 - XSRF*, 156, 159
 - XSS*, 156, 159
 - zero day attacks*, 158-159

Programs and Features window (Windows), OS hardening, 91

promiscuous mode

- network adapters, 440
- NIDS, 268

propagating permissions, 375

proprietary information, classifying (data sensitivity), 615

protocol analyzers, 415

- broadcast storms, 441
- network adapters, 440
- NIDS, 271
- packet capturing, 440
- TCP/IP handshakes, 441
- Wireshark, 441-442

protocols, port associations with

- associated protocols table, 219-221
- Diameter, 221
- DNS, 220
- FCIP, 221
- FTP, 219, 225

- HTTP, 220
- IMAP, 220
- iSCSI, 221
- Kerberos, 220
- L2TP, 221
- LDAP, 221
- MS-sql-s, 221
- NetBIOS, 220
- NNTP, 220
- POP3, 220
- PPTP, 221
- RADIUS, 221
- RDP, 221
- RPC, 220
- RTP, 222
- SMB, 221
- SMTP, 220
- SNMP, 220
- SNMPTRAP, 220
- SSH, 219
- Syslog, 221
- TACACS+, 220
- Telnet, 220
- TFTP, 220
- proximity sensors, physical security, 325**
- proxy servers, 133-134**
 - application proxies, 264
 - caching proxies, 263-264
 - forward proxies, 264
 - HTTP proxies, 263
 - Internet content filtering, 265
 - IP proxies, 263
 - PAC files, 263
 - reverse proxies, 264
 - transparent proxies, 265
- pseudocodes. *See* error-handling**
- PSK (Pre-Shared Keys), WAP, 298**
- public clouds, 194**
- public information, classifying (data sensitivity), 615**

- public IPv4 addresses, 180**
- public key cryptography, 481-483**
 - certificates, 484
 - digital signatures, 484
 - ECC, 492-493
 - ECDHE, 492
 - RSA, 490

- public networks, split tunneling, 342**

- punch blocks, wiretapping, 293**

- purging (data removal), 626**

Q - R

- QKD (Quantum Key Distribution), 493**

- qualitative risk assessment, 399, 402**

- quality assurance policies, 147**

- quantitative risk assessment, 400-402**

- quantum cryptography, 493**

- questions (end-of-chapter), exam preparation, 648**

- RA (Registration Authority), certificate verification, 527**

- race condition exploits, 408**

- RADIUS (Remote Authentication Dial-In User Service)**

- port associations with, 221

- RADIUS federation, 343-345

- RAID (Redundant Array of Independent Disks)**

- high availability, 63

- RAID 0, 555

- RAID 0+1, 556

- RAID 1, 556-557

- RAID 5, 556-557

- RAID 6, 556-558

- RAID 10, 556

- rainbow tables, 419, 498**

- ransomware, 22**

- CryptoLocker, 23, 26
- definition of, 26
- preventing/troubleshooting, 35
- RAS (Remote Access Service), 337, 340, 344**
 - CHAP, 338-339
 - MS-CHAP, 338
- RAT (Remote Access Trojans), 22, 29, 202-203**
- RBAC (Role-Based Access Control), 364-366**
- RC (Rivest Cipher)**
 - RC4, 488-489
 - RC5, 489
 - RC6, 489
- RCE (Remote Code Execution), 155, 159**
- RDBMS (Relatable Database Management System), 156-157**
- RDP (Remote Desktop Protocol), port**
 - associations with, 221
- record time offset, 631
- recovering certificate keys, 528
- recovery phase (incident response procedures), 628
- recycling/donating equipment policies, 625
- Red Book, 362**
- Red Hat Enterprise, Kerberos and PAM, 336**
- Red October, 24**
- reduced sign-ons, 328
- reducing risk, 398
- redundancy planning
 - data, 555-558
 - employees, 562
 - fail-closed, 549
 - fail-open, 549
 - failover redundancy, 548
 - networks
 - ISP, 559
 - network adapters, 558-559
 - network connections, 558
 - servers, 560-561
 - switches, 559
 - power supplies, 549-550
 - backup generators, 553-554
 - battery backups, 552
 - standby generators, 553
 - UPS, 551-552
- RAID, 555-558
- single points of failure, 547-548
- succession planning, 562
- websites, 561
- reference frameworks (IT security), 634**
- registered ports, 218**
- registering for exams, 650**
- relational databases**
 - normalization, 157
 - RDBMS, 156-157
- remanence (data), 8**
- remote authentication**
 - RADIUS, 343-345
 - RAS, 337, 340, 344
 - CHAP, 338-339
 - MS-CHAP, 338
 - TACACS+, 220, 343-345
 - VPN
 - always-on VPN, 342
 - GRE, 342
 - illustration of, 340
 - L2TP, 340-342
 - PPTP, 340-342
 - RRAS, 341
 - split tunneling, 342
 - VPN concentrators, 342
- remote control programs, OS hardening, 90**
- Remote Desktop Connection, OS hardening, 90**
- Remote Desktop Services, 93, 336-337**

remote ports, wired network/device security, 289

removable media controls, 63

removable storage/media, 62-63

removing

applications, 90-91

data, 8

clearing, 626

destroying storage media (physical data removal), 627

purging, 626

services, 90-91

unnecessary applications/services, 90-91

replay attacks, 234-235, 241

residual risk, 398

restore points, hard disks, 107

reverse proxies, 264

revoking certificates

CRL, 527

OCSF, 528

RFI (Radio Frequency Interference), cabling, 291

RFID (Radio-Frequency Identification), 307

RIPEMD (RACE Integrity Primitives Evaluation Message Digest), 499

risk

analysis, IT security frameworks, 635

assessment

defining risk, 397-398

impact assessment, 399

qualitative risk assessment, 399, 402

qualitative risk mitigation, 400

quantitative risk assessment, 400-402

residual risk, 398

risk acceptance, 398

risk avoidance, 398

risk management, 397-399

risk reduction, 398

risk registers, 399

risk transference, 398

security analysis, 402-403

security controls, 404-405

vulnerability assessment, 396, 406, 410-420

vulnerability management, 405-410

GRC, 617

Rivest, Ron

MD5, 498

RC, 488-489

RSA, 490

RJ11 jacks, wiretapping, 293

RJ45 jacks, wiretapping, 293

RJ45 wall plates, wiretapping, 293

rogue AP (Access Points), 296

Ron's Code. See RC

room security. See physical security

root of trust, 62

rooting, 75, 135

rootkits

Alureon rootkits, 24-26

definition of, 26

detecting, 24

Evil Maid Attacks, 26

preventing/troubleshooting, 38, 41

routers

ACL, 179

Cisco routers, 178

content filtering, 179

firewalls, 178

IPS, 179

secure configurations, 178

secure VPN connectivity, 179

SOHO firewall configuration, 55

SOHO routers

configuring, 55

default accounts, 286

firewalls, 178

firewalls and, 260

privilege escalation, 288

secure VPN connectivity, 179

WIC, 179

RPC (Remote Procedure Calls), port associations with, 220

RPO (Recovery Point Objective), BCP, 569

RRAS (Routing and Remote Access Service), VPN connections, 341

RSA (Rivest, Shamir, and Adleman), 490

RSA tokens. *See* security, tokens

RTBH (Remotely Triggered Blackholes), 230

RTO (Recovery Time Objective), BCP, 569

RTP (Real-time Transport Protocol) and ports, 222

runtime errors, 150

S

S/MIME (Secure/Multipurpose Internet Mail Extensions), 530-531

SA (Secure Associations), IPsec, 534

SaaS (Software as a Service), 193

SACL (System Access Control Lists), 372

Safe Mode

antivirus software, 34

spyware, preventing/troubleshooting, 37

sags (power supplies), 550

salting, cryptanalysis attacks, 419

SAN (Storage Area Networks), NAS, 64

SAN (Subject Alternative Name) field, certificates, 523

sandboxes, definition of, 149

sanitizing mobile devices (data removal), 70, 626

SATCOM (Satellite Communications), wireless network security, 308

SB 1386, 617

SCADA (Supervisory Control and Data Acquisition), HVAC (facilities security), 598, 600

scanning

ports, 413

vulnerabilities, 412-414

SCCM (System Center Configuration Manager), 102

scheduling incremental data backups, 563-564

Schneier, Bruce, 489

SCP (Secure Copy), 226

screen locks, mobile devices, 71

screenshots, incident response procedures, 631

script kiddies, 11

SCRM (Supply Chain Risk Management), 399

SDLC (Software Development Life Cycle)

agile model, 146

principles of, 146-148

V-shaped model, 145

waterfall model, 145

SECaaS (Security as a Service), 193

secret information, classifying (data sensitivity), 615

secure boot option, BIOS, 61

secure code review, 146

secure coding concepts, definition of, 144

secure VPN connectivity, routers, 179

security

analysis, 402

active reconnaissance, 403

passive reconnaissance, 403

controls

compensating controls, 405

corrective controls, 405

detective controls, 405

management controls, 404

operational controls, 404

preventive controls, 404

technical controls, 404

events

audit trails, 451

failure to see events in security logs, 450

SIEM, 460

logs

application logs, 452

audit trails, 451

DFS Replication logs, 452

DNS Server logs, 452

file maintenance/security, 455-457

firewall logs, 453

non-repudiation, 450

security events, failure to see events, 450

Syslog, 454-455

system logs, 452

plans, 7

postures, baseline reporting, 438

protocols, 529

IPsec, 534-535

L2TP, 534

PPTP, 533

S/MIME, 530-531

SSH, 532-533

SSL/TLS, 531-532

templates, OS hardening, 103-104

tokens, 325

updates, 98

security zones, browsers, 135

SED (Self-Encrypting Drives), 64

segregation of duties, 405

SEH (Structured Exception Handling), 150

SELinux, 57

sensitive data

classifying, 615

data handling (DHE), 616

exposure of, 151

legislative policies, 616-617

separation of duties

access control, 368

job rotation policies, 619, 622

server clusters, 561

failover clusters, 560

load-balancing clusters, 560

server rooms

physical security, 323

mantraps, 589

servers

Apache servers

CVE listings, 201

Darkleech, 201

authentication, 72

authentication servers (802.1X), 331

back office applications, securing, 143

banner grabbing, 414

DNS servers

altered host files, 237, 241

DNS poisoning, 236, 241

domain name kiting, 238, 241

pharming, 237

unauthorized zone transfers, 237, 241

email servers, security, 199-200

file servers, security, 198-199

FTP servers

ports and, 223

protocol analysis, 443

security, 202-203

key management, 72

network controllers, security, 199

proxy servers

application proxies, 264

caching proxies, 263-264

forward proxies, 264

HTTP proxies, 263

Internet content filtering, 265

IP proxies, 263

PAC files, 263

- reverse proxies*, 264
 - transparent proxies*, 265
- redundancy planning, clusters, 560-561
- security
 - email servers*, 199-200
 - file servers*, 198-199
 - FTP servers*, 202-203
 - network controllers*, 199
 - web servers*, 200-202
- standard loads, 438
- web servers, security, 200-202
- Windows Server, network shares, 457
- service packs, updates, 98**
- services**
 - backward compatibility, 91
 - cloud computing, 197
 - consolidating, 144
 - disabling, 95-97
 - OS hardening, 90-97
 - Remote Desktop Services, 93
 - removing, 90-91
- Session layer (OSI model), 174**
- sessions**
 - hijacking
 - blind hijacking*, 233
 - clickjacking*, 233
 - MITB attacks*, 233-234, 240
 - MITM attacks*, 233, 240
 - session theft*, 232, 240
 - TCP/IP hijacking*, 232, 240
 - watering hole attacks*, 234, 240
 - XSS*, 137
 - monitoring, Computer Management, 445
 - theft of, 28
- SFTP (Secure FTP), 225**
- SHA (Secure Hash Algorithm), 498-499**
- sharing risk, 398**
- shielding, facilities security, 598**
 - Faraday cages, 599
 - HVAC shielding, 599
 - STP cabling, 599
 - TEMPEST, 599-600
- shoulder surfing, social engineering attacks, 588-590**
- SHTTP (Secure Hypertext Transfer Protocol Secure), 532**
- sideloading mobile devices, 75**
- SIEM (Security Information and Event Management), 460**
- signal emanation. *See* data emanation**
- signal jammers (wireless), 302**
- signatures**
 - IDS signature-based detection, 56
 - public key cryptography, 484
 - signature-based monitoring, 435-437
- SIM cloning, 68, 77**
- simulations/videos, exam preparation, 648**
- single points of failure, redundancy planning, 547-548**
- single-sided certificates, 523**
- sinkholes, 230**
- SLA (Service-Level Agreements), 623-624**
- SLE (Single Loss Expectancy), quantitative risk assessment, 400-401**
- smart cards, physical security, 325**
- smartphones, 66**
 - access control, 75
 - application security, 78
 - application blacklisting*, 73
 - application whitelisting*, 73
 - geotagging*, 74
 - HTTPS connections*, 71-72
 - key management*, 72
 - MMS attacks*, 73
 - server/network authentication*, 72
 - SMS attacks*, 73
 - transitive trust*, 72
 - bluejacking, 69
 - bluesnarfing, 69

- botnets, 68, 77
- browser security, 135
- BYOD, 74-78
- carrier unlocking, 69
- COPE, 74
- CYOD, 74
- encryption, 67
- full device encryption, 70
- GPS tracking, 70, 74
- jailbreaking, 75, 135
- lockout programs, 70
- malware, 27, 67, 77
- MDM, 75
- offboarding, 76
- onboarding, 76
- passwords, 67, 71
- rooting, 75, 135
- sanitizing, 70
- screen locks, 71
- sideloading, 75
- SIM cloning, 68, 77
- social engineering attacks, 68
- storage segmentation, 75
- theft of, 70-71, 77
- wireless attacks, 69-70
- SMB (Server Message Blocks), port associations with, 221**
- SMS attacks, 73**
- SMTP (Simple Mail Transfer Protocol)**
 - port associations with, 220
 - preventing/troubleshooting spam
 - open relays, 39*
 - servers, 39*
- Smurf attacks, 226, 239**
- snapshots**
 - backups, 566
 - VM disk files, 114
- sniffers (network), 415-417**

- SNMP (Simple Network Management Protocol), 220, 443-445**
- SNMPTRAP, port associations with, 220**
- social engineering attacks, 6**
 - baiting, 589-591
 - CA and, 527
 - confidence tricks (cons), 588
 - defining, 584
 - diversion theft, 586, 590
 - dumpster diving, 588-590
 - eavesdropping, 588-590
 - hoaxes, 587, 590
 - malicious insiders, 585, 590
 - mobile devices, 68
 - OSINT, 584
 - phishing, 586, 590
 - piggybacking, 589-591
 - pretexting, 584, 590
 - shoulder surfing, 588-590
 - tailgating, 589-591
 - techniques/principles, 584
 - war-dialing, 587
 - watering hole attacks, 589-591
- social media, cloud computing and, 197**
- software**
 - anti-malware, 8, 108
 - antivirus software
 - Safe Mode, 34*
 - Trojan prevention/troubleshooting, 35*
 - virus prevention/troubleshooting, 31, 34*
 - worm prevention/troubleshooting, 35*
 - badware, 37
 - crimeware, 27
 - DevOps, 146-148
 - firewalls, 53
 - IPFW, 54*
 - iptables, 54*
 - PF, 54*
 - SOHO router/firewall configuration, 55*

- Windows Firewall*, 54
- ZoneAlarm*, 54
- malware, 6, 19
 - adware*, 23
 - anti-malware*, 8, 108
 - APT*, 22
 - attack vectors*, 26
 - badware*, 37
 - delivery of*, 26-30
 - exploit kits*, 27
 - grayware*, 23
 - keyloggers*, 27
 - malvertising*, 23
 - non-malware*, 24
 - ransomware*, 22-23, 35
 - rootkits*, 24-26, 38, 41
 - spam*, 25, 38-41
 - spim*, 25
 - spyware*, 23-24, 35-37, 41
 - threat vectors*, 26
 - Trojans*, 22, 25, 29, 35, 41, 67
 - unsavable computers*, 40
 - URL hijacking*, 27
 - viruses*, 20-21, 25, 31-35, 41
 - websites*, 27
 - worms*, 21, 25, 35, 41
- ransomware, worms, 26
- SLDC
 - agile model*, 146
 - principles of*, 146-148
 - V-shaped model*, 145
 - waterfall model*, 145
- spyware, worms, 26
- use case analysis, 634
- SOHO (Small Office/Home Office) routers**
 - configuring, 55
 - default accounts, 286
 - firewalls, 55, 178, 260
 - privilege escalation, 288
 - secure VPN connectivity, 179
- Solitaire, Easter Eggs**, 30
- SOX (Sarbanes-Oxley) act**, 616-617
- SPA (Security Posture Assessments)**,
 - baseline reporting, 438
- spam**, 25
 - definition of, 26
 - filters, 38
 - firewalls, 38
 - honeypots, 266
 - identity theft emails, 26
 - lottery scam emails, 26
 - preventing/troubleshooting, 38-41
- SPAN. See ports, mirroring**
- spear phishing**, 586, 590
- special hazard protection systems**, 596
- spectral analyzers, data emanations**, 294
- SPI (Stateful Packet Inspection)**, 258
- spikes (power supplies)**, 550, 599
- spim**, 25
- split tunneling**, 342
- spoofing attacks**, 231-232, 240
 - ARP spoofing, 177
 - IP spoofing attacks, 179
 - MAC spoofing, 176-177
 - spoofed MAC addresses, 305
 - stateless packet filters, 259
 - switch spoofing, 189
- sprinkler systems**
 - pre-action sprinkler systems, 596
 - wet pipe sprinkler systems, 595
- spyware**, 23-24
 - definition of, 26
 - Internet Optimizer, 26
 - preventing/troubleshooting, 35-37, 41
 - symptoms of, 36
 - tracking cookies, 137
- SQL injections**, 156
- SSH (Secure Shell)**, 219, 532-533

SSID (Service Set Identifiers)

broadcasting, disabling, 262

WAP, 296

SSL pinning. *See* digital certificates, pinning

SSL/TLS (Secure Sockets Layer/Transport Layer Security), 531-532

SSO (Single Sign-On), 328-329

standard loads, servers, 438

standby generators, 553

statements (witness), incident response procedures, 631

static and dynamic analytical monitoring tools, 447

static code analysis, 151-152

static NAT (Network Address Translation), 180

statistical anomaly detection (IDS), 56

stealth viruses, 21

steganography, defining, 485

storage, 62

destroying storage media (data removal), 627

DLP systems, 59

flash drives, 63

hard drive encryption, 64-65

HSM, 65-66

mobile devices, storage segmentation, 75

NAS, 63-64

removable storage/media, 62-63

USB devices, 63

stored procedures, 157

STP (Shielded Twisted-Pair) cabling, 292, 599

STP (Spanning Tree Protocol) switches, 177

stream ciphers, 482

one-time pads, 493-494

RC4, 488-489

stress testing, 149

stylometry and genetic algorithms, 496

subnetting, 186-187

SubSeven, 22

succession planning, 562

supplicants (802.1X), 331

surge protectors, 108

surges (power supplies), 550

surveys

interference, 302

jamming, 302

wireless site surveys, 302

switches, 175

aggregation switches, 177

ARP spoofing, 177

DHCP starvation attacks, 177

fail-open mode, 176

looping, 177

MAC flooding, 176, 189

MAC spoofing, 176-177

physical tampering, 177

port security, 176-177

redundancy planning, 559

STP, 177

switch spoofing, 189

symmetric algorithms, 481

3DES, 486

AES, 487-489

block ciphers, 482

Blowfish, 489

DEA, 486

DES, 486, 489

IDEA, 486

RC, 488-489

stream ciphers, 482

Threefish, 489

Twofish, 489

SYN floods, 227, 239

SYN packets, TCP/IP hijacking, 232

Syslog, 221, 454-455
system failure, 6
system files, OS hardening, 107
system images, 109, 630
system logs, 452
System Monitor, 440
system security, auditing, 457-460
system VM (Virtual Machines), 111

T

tables (rainbow), 498
tablets, 66

- access control, 75
- application security, 78
 - application blacklisting*, 73
 - application whitelisting*, 73
 - geotagging*, 74
 - HTTPS connections*, 71-72
 - key management*, 72
 - MMS attacks*, 73
 - server/network authentication*, 72
 - SMS attacks*, 73
 - transitive trust*, 72
- bluejacking, 69
- bluesnarfing, 69
- botnets, 68, 77
- browser security, 135
- BYOD, 74-78
- COPE, 74
- CYOD, 74
- encryption, 67
- full device encryption, 70
- GPS tracking, 70, 74
- jailbreaking, 75, 135
- lockout programs, 70
- malware, 67, 77
- MDM, 75
- offboarding, 76

- onboarding, 76
- passwords, 67, 71
- rooting, 75, 135
- sanitizing, 70
- screen locks, 71
- sideloading, 75
- social engineering attacks, 68
- storage segmentation, 75
- theft of, 70-71, 77
- wireless attacks, 69-70

TACACS+ (Terminal Access Controller Access-Control System Plus), 220, 343-345

tailgating, social engineering attacks, 589-591

taking exams, 651-654

TCP (Transmission Control Protocol)

- ports, 217-221
- reset attacks, 225

TCP/IP (Transmission Control Protocol/Internet Protocol)

- fingerprinting, 403
- handshakes, 441
- hijacking, 232, 240
- network design, OSI model versus TCP/IP model, 175

tcpdump packet analyzer, 443

TCSEC (Trusted Computer System Evaluation Criteria), 361

teardrop attacks, 229, 239

technical controls, 404

technical security plans, 7

telephony

- modems, 190-191
- network design, 190-191
- VoIP, 191

Telnet, 415

- port associations with, 220
- remote network access, 289

TEMPEST (Transient ElectroMagnetic Pulse Emanations Standard), 293, 599-600

templates (security), OS hardening, 103-104

temporary files

OS hardening, 106

securing, 138

testing

penetration testing, 407-408

testing programs

black-box testing, 149

compile-time errors, 150

dynamic code analysis, 152

fuzz testing, 152

gray-box testing, 149

input validation, 150-151

penetration tests, 149

runtime errors, 150

sandboxes, 149

SEH, 150

static code analysis, 151-152

stress testing, 149

white-box testing, 149

TFTP (Trivial File Transfer Protocol), port associations with, 220

theft

disaster recovery, 568

diversion theft, social engineering attacks, 586, 590

mobile devices, 70-71, 77

threat actors. *See also* hackers

APT, 11

cyber-criminals, 11

hactivists, 11

organized crime, 11

script kiddies, 11

threat modeling, 147

threat vectors, malware delivery, 26

Threefish, 489

tickets (KDC), 334

time bombs, malware delivery, 29

time-of-day restrictions, user accounts, 370

TKIP (Temporal Key Integrity Protocol), 298

TOC (Time-of-Check) attacks, 408

top secret information, classifying (data sensitivity), 615

torrents (bit), malware delivery, 27

TOS (Trusted Operating Systems), 97

TOU (Time-of-Use) attacks, 408

Towers of Hanoi backup scheme, 566

tracking cookies, 137

training

awareness training, 7, 621-622

users, 7, 591-593

transferring risk, 398

transitive access, 236, 241

transitive trust, 72

transmitting malware

active interception, 28

attack vectors, 26

backdoors, 29

bit torrents, 27

botnets, 28

Easter eggs, 30

email, 26

exploit kits, 27

FTP servers, 26

instant messaging, 26

keyloggers, 27

logic bombs, 29

media-based delivery, 27

memory cards, 27

optical disks, 27

P2P networks, 27

privilege escalation, 29

smartphones, 27

software, 26

- threat vectors, 26
- time bombs, 29
- typosquatting, 27
- URL hijacking, 27
- USB flash drives, 27
- user error, 27
- websites, 27
- zip files, 26
- zombies, 28
- transparent proxies, 265**
- transparent testing. *See* white-box testing**
- Transport layer (OSI model), 174**
- transport mode, IPsec, 535**
- Trend Micro OSSEC, 56**
- Triple DES (Data Encryption Standard).**
See 3DES
- Tripwire, 57**
- Trojans**
 - definition of, 25
 - GinMaster Trojan, 67
 - MITB attacks, 233-234, 240
 - PlugX Trojans, 25
 - preventing/troubleshooting, 35, 41
 - RAT, 22, 29, 202-203
 - time bombs, 29
 - ZeroAccess botnet, 28
- troubleshooting**
 - ransomware, 35
 - rootkits, 38, 41
 - spam, 38-41
 - spyware, 35-37, 41
 - Trojans, 35, 41
 - viruses, 41
 - antivirus software, 31, 34*
 - encryption, 33*
 - Linux-based tools, 35*
 - Windows Firewall, 31*
 - Windows Update, 31*
 - worms, 35, 41

- trust**
 - chain of (certificates), 523, 528
 - web of, 529
- Trusted Network Interpretation standard, 362**
- trusting user input, 147**
- Trustworthy Computing principle, 30**
- tunneling mode, IPsec, 535**
- tunneling protocols**
 - L2TP, 534
 - PPTP, 533
- twisted-pair cabling, 290**
 - crosstalk, 291-292
 - wiretapping, 293
- Twofish, 489**
- typosquatting, 27**
- Tzu, Sun, 2**

U

- UAC (User Account Control), 140, 383-384**
- UAV (Unmanned Aerial Vehicles), facilities security, 601**
- UDP (User Datagram Protocol)**
 - flood attacks, 227
 - ports, 217-221
- UEFI (Unified Extensible Firmware Interface), updates, 108**
- UEFI/BIOS, malware and unsavable computers, 40**
- unauthorized access, 6**
- unauthorized zone transfers, DNS servers, 237, 241**
- unicast IPv6 addresses, 181**
- uninstalling. *See also* installing**
 - applications, 36, 90-91
 - services, 90-91
- Unix**
 - tcpdump packet analyzer, 443
 - vulnerability scanning, 414

**unnecessary applications/services,
removing, 90-91****unsavable computers, malware, 40****updates**

anti-malware, 8, 108

BIOS, 108

browsers, 128, 135

critical updates, 98

driver updates, 99

firewalls, 108

OS hardening, 98-99, 108

security updates, 98

service packs, 98

UEFI, 108

virtualization, 115

Windows Update

*OS hardening, 98-99**preventing/troubleshooting viruses, 31***UPS (Uninterruptible Power Supplies),
108, 551-552****uptime (generators), 554****URI (Uniform Resource Identifiers),
spoofing attacks, 231****URL (Uniform Resource Locators)**

hijacking, 27

spoofing attacks, 231

**US-CERT (U.S. Computer Emergency
Readiness Team), mobile device secu-
rity, 67****USB devices**

encryption, 63

flash drives, malware delivery, 27

use case analysis, 634**users**

access control

*Account Expiration dates, 370**ADUC, 369**group access control, 371**multiple user accounts, 371**time-of-day restrictions, 370*

access recertification, 374

Account Expiration dates, 370

ADUC, 369

applications, trusting user input, 147

authentication, 7

awareness training, 7, 621-622

clean desk policy, 592

educating, 591-593, 621-622

first responders (incident response proce-
dures), 629

groups, access control, 371

malware delivery, 27

multiple user accounts, 371

offboarding, 620

onboarding, 620, 623

passwords, 376-377

personal security policies, 617

*AUP, 618, 622**awareness training, 621-622**change management policies, 619, 622**due care policies, 621-623**due diligence, infrastructure security,
621-623**due process policies, 621-623**mandatory vacations, 620-622**offboarding, 620**onboarding, 620, 623**privacy policies, 618**separation of duties/job rotation policies,
619, 622**user education, 621-622*

PII, 616-617, 622

privilege creep, 374

safety, 324

time-of-day restrictions, 370

training, 7, 591-593, 621-622

UAC, 140, 383-384

usernames, 376-377

vacations, 620-622

verifying identification. *See* authentication
vetting, 592

UTM (Unified Threat Management), 272

UTP (Unshielded Twisted-Pair) cabling, 292

V

V-shaped model (SDLC), 145

V2 cards, SIM cloning, 69

vacations (mandatory), 620-622

validation

CA, 525

certificates, 525

DV certificates, 522

EV certificates, 522

identity validation, 322

input validation, 150-151

OV certificates, 522

vehicles, facilities security

air gaps, 600-601

CAN, 600

drones, 601

locking systems, 601

UAV, 601

Wi-Fi, 601

vendor policies

BPA, 623-624

ISA, 624

MoU, 624

SLA, 623-624

verifying

attestation, BIOS, 62

certificates with RA, 527

user identity. *See* authentication

VeriSign certificates, 72, 525

Verisys, 57

Vernam ciphers. *See* one-time pads

vertical privilege escalation, 288

vetting employees, 592

video

exam preparation, 648

incident response procedures, 631

record time offset, 631

video surveillance, physical security, 323

virtualization. *See also* VM (Virtual Machines)

application containerization, 112

definition of, 109

emulators, 111

hardware, disabling, 115

Hyper-V, 114

hypervisors, 111-112

network security, 115

updates, 115

virtual appliances, 111

virtual escape protection, 115

virtualization sprawl, 114

viruses

armored viruses, 21

boot sector viruses, 20, 34

definition of, 25

encrypted viruses, 20

Love Bug virus, 25

macro viruses, 20

metamorphic viruses, 21

multipartite viruses, 21

polymorphic viruses, 20

preventing/troubleshooting, 41

antivirus software, 31, 34

encryption, 33

Linux-based tools, 35

Windows Firewall, 31

Windows Update, 31

program viruses, 20

stealth viruses, 21

symptoms of, 33-34

virus hoaxes, 21

vishing, 586, 590

VLAN (Virtual Local Area Networks), 188

MAC flooding, 189

VLAN hopping, 189

VM (Virtual Machines), 110, 570

disk files, 114

monitoring, 115

preventing/troubleshooting spyware, 36

process VM, 111

securing, 113-114

security, 115

system VM, 111

virtualization sprawl, 114

virtual machine escape, 113

VMM (Virtual Machine Manager).*See* hypervisors**voice recognition software, 327****VoIP (Voice over Internet Protocol),
network design, 191****VPN (Virtual Private Networks)**

always-on VPN, 342

GRE, 342

illustration of, 340

L2TP, 340-342, 534

on-demand VPN, 535

PPTP, 340-342, 533

RRAS, 341

secure VPN connectivity, routers, 179

split tunneling, 342

VPN concentrators, 342

WAP, 300

vulnerabilities

assessing, 406, 410

*definition of vulnerabilities, 396**IT security frameworks, 635**network mapping, 411-412**network sniffers, 415-417**password analysis, 417-420**vulnerability scanning, 412-414*

browsers, 128

CVE, 200-201

definition, 396

managing

*general vulnerabilities/basic prevention**methods table, 409-410**OSVAL, 408-409**penetration testing, 407-408**process of, 405-406*

programming vulnerabilities/attacks

*arbitrary code execution, 155**backdoor attacks, 22, 29, 153, 159**buffer overflows, 153, 159**code injections, 156-159**directory traversals, 158-159**DLL injections, 158**integer overflows, 154**LDAP injections, 157**memory leaks, 154**NoSQL injections, 157**null pointer dereferences, 154**RCE, 155, 159**SQL injections, 156**XML injections, 157**XSRF, 156, 159**XSS, 156, 159**zero day attacks, 158-159*

scanning, 412-414

W**WAN (Wide Area Networks)**

LAN versus, 183

routers, 178

WAP (Wireless Access Points)

ad hoc networks, 299-300

administration interface, 295-296

AP isolation, 303

brute-force attacks, 299, 305

encryption, 297-299, 303

- evil twins, 297
- firewalls, 302
- MAC filtering, 302
- placement of, 300
- PSK, 298
- rogue AP, 296
- SSID, 296
- VPN, 300
- wireless network security, 295-305
- wireless point-to-multipoint layouts, 301
- WLAN controllers, 303
- WPS, 299
- war-chalking, 304**
- war-dialing, 190, 587**
- war-driving, 304**
- warm sites, 561**
- waterfall model (SDLC), 145**
- watering hole attacks, 234, 240, 589-591**
- web application firewalls, 262**
- web-based SSO (Single Sign-On), 329**
- web browsers**
 - automatically updating, 128
 - choosing, 127-128
 - company requirements, 128
 - functionality, 129
 - HTTP connections, 71
 - HTTPS connections, 71-72
 - MITB attacks, 233-234, 240
 - OS, determining, 128
 - PAC files, 263
 - pop-up blockers, 53, 57-59
 - preventing/troubleshooting spyware, 35
 - recommendations, 127-128
 - security
 - ad-blocking, 135*
 - add-ons, 137-138*
 - advanced security settings, 138-139*
 - content filtering, 133-134*
 - cookies, 136-137*
 - LSO, 137*
 - mobile devices, 135*
 - passwords, 139*
 - policy implementation, 129-131*
 - pop-up blocking, 135*
 - proxy servers, 133-134*
 - security zones, 135*
 - temporary files, 138*
 - updates, 135*
 - user training, 133*
 - updates, 128, 135
 - vulnerabilities/fixes, 128
- web of trust, defining, 529**
- web proxies. See proxy servers**
- web resources, exam preparation, 649**
- web security gateways, 265**
- web servers**
 - exploit kits, 27
 - security, 200-202
- web shells, FTP servers, 202-203**
- websites**
 - cold sites, 561
 - exam preparation, 649
 - hot sites, 561
 - HTTP connections, 71
 - HTTPS connections, 71-72
 - input validation, 150-151
 - malware delivery, 27
 - pop-up blockers, 53, 57-59
 - redundancy planning, 561
 - typosquatting, 27
 - URL hijacking, 27
 - warm sites, 561
- WEP (Wired Equivalent Privacy) protocol, 298**
- wet pipe sprinkler systems, 595**
- whaling, 586, 590**
- white-box testing, 149**
- white hats, 9**

whitelists

- applications, 73, 92
- OS hardening, 92
- preventing/troubleshooting spam, 40
- services, 92

whole disk encryption, 108**WIC (WAN Interface Cards), 179****WiDi (Wi-Fi Direct), 66****WIDS (Wireless Intrusion Detection Systems), 272****Wi-Fi, 77**

- bluejacking, 69
- bluesnarfing, 69
- disassociation attacks, 305
- facilities security, 601
- vehicle security, 601
- vulnerabilities, 70

wildcard certificates, 523**Windows**

- analytical monitoring
 - net file command*, 446
 - netstat command*, 446
 - openfiles command*, 445
- Computer Management, 445
- Group Policies, accessing, 103-104
- hotfixes, 100
- OS hardening, starting/stopping services, 95-97
- patch management, 101-102
- Performance Monitor, 445

Windows 7, Internet Explorer Maintenance Security, 131**Windows 10**

- Internet Explorer Maintenance Security, 130-131
- Local Group Policy, browser security, 129

Windows BitLocker, 63**Windows Defender, preventing/troubleshooting spyware, 35****Windows Firewall, 31, 54****Windows Programs and Features window, OS hardening, 91****Windows Server**

- domain controller-managed IE policies, 131-132
- Import Policy From window, 104
- network shares, 457
- security templates, 104

Windows Update, 31, 98-99**Windows XP**

- OS hardening, 94
- Solitaire, Easter eggs, 30

WinDump, 443**WinPcap**

- WinDump, 443
- Wireshark installation, 441

WIPS (Wireless Intrusion Prevention Systems), 272**wired network/device security, 285**

- backdoors, 288-289
- cabling
 - crosstalk*, 291-292
 - data emanation*, 292-294
 - interference*, 290-291
 - PDS*, 295
 - wire closets*, 294
 - wiretapping*, 293-294
- default accounts, 286
- network attacks, 289
- passwords, 286-287
- privilege escalation, 287-288
- remote ports, 289
- Telnet, 289

wireless networks, 77

- Bluetooth, 306
 - AP*, 306
 - bluejacking*, 69, 306
 - bluesnarfing*, 69, 306-307
 - frequency hopping*, 306

- cellular networks, 308
- documenting network design, 309
- facilities security, 601
- geofences, 308
- GPS, 308
- NFC, 306-307
- RFID, 307
- SATCOM, 308
- third-party wireless adapter connections, 296
- vehicle security, 601
- vulnerabilities, 70
- WAP
 - ad hoc networks*, 299-300
 - administration interface*, 295-296
 - AP isolation*, 303
 - brute-force attacks*, 299, 305
 - encryption*, 297-299, 303
 - evil twins*, 297
 - firewalls*, 302
 - MAC filtering*, 302
 - placement of*, 300
 - PSK*, 298
 - rogue AP*, 296
 - SSID*, 296
 - VPN*, 300
 - wireless point-to-multipoint layouts*, 301
 - wireless site surveys*, 302
 - WLAN controllers*, 303
 - WPS*, 299
- wireless protocols, 298
- wireless transmission vulnerabilities
 - brute-force attacks*, 305
 - IV attacks*, 304
 - spoofed MAC addresses*, 305
 - war-chalking*, 304
 - war-driving*, 304
 - Wi-Fi disassociation attacks*, 305

- wireless peripherals, 66
- wireless signal jammers, 302
- wireless site surveys, 302
- Wireshark, 415-417, 441-442
- wiretapping, 293-294
- wiring closets, 294
- witness statements, incident response procedures, 631
- WLAN (Wireless Local Area Networks)
 - AP, 306
 - bridges, 178
- WLAN controllers, WAP, 303
- Word (MS), securing, 143
- worms
 - definition of, 25
 - Nimda, 21
 - Nimda worm, 25
 - preventing/troubleshooting, 35, 41
- WPA (Wi-Fi Protected Access) protocol, 298
- WPA2 (Wi-Fi Protected Access version 2) protocol, 298
- WPS (Wi-Fi Protected Setup), WAP, 299
- wraps, integer overflows, 154
- WTLS (Wireless Transport Layer Security) protocol, 298-299
- WWN (World Wide Names), spoofing attacks, 232

X - Y - Z

- X.509 standard, certificates and, 522
- XaaS (Anything as a Service), 194
- Xmas attacks, 228
- XML injections, 157
- XSRF (Cross-Site Request Forgery), 156, 159
- XSS (Cross-Site Scripting), 137, 156, 159, 234

zero day attacks, 158-159

ZeroAccess botnet, 28

Zimmerman, Philip, 495

zip files, malware delivery, 26

zombies, malware delivery, 28

zone transfers, 237, 241, 258

ZoneAlarm, 54