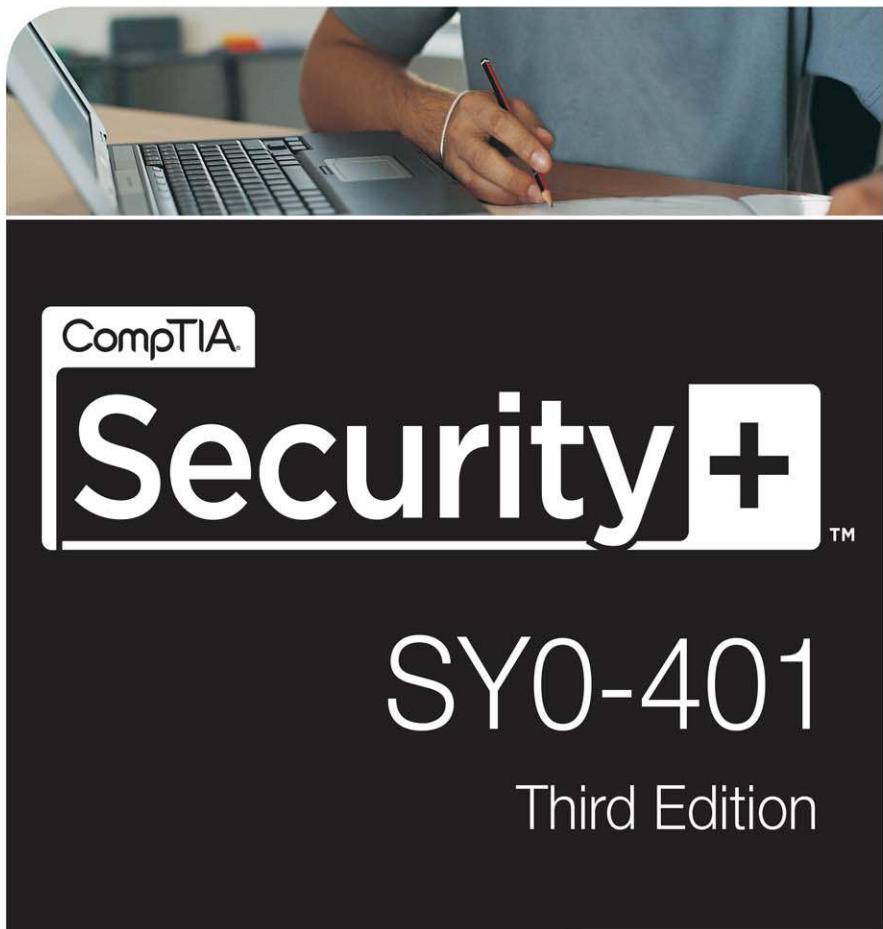


DAVID L. PROWSE



Authorized Cert Guide

Learn, prepare, and practice for exam success



PEARSON IT
CERTIFICATION

From the Library of Kingfisher NET+

CompTIA® Security+ SY0-401 Cert Guide, Deluxe Edition

Third Edition

David L. Prowse

PEARSON

800 East 96th Street,
Indianapolis, Indiana 46240 USA

CompTIA® Security+ SY0-401 Cert Guide, Deluxe Edition, Third Edition

Copyright © 2015 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: 978-0-7897-5333-5

ISBN-10: 0-7897-5333-2

Library of Congress Control Number: 2014941826

Printed in the United States of America

Third Printing: November 2014

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.

Windows is a registered trademark of 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 or from the use of the CD or programs accompanying it.

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 international@pearsoned.com.

Associate Publisher

Dave Dusthimer

Acquisitions Editor

Betsy Brown

Development Editor

Andrew Cupp

Managing Editor

Sandra Schroeder

Project Editor

Mandie Frank

Copy Editor

Bill McManus

Indexer

Lisa Stumpf

Proofreader

The Wordsmithery LLC

Technical Editors

Chris Crayton

Aubrey Adams

Publishing Coordinator

Vanessa Evans

Multimedia Developer

Lisa Matthews

Designer

Alan Clements

Composition

Mary Sudul

Contents at a Glance

Introduction	xxii
CHAPTER 1	Introduction to Security 3
CHAPTER 2	Computer Systems Security 17
CHAPTER 3	OS Hardening and Virtualization 83
CHAPTER 4	Application Security 127
CHAPTER 5	Network Design Elements 179
CHAPTER 6	Networking Protocols and Threats 225
CHAPTER 7	Network Perimeter Security 267
CHAPTER 8	Securing Network Media and Devices 299
CHAPTER 9	Physical Security and Authentication Models 339
CHAPTER 10	Access Control Methods and Models 383
CHAPTER 11	Vulnerability and Risk Assessment 423
CHAPTER 12	Monitoring and Auditing 465
CHAPTER 13	Encryption and Hashing Concepts 507
CHAPTER 14	PKI and Encryption Protocols 551
CHAPTER 15	Redundancy and Disaster Recovery 575
CHAPTER 16	Policies, Procedures, and People 611
CHAPTER 17	Taking the Real Exam 663
PRACTICE EXAM 1 SY0-401	673
Glossary	725
Index	749

On the DVD:

APPENDIX A View Recommended Resources

APPENDIX B Master List of Key Topics

Acronyms

Case Studies

Case Study Solutions (Video and Simulations)

Table 6-2

Table of Contents

	Introduction	xxii
Chapter 1	Introduction to Security	3
	Foundation Topics	3
	Security 101	3
	The CIA of Computer Security	3
	The Basics of Information Security	5
	Think Like a Hacker	8
	Chapter Review Activities	10
	Review Key Topics	10
	Define Key Terms	11
	Review Questions	11
	Answers and Explanations	13
Chapter 2	Computer Systems Security	17
	Foundation Topics	17
	Computer Systems Security Threats	17
	Malicious Software	18
	<i>Viruses</i>	18
	<i>Worms</i>	19
	<i>Trojan Horses</i>	20
	<i>Ransomware</i>	20
	<i>Spyware</i>	21
	<i>Rootkits</i>	22
	<i>Spam</i>	22
	<i>Summary of Malware Threats</i>	23
	Ways to Deliver Malicious Software	24
	<i>Via Software, Messaging, and Media</i>	24
	<i>Botnets and Zombies</i>	25
	<i>Active Interception</i>	26
	<i>Privilege Escalation</i>	26
	<i>Backdoors</i>	26
	<i>Logic Bombs</i>	27
	Preventing and Troubleshooting Malware	28
	<i>Preventing and Troubleshooting Viruses</i>	28
	<i>Preventing and Troubleshooting Worms and Trojans</i>	32
	<i>Preventing and Troubleshooting Spyware</i>	33
	<i>Preventing and Troubleshooting Rootkits</i>	35
	<i>Preventing and Troubleshooting Spam</i>	36
	<i>You Can't Save Every Computer from Malware!</i>	38
	<i>Summary of Malware Prevention Techniques</i>	38

Implementing Security Applications	39
Personal Software Firewalls	39
Host-Based Intrusion Detection Systems	41
Pop-Up Blockers	43
Data Loss Prevention Systems	45
Securing Computer Hardware, Peripherals, and Mobile Devices	45
Securing the BIOS	46
Securing Storage Devices	47
<i>Removable Storage</i>	47
<i>Network Attached Storage</i>	48
<i>Whole Disk Encryption</i>	48
<i>Hardware Security Modules</i>	50
Securing Mobile Devices	50
<i>Malware</i>	51
<i>Botnet Activity</i>	52
<i>SIM Cloning</i>	52
<i>Wireless Attacks</i>	53
<i>Theft</i>	53
<i>Application Security</i>	54
<i>BYOD Concerns</i>	57
Chapter Summary	60

Chapter Review Activities	62
Review Key Topics	62
Define Key Terms	62
Review Questions	63

Answers and Explanations	71
Case Studies for Chapter 2	77
Case Study Solutions	79

Chapter 3 OS Hardening and Virtualization 83

Foundation Topics	83
Hardening Operating Systems	83
Removing Unnecessary Applications and Services	84
Service Packs	92
Windows Update, Patches, and Hotfixes	95
<i>Patches and Hotfixes</i>	96
<i>Patch Management</i>	99
Group Policies, Security Templates, and Configuration Baselines	100
Hardening File Systems and Hard Drives	103
Virtualization Technology	107
Types of Virtualization and Their Purposes	107
Hypervisor	109
Securing Virtual Machines	110
Chapter Summary	112

Chapter Review Activities	113
Review Key Topics	113
Define Key Terms	114
Review Questions	114
Answers and Explanations	118
Case Studies for Chapter 3	121
Case Study Solutions	123

Chapter 4 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>	132
<i>Use a Proxy and Content Filter</i>	133
<i>Secure Against Malicious Code</i>	135
Securing Internet Explorer	135
Securing Firefox	141
Securing Other Browsers	145
Securing Other Applications	147
Secure Programming	151
Systems Development Life Cycle	151
Programming Testing Methods	154
Programming Vulnerabilities and Attacks	156
<i>Backdoors</i>	157
<i>Buffer Overflows</i>	157
<i>Arbitrary Code Execution/Remote Code Execution</i>	158
<i>XSS and XSRF</i>	159
<i>More Code Injection Examples</i>	159
<i>Directory Traversal</i>	161
<i>Zero Day Attack</i>	161
Chapter Summary	163
Chapter Review Activities	164
Review Key Topics	164
Define Key Terms	165
Review Questions	165
Answers and Explanations	170
Case Studies for Chapter 4	174
Case Study Solutions	175

Chapter 5 Network Design Elements 179

Foundation Topics	179
Network Design	179
The OSI Model	180

Network Devices	182
<i>Hub</i>	182
<i>Switch</i>	182
<i>Router</i>	184
Network Address Translation, and Private Versus Public IP	185
Network Zones and Interconnections	188
<i>LAN Versus WAN</i>	188
<i>Internet</i>	189
<i>Demilitarized Zone (DMZ)</i>	189
<i>Intranets and Extranets</i>	190
Network Access Control (NAC)	192
Subnetting	192
Virtual Local Area Network (VLAN)	194
Telephony Devices	196
<i>Modems</i>	196
<i>PBX Equipment</i>	197
<i>VoIP</i>	197
Cloud Security and Server Defense	198
Cloud Computing	198
Cloud Security	200
Server Defense	203
<i>File Servers</i>	203
<i>Network Controllers</i>	204
<i>E-mail Servers</i>	204
<i>Web Servers</i>	205
<i>FTP Server</i>	207
Chapter Summary	208
Chapter Review Activities	210
Review Key Topics	210
Define Key Terms	210
Review Questions	210
Answers and Explanations	215
Case Studies for Chapter 5	219
Case Study Solutions	220
Chapter 6 Networking Protocols and Threats	225
Foundation Topics	225
Ports and Protocols	225
Ports Ranges, Inbound Versus Outbound, and Common Ports	225
Protocols That Can Cause Anxiety on the Exam	235
Malicious Attacks	236
DoS	236
DDoS	239
Sinkholes and Blackholes	239

Spoofing 240
Session Hijacking 241
Replay 243
Null Sessions 244
Transitive Access and Client-Side Attacks 244
DNS Poisoning and Other DNS Attacks 245
ARP Poisoning 247
Summary of Network Attacks 247

Chapter Summary 251

Chapter Review Activities 252
Review Key Topics 252
Define Key Terms 252
Review Questions 252

Answers and Explanations 258
Case Studies for Chapter 6 262
Case Study Solutions 263

Chapter 7 Network Perimeter Security 267

Foundation Topics 268
Firewalls and Network Security 268
Firewalls 268
Proxy Servers 274
Honeypots and Honeynets 277
Data Loss Prevention (DLP) 278

NIDS Versus NIPS 279
NIDS 279
NIPS 280
Summary of NIDS Versus NIPS 282
The Protocol Analyzer's Role in NIDS and NIPS 282
Unified Threat Management 283

Chapter Summary 283

Chapter Review Activities 284
Review Key Topics 284
Define Key Terms 285
Review Questions 285

Answers and Explanations 290
Case Studies for Chapter 7 294
Case Study Solutions 295

Chapter 8 Securing Network Media and Devices 299

Foundation Topics 299
Securing Wired Networks and Devices 299
Network Device Vulnerabilities 300
Default Accounts 300

<i>Weak Passwords</i>	300
<i>Privilege Escalation</i>	302
<i>Back Doors</i>	303
<i>Network Attacks</i>	303
<i>Other Network Device Considerations</i>	303
Cable Media Vulnerabilities	304
<i>Interference</i>	305
<i>Crosstalk</i>	305
<i>Data Emanation</i>	306
<i>Tapping into Data and Conversations</i>	307
Securing Wireless Networks	309
Wireless Access Point Vulnerabilities	309
<i>The Administration Interface</i>	310
<i>SSID Broadcast</i>	310
<i>Rogue Access Points</i>	311
<i>Evil Twin</i>	311
<i>Weak Encryption</i>	311
<i>Wi-Fi Protected Setup</i>	313
<i>VPN over Open Wireless</i>	314
<i>Wireless Access Point Security Strategies</i>	314
Wireless Transmission Vulnerabilities	317
Bluetooth Vulnerabilities	318
<i>Bluejacking</i>	319
<i>Bluesnarfing</i>	319
Chapter Summary	321
Chapter Review Activities	323
Review Key Topics	323
Define Key Terms	323
Review Questions	324
Answers and Explanations	328
Case Studies for Chapter 8	330
Case Study Solutions	333
Chapter 9 Physical Security and Authentication Models	339
Foundation Topics	340
Physical Security	340
General Building and Server Room Security	340
Door Access	342
Biometric Readers	344
Authentication Models and Components	345
Authentication Models	345
Localized Authentication Technologies	348
802.1X and EAP	348
LDAP	351

<i>Kerberos and Mutual Authentication</i>	352
<i>Remote Desktop Services</i>	354
Remote Authentication Technologies	356
<i>Remote Access Service</i>	356
<i>Virtual Private Networks</i>	358
<i>RADIUS Versus TACACS</i>	360

Chapter Summary 362

Chapter Review Activities 363

Review Key Topics	363
Define Key Terms	364
Review Questions	365
Answers and Explanations	372
Case Studies for Chapter 9	376
Case Study Solutions	379

Chapter 10 Access Control Methods and Models 383

Foundation Topics 383

Access Control Models Defined 383

Discretionary Access Control	384
Mandatory Access Control	386
Role-Based Access Control (RBAC)	387
Access Control Wise Practices	388

Rights, Permissions, and Policies 391

Users, Groups, and Permissions	391
Permission Inheritance and Propagation	396
Moving and Copying Folders and Files	397
Usernames and Passwords	397
Policies	400
User Account Control (UAC)	403

Chapter Summary 404

Chapter Review Activities 405

Review Key Topics	405
Define Key Terms	406
Review Questions	406
Answers and Explanations	412
Case Studies for Chapter 10	416
Case Study Solutions	417

Chapter 11 Vulnerability and Risk Assessment 423

Foundation Topics 423

Conducting Risk Assessments 423

Qualitative Risk Assessment	425
Quantitative Risk Assessment	426

Security Analysis Methodologies	429
Security Controls	430
Vulnerability Management	431
<i>Penetration Testing</i>	433
<i>OVAL</i>	434
Assessing Vulnerability with Security Tools	435
Network Mapping	435
Vulnerability Scanning	438
Network Sniffing	441
Password Analysis	443
Chapter Summary	446
Chapter Review Activities	447
Review Key Topics	447
Define Key Terms	448
Review Questions	448
Answers and Explanations	454
Case Studies for Chapter 11	459
Case Study Solutions	460
Chapter 12 Monitoring and Auditing	465
Foundation Topics	465
Monitoring Methodologies	465
Signature-Based Monitoring	466
Anomaly-Based Monitoring	466
Behavior-Based Monitoring	467
Using Tools to Monitor Systems and Networks	467
Performance Baseling	468
Protocol Analyzers	470
<i>Wireshark</i>	471
<i>Network Monitor</i>	472
<i>SNMP</i>	474
Analytical Tools	475
Conducting Audits	478
Auditing Files	478
Logging	481
Log File Maintenance and Security	485
Auditing System Security Settings	486
Chapter Summary	490
Chapter Review Activities	491
Review Key Topics	491
Define Key Terms	492
Review Questions	492
Answers and Explanations	498

Case Studies for Chapter 12 503
Case Study Solutions 504

Chapter 13 Encryption and Hashing Concepts 507

Foundation Topics 507
Cryptography Concepts 507
 Symmetric Versus Asymmetric Key Algorithms 512
 Symmetric Key Algorithms 512
 Asymmetric Key Algorithms 513
 Public Key Cryptography 513
 Key Management 515
 Steganography 515
Encryption Algorithms 516
 DES and 3DES 516
 AES 517
 RC 518
 Blowfish and Twofish 518
 Summary of Symmetric Algorithms 519
 RSA 519
 Diffie-Hellman 521
 Elliptic Curve 521
 More Encryption Types 523
 One-Time Pad 523
 PGP 524
Hashing Basics 526
 Cryptographic Hash Functions 527
 MD5 527
 SHA 527
 RIPEMD and HMAC 528
 Happy Birthday! 528
 LANMAN, NTLM, and NTLMv2 529
 LANMAN 529
 NTLM and NTLMv2 531
 Additional Password Hashing Concepts 531
Chapter Summary 533
Chapter Review Activities 534
 Review Key Topics 534
 Define Key Terms 535
 Review Questions 535
 Answers and Explanations 542
 Case Studies for Chapter 13 546
 Case Study Solutions 547

Chapter 14 PKI and Encryption Protocols 551

Foundation Topics	551
Public Key Infrastructure	551
Certificates	552
Certificate Authorities	552
Single-Sided and Dual-Sided Certificates	556
Web of Trust	556
Security Protocols	557
S/MIME	557
SSL/TLS	558
SSH	559
PPTP, L2TP, and IPsec	560
<i>PPTP</i>	560
<i>L2TP</i>	560
<i>IPsec</i>	561
Chapter Summary	561
Chapter Review Activities	562
Review Key Topics	562
Define Key Terms	563
Review Questions	563
Answers and Explanations	568
Case Studies for Chapter 14	571
Case Study Solutions	571

Chapter 15 Redundancy and Disaster Recovery 575

Foundation Topics	575
Redundancy Planning	575
Redundant Power	577
<i>Redundant Power Supplies</i>	579
<i>Uninterruptible Power Supplies</i>	579
<i>Backup Generators</i>	581
Redundant Data	582
Redundant Networking	586
Redundant Servers	587
Redundant Sites	588
Redundant People	589
Disaster Recovery Planning and Procedures	590
Data Backup	590
DR Planning	594
Chapter Summary	598
Chapter Review Activities	598
Review Key Topics	598

Define Key Terms	599
Review Questions	599
Answers and Explanations	604
Case Study for Chapter 15	607
Case Study Solution	607
Chapter 16 Policies, Procedures, and People	611
Foundation Topics	611
Environmental Controls	611
Fire Suppression	611
<i>Fire Extinguishers</i>	612
<i>Sprinkler Systems</i>	613
<i>Special Hazard Protection Systems</i>	614
HVAC	615
Shielding	616
Social Engineering	617
Pretexting	618
Malicious Insider	618
Diversion Theft	619
Phishing	619
Hoaxes	621
Shoulder Surfing	621
Eavesdropping	622
Dumpster Diving	622
Baiting	622
Piggybacking/Tailgating	622
Summary of Social Engineering Types	623
User Education and Awareness	624
Legislative and Organizational Policies	625
Data Sensitivity and Classification of Information	626
Personnel Security Policies	628
<i>Privacy Policies</i>	628
<i>Acceptable Use</i>	629
<i>Change Management</i>	629
<i>Separation of Duties/Job Rotation</i>	630
<i>Mandatory Vacations</i>	630
<i>Onboarding and Offboarding</i>	631
<i>Due Diligence</i>	631
<i>Due Care</i>	631
<i>Due Process</i>	632
<i>User Education and Awareness Training</i>	632
<i>Summary of Personnel Security Policies</i>	633
How to Deal with Vendors	633

How to Dispose of Computers and Other IT Equipment Securely	634
Incident Response Procedures	636
Chapter Summary	642
Chapter Review Activities	643
Review Key Topics	643
Review Questions	644
Answers and Explanations	653
Case Studies for Chapter 16	658
Case Study Solutions	659
Chapter 17 Taking the Real Exam	663
Getting Ready and the Exam Preparation Checklist	663
Tips for Taking the Real Exam	667
Beyond the CompTIA Security+ Certification	670
Case Study for Chapter 17	671
Case Study 17-1: Analyzing Test Questions	671
Practice Exam 1: SY0-401	673
Answers to Practice Exam 1	694
Glossary	725
Index	749

On the DVD:**APPENDIX A View Recommended Resources****APPENDIX B Master List of Key Topics****Acronyms****Case Studies****Case Study Solutions (Video and Simulations)****Table 6-2**

About the Author

David L. Prowse is an author, a computer network specialist, and a technical trainer. Over the past several years he has authored several titles for Pearson Education, including the well-received *CompTIA A+ Exam Cram*. As a consultant, he installs and secures the latest in computer and networking technology. Over the past decade he has also taught CompTIA A+, Network+, and Security+ certification courses, both in the classroom and via the Internet.

He runs the website www.davidlprowse.com, where he gladly answers questions from students and readers.

Dedication

This book is dedicated to James. Your little smiling face invigorates me as I write, especially in the wee hours of the morning.

Acknowledgments

I'd like to acknowledge Dave Dushtimer and Betsy Brown for giving me the opportunity to write this book. I am honored to have your support and trust.

Special thanks go to Andrew Cupp, Chris Crayton, Aubrey Adams, Lisa Matthews, Mandie Frank, and all of the other people at Pearson (and beyond) that helped make this book a reality. I appreciate everything you do!

Ultimately, the support of one's family is the most important factor when inscribing any tome. My colossal appreciation is second only to the encouragement and support I receive from my family.

About the Reviewers

Chris Crayton (MCSE) is an author, technical consultant, and trainer. Formerly, he 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 of the 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.

Aubrey Adams is an IT networking and data communications lecturer, and Cisco Networking Academy instructor, at Central Institute of Technology, and at Murdoch University, in Perth, Western Australia. With a background in telecommunications design, Aubrey has qualifications in electronic engineering and management, and graduate diplomas in computing and education. He teaches across a broad range of related vocational and education training areas. Since 2007 Aubrey has technically reviewed a number of Pearson Education and Cisco Press publications, including video, simulation, and online projects.

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

Visit our website and register this book at www.pearsonitcertification.com/title/9780789753335 for convenient access to any updates, downloads, or errata that might be available for this book.

CompTIA

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill.

Certification demonstrates that you have the knowledge and skill to solve technical or business problems in virtually any business environment. CompTIA certifications are highly-valued credentials that qualify you for jobs, increased compensation, and promotion.



Certification Helps Your Career



- **Security is one of the highest demand job categories**—growing in importance as the frequency and severity of security threats continues to be a major concern for organizations around the world.
- **Jobs for security administrators are expected to increase by 18%**—the skill set required for these types of jobs maps to the CompTIA Security+ certification.
- **Network Security Administrators**—can earn as much as \$106,000 per year.
- **CompTIA Security+** is the first step—in starting your career as a Network Security Administrator or Systems Security Administrator.
- **More than 1/4 million**—individuals worldwide are CompTIA Security+ certified.
- **CompTIA Security+ is regularly used in organizations**—such as Hitachi Systems, Fuji Xerox, HP, Dell, and a variety of major U.S. government contractors.
- **Approved by the U.S. Department of Defense (DoD)**—as one of the required certification options in the DoD 8570.01-M directive, for Information Assurance Technical Level II and Management Level I job roles.

Steps to Getting Certified and Staying Certified

Review Exam Objectives

Review the Certification objectives to make sure you know what is covered in the exam.<http://certification.comptia.org/examobjectives.aspx>

Practice for the Exam

After you have studied for the certification, review and answer the sample questions to get an idea what type of questions might be on the exam.<http://certification.comptia.org/samplequestions.aspx>

Purchase an Exam Voucher

Purchase exam vouchers on the CompTIA Marketplace. www.comptiastore.com

Take the Test!

Go to the Pearson VUE website and schedule a time to take your exam. <http://www.pearsonvue.com/comptia/>

Stay Certified!

Effective January 1, 2011, new CompTIA Security+ certifications are valid for three years from the date of certification. There are a number of ways the certification can be renewed. For more information go to: <http://certification.comptia.org/ce>

Continuing Education

How to obtain more information

- Visit CompTIA online—<http://certification.comptia.org/home.aspx> to learn more about getting CompTIA certified.
- Contact CompTIA—call 866-835-8020 and choose Option 2 or email questions@comptia.org.
- Connect with us—



Introduction

Welcome to the *CompTIA Security+ SY0-401 Cert Guide, Deluxe Edition*. 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. On my site you will also find videos, articles, bonus test questions, and other additional content. And of course, you can contact me directly from my website to ask me questions about the book. You can reach the Security+ page of my website directly at the following link: www.SY0-401.com

Or, go to my home page at the following link: www.davidlprowse.com

Goals and Methods

The number one goal of this book is to help you pass the SY0-401 version of the CompTIA Security+ Certification Exam. To that effect, I have filled this book and DVD with more than 700 questions/answers and explanations in total, including three 100-question practice exams. One of the three exams is printed at the end of the book, and all three exams are located on the disc in a custom simulated 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; it also lists the corresponding CompTIA Security+ objective numbers.
- **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.
- **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.
- **Case Studies:** At the end of each chapter are case studies. These offer the reader real-world scenarios with problems that must be solved. The questions are often open-ended, and can have several different solutions. The book gives one or more possible solutions and then points to video-based solutions and simulation exercises on the disc to further reinforce the concepts.

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 IT 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 technical networking experience with an emphasis on security. The CompTIA Network+ certification is also recommended as a prerequisite. 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.

Important! If you do not feel that you have the required experience, have never attempted to secure a computer or network, or are new to the IT field, I recommend considering an IT course that covers the CompTIA Security+ objectives. You can choose from plenty of technical training schools, community colleges, and online courses. Use this book with the course and any other course materials you obtain.

CompTIA Security+ Exam Topics

Table I-1 lists the exam topics for the CompTIA Security+ exam. This table lists the chapter in which each exam topic is covered. Chapter 1 is an introductory chapter and as such does not map to any specific exam objectives. Chapter 17 gives strategies for taking the exam and does not map to any specific objectives either.

Table I-1 CompTIA Security+ Exam Topics

Chapter	Exam Topic	CompTIA Security+ Exam Objectives Covered
1	Security 101 Think Like a Hacker	n/a
2	Computer Systems Security Threats Implementing Security Applications Securing Computer Hardware, Peripherals, and Mobile Devices	Objectives 2.1, 2.3, 3.1, 3.2, 4.2, 4.3
3	Hardening Operating Systems Virtualization Technology	Objectives 3.6, 4.1, 4.3

Chapter	Exam Topic	CompTIA Security+ Exam Objectives Covered
4	Securing the Browser Securing Other Applications Secure Programming	Objectives 3.5, 4.1, 4.3
5	Network Design Cloud Security and Server Defense	Objectives 1.1, 1.2, 1.3, 4.4
6	Ports and Protocols Malicious Attacks	Objectives 1.2, 1.3, 1.4, 3.2, 3.5
7	Firewalls and Network Security NIDS Versus NIPS	Objectives 1.1, 1.2, 3.6
8	Securing Wired Networks and Devices Securing Wireless Networks	Objectives 1.4, 1.5, 3.4, 6.2
9	Physical Security Authentication Models and Components	Objectives 2.7, 2.9, 3.6, 4.3, 5.1, 5.2
10	Access Control Models Defined Rights, Permissions, and Policies	Objectives 4.4, 5.2, 5.3
11	Conducting Risk Assessments Assessing Vulnerability with Security Tools	Objectives 2.1, 2.2, 2.7, 3.2, 3.7, 3.8, 4.5
12	Monitoring Methodologies Using Tools to Monitor Systems and Networks Conducting Audits	Objectives 2.3, 3.6, 3.7
13	Cryptography Concepts Encryption Algorithms Hashing Basics	Objectives 4.4, 6.1, 6.2
14	Public Key Infrastructure Security Protocols	Objectives 1.4, 6.2, 6.3
15	Redundancy Planning Disaster Recovery Planning and Procedures	Objectives 1.1, 2.8
16	Environmental Controls Social Engineering Legislative and Organizational Policies	Objectives 2.1 through 2.7, 2.9, 3.2, 3.3, 4.2, 4.3, 4.4, 4.5

Chapter	Exam Topic	CompTIA Security+ Exam Objectives Covered
17	Getting Ready and the Exam Preparation Checklist Tips for Taking the Real Exam Beyond the CompTIA Security+ Certification	n/a

Pearson IT Certification Practice Test Engine and Questions on the DVD

The DVD in the back of the book includes the Pearson IT Certification Practice Test engine, software that displays and grades a set of exam-realistic multiple-choice questions. This book comes with three practice exams for use with the Pearson IT Certification Practice Test engine. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode, or take a simulated exam that mimics real exam conditions.

The installation process requires two major steps: installing the software and then activating the exam. The DVD in the back of this book has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam—the database of exam questions—is not on the DVD.

Note The cardboard DVD case in the back of this book includes the DVD and 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.

Install the Software from the DVD

The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows virtual machine, but it was built specifically for the PC platform. The minimum system requirements are as follows:

- Windows XP (SP3), Windows Vista (SP2), Windows 7, or Windows 8
- Microsoft .NET Framework 4.0 Client

- Pentium-class 1-GHz processor (or equivalent)
- 512 MB RAM
- 650 MB disc space plus 50 MB for each downloaded practice exam
- Access to the Internet to register and download exam databases

The software installation process is relatively routine. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, there is no need for you to reinstall the software. Simply launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the DVD sleeve.

The following steps outline the installation process:

- Step 1.** Insert the DVD into your PC.
- Step 2.** The software that automatically runs is the Pearson software to access and use all DVD-based features, including the exam engine and the DVD-only appendices. From the Practice Exam tab, click the option **Install Practice Exam**.
- Step 3.** Respond to the prompts as with any typical software installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the DVD sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please do register when prompted. If you already have a Pearson website login, there is no need to register again. Just use your existing login.

Activate and Download the Practice Exam

After the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process) as follows:

- Step 1.** Start the Pearson IT Certification Practice Test software from the Windows Start menu or from your desktop shortcut icon.
- Step 2.** To activate and download the exam associated with this book, from the My Products or Tools tab, click the **Activate** button.
- Step 3.** At the next screen, enter the Activation Key from the paper inside the cardboard DVD holder in the back of the book. Once entered, click the **Activate** button.
- Step 4.** The activation process will download the practice exam. Click **Next**, and then click **Finish**.

When the activation process is completed, the My Products tab should list your new exam. If you do not see the exam, make sure you have selected the **My Products** tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Open Exam** button.

To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Updating your exams ensures you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson IT Certification Practice Test software, simply click the **Tools** tab and click the **Update Engine** button. You can then ensure you are running the latest version of the software engine.

Activate Other Exams

You need to complete the exam software installation process and the registration process only once. Then, for each new exam, you have to follow only a few steps. For instance, if you buy another new Pearson IT Certification Cert Guide or Cisco Press Official Cert Guide, extract the activation code from the DVD sleeve in the back of that book. From there, all you have to do is start the exam engine (if not still up and running) and perform Steps 2 through 4 from the previous list.

Obtain the Premium Edition

In addition to the free practice exams provided with this book, you can purchase one additional exam with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains an additional full practice exam as well as an eBook (in both PDF and ePUB format). In addition, the Premium Edition title also has remediation for each question to the specific part of the eBook that relates to that question.

Because you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. A coupon code in the DVD sleeve contains a one-time-use code and instructions for where you can purchase the Premium Edition.

To view the Premium Edition product page, go to www.pearsonitcertification.com/title/9780133836509.

This page intentionally left blank



This chapter covers the following subjects:

- **Security 101:** School is in session. This section discusses some of the basic principles of information security such as CIA and AAA, some basic threats, and various ways to mitigate those threats.
- **Think Like a Hacker:** “To know your Enemy, you must become your Enemy” (Sun Tzu). However, sometimes the hacker is your adversary, sometimes not. This section describes the various hats worn in the hacker society.

Welcome! Before we launch into heavy-duty security, I'd like to go over some foundation-level security concepts. I recommend that everyone read this chapter, but if you are a seasoned professional, you might opt to scan or skip it. For those of you new to the IT security field, this chapter (and the rest of the book) acts as the basis of your IT sleuthing career.

It is so important in today's organizations to protect information and information systems from unauthorized access and to prevent the modification, disruption, or destruction of data unless it is approved by the organization. That in a nutshell is **information security**. Companies consider it so important that many IT directors have transformed into full-fledged executives—chief information officer (CIO) or chief technology officer (CTO). But let's not get ahead of ourselves! This book is for persons wanting to embark on, or continue along, the path as a security administrator. Many other names are given to that particular position, but we'll stick with that one for the sake of continuity throughout this book.

This entire book is all about information security; it's about locating risks and vulnerabilities to your information, and eliminating those risks, or at least reducing them to a point acceptable to your organization.

This first chapter talks about some basic fundamental security concepts and teaches you to think like a hacker but act like an administrator.

Let's begin!

Introduction to Security

Foundation Topics

Security 101

The first thing we need to get out of the way is that nothing is ever completely or truly secure. People might give clever definitions of something that could be completely secure, but it is a utopia—something that can be imagined but never achieved. There is always a way around or through any security precaution that we construct.

Now that it's understood that there is no perfect scenario, we can move on to some security basics that can help to build a solid foundation upon which proper mitigating of security risks can begin.

The CIA of Computer Security

No, we're not talking about the acronym associated with national security, but computers can indeed be the victim of covert operations. To defend against the worst, IT people attempt to adhere to three core principles of information security: confidentiality, integrity, and availability. Collectively, these three are known as the CIA triad as illustrated in Figure 1-1.

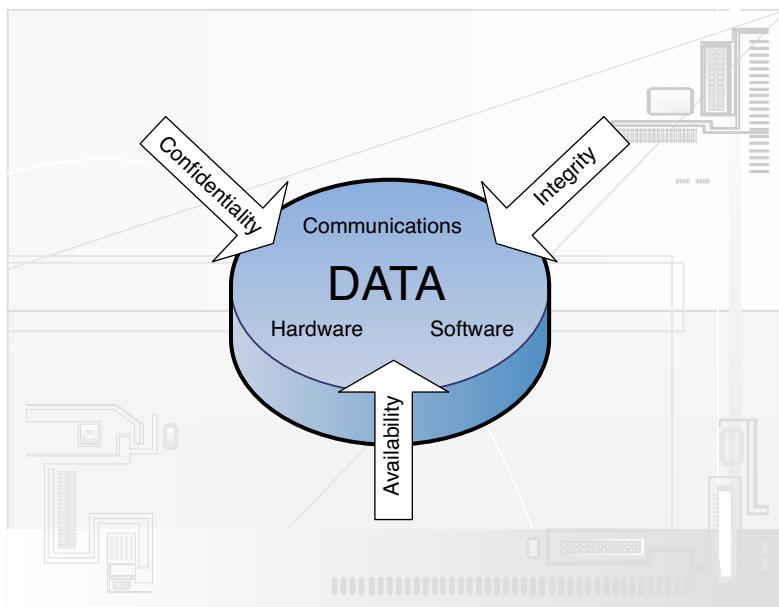
Key Topic

Figure 1-1 The CIA of Computer Security

By employing the concepts of confidentiality, integrity, and availability to its data, an organization can properly secure its hardware, software, and communications. Let's discuss each of the three items of the CIA triad in a little more depth.

Key Topic

- **Confidentiality:** This concept centers on preventing the disclosure of information to unauthorized persons. For the public it signifies Social Security numbers (or other country-specific identification), driver license information, bank accounts and passwords, and so on. For organizations this can include all the preceding information, but it actually denotes the confidentiality of data. To make data confidential, the organization must work hard to make sure that it can be accessed only by authorized individuals. This book spends a good amount of time discussing and showing how to accomplish this. For example, when you use a credit card number at a store or online, the number should be encrypted with a strong cipher so that the card number cannot be compromised. Next time you buy something online, take a look at how the credit card number is being kept confidential. As a security professional, confidentiality should be your number one goal. In keeping data confidential, you remove threats, absorb vulnerabilities, and reduce risk.
- **Integrity:** This means that data has not been tampered with. Authorization is necessary before data can be modified in any way; this is done to protect the data's integrity. For example, if a person were to delete a required file, either

maliciously or inadvertently, the integrity of that file will have been violated. There should have been permissions in place to stop the person from deleting the file. Here's a tip for you: Some organizations do not delete data—ever!

- **Availability:** Securing computers and networks can be a strain on resources. Availability means that data is obtainable regardless of how information is stored, accessed, or protected. It also means that data should be available regardless of the malicious attack that might be perpetrated on it.

These three principles should be applied whenever dealing with the security of hardware, software, or communications. They should be foremost in the mind of a security administrator.

Another acronym to live by is the AAA of computer security: authentication, authorization, and accounting.

- **Authentication:** When a person's identity is established with proof and confirmed by a system. Typically, this requires a digital identity of some sort, username/password, or other authentication scheme.
- **Authorization:** When a user is given access to certain data or areas of a building. Authorization happens after authentication and can be determined in several ways, including permissions, access control lists, time-of-day restrictions, and other login and physical restrictions.
- **Accounting:** The tracking of data, computer usage, and network resources. Often it means logging, auditing, and monitoring of the data and resources. Accountability is quickly becoming more important in today's secure networks. Part of this concept is the burden of proof. You as the security person must provide proof if you believe that someone committed an unauthorized action. When you have indisputable proof of something users have done and they cannot deny it, it is known as **non-repudiation**.

Key Topic

This AAA concept should also be applied to any security plan you develop. But it goes further than this. There are authentication protocols based on the concept of AAA such as RADIUS and TACACS+, which we cover in more depth in Chapter 9, "Physical Security and Authentication Models." Because of this, AAA is also referred to as a protocol. The details of AAA are set in stone within several RFC documents that can be downloaded from the following link:

<http://tools.ietf.org/wg/aaa/>

The Basics of Information Security

Information security is the act of protecting data and information systems from unauthorized access, unlawful modification and disruption, disclosure, corruption,

and destruction. We discuss how to implement information security throughout the entire book, but for now let's talk about several basic types of threats you need to be aware of to be an effective security administrator:

- **Malicious software:** Known as malware, this includes computer viruses, worms, Trojan horses, spyware, rootkits, adware, and other types of unwanted software. Everyone has heard of a scenario in which a user's computer was compromised to some extent due to malicious software.
- **Unauthorized access:** Access to computer resources and data without consent of the owner. It might include approaching the system, trespassing, communicating, storing and retrieving data, intercepting data, or any other methods that would interfere with a computer's normal work. Access to data must be controlled to ensure privacy. Improper administrative access falls into this category as well.
- **System failure:** Computer crashes or individual application failure. This can happen due to several reasons, including user error, malicious activity, or hardware failure.
- **Social engineering:** The act of manipulating users into revealing confidential information or performing other actions detrimental to the user. Almost everyone gets e-mails nowadays from unknown entities making false claims or asking for personal information (or money!); this is one example of social engineering.

Many information security technologies and concepts can protect against, or help recover from, the preceding threats. The question is, does your organization have the resources to implement them? Even on a low budget the answer is usually "yes." It all starts with planning, which is effectively free.

In general, a security administrator should create a proactive security plan that usually starts with the implementation of security controls. When creating the security plan, some IT professionals divide the plan into three categories of controls as follows:

- **Physical:** Things such as alarm systems, surveillance cameras, locks, ID cards, security guards, and so on.
- **Technical:** Items such as smart cards, access control lists (ACLs), encryption, and network authentication.
- **Administrative:** Various policies and procedures, security awareness training, contingency planning, and disaster recovery plans (DRPs). Administrative controls can also be broken down into two subsections: procedural controls and legal/regulatory controls.

NOTE We'll expand on these and other security controls in Chapter 11, "Vulnerability and Risk Assessment."

These information security controls are used to protect the confidentiality, integrity, and availability, or "CIA" of data.

More specifically, several ways to prevent and help recover from the previous threats include

- **User awareness:** The wiser the user, the less chance of security breaches. Employee training and education, easily accessible and understandable policies, security awareness e-mails, and online security resources all help to provide user awareness. These methods can help to protect from all the threats mentioned previously. Although it can only go so far while remaining cost-effective and productive, educating the user can be an excellent method when attempting to protect against security attacks.
- **Authentication:** Verifying a person's identity helps to protect against unauthorized access. Authentication is a preventative measure that can be broken down into five categories:
 - Something the user knows; for example, a password or PIN
 - Something the user has; for example, a smart card or other security token
 - Something the user is; for example, the biometric reading of a fingerprint or retina scan
 - Something a user does; for example, voice recognition or a written signature
 - Somewhere a user is; for example, a GPS-tracked individual, or when a system is authenticated through geographic location
- **Anti-malware software:** Anti-malware protects a computer from the various forms of malware and, if necessary, detects and removes them. Types include antivirus and anti-spyware software. Well-known examples include programs from Symantec and McAfee, as well as Microsoft's Windows Defender. Nowadays, a lot of the software named "antivirus" can protect against spyware and other types of malware as well.
- **Data backups:** Backups won't stop damage to data, but they can enable you to recover data after an attack or other compromise, or system failure. From programs such as Windows Backup and Restore and Bacula to enterprise-level

programs such as IBM’s Tivoli and Symantec’s Backup Exec, data backup is an important part of security. Note that fault-tolerant methods such as **RAID 1, 5, and 6** are good preventative measures against hardware failure but *might* not offer protection from data corruption or erasure. For more information on RAID, see Chapter 15, “Redundancy and Disaster Recovery.”

- **Encryption:** The act of changing information using an algorithm (known as a cipher) to make that information unreadable to anyone except users who possess the proper “key”. Examples of this include wireless sessions encrypted with Advanced Encryption Standard (AES), web pages encrypted with HTTP Secure (HTTPS), and e-mails encrypted with Secure/Multipurpose Internet Mail Extensions (S/MIME) or Pretty Good Privacy (PGP).
- **Data removal:** Proper data removal goes far beyond file deletion or the formatting of digital media. The problem with file deletion/formatting is data *remanence*, or the residue, left behind, from which re-creation of files can be accomplished by some less-than-reputable people with smart tools. Companies typically employ one of three options when met with the prospect of data removal: clearing, purging (also known as sanitizing), and destruction. We talk more about these in Chapter 16, “Policies, Procedures, and People.”

By combining a well-thought-out security plan with strong individual security methods, a security professional can effectively stop threats before they become realities, or at the least, in worst-case scenarios, recover from them quickly and efficiently. The strongest security plans take many or all of these methods and combine them in a layering strategy known as **defense in depth**, which can be defined as the building up and layering of security measures that protect data throughout the entire life cycle starting from inception, on through usage, storage, and network transfer, and finally to disposal.

Think Like a Hacker

I’m not condoning any malicious activity, but to think like a hacker, you have to understand the hacker. A good hacker understands the mind of a security administrator, making computer and network security a difficult proposition. But the converse is true as well—the smart security person is aware of hackers and their methods.

So ask yourself, why do people decide to become hackers? In the minds of some malicious individuals, it may simply be because users are there to be taken advantage of! Another common answer is greed—in this case the act of hacking for illegal monetary gain. Other attackers have an agenda, or believe in a cause. Some want to get free access to movies and music. Finally, some just want to cause mayhem and anarchy. Consider this when you secure your organization’s computers—they just

might be a target! Of course, people use different names to classify these types of individuals: hacker, cracker, cyber-criminal, and so on. It doesn't matter what you call them, but the accepted term in most network security circles is hacker—which we will use throughout this book.

Now consider this: Not all hackers are malicious. That's right! There are different types of hackers. Various names are used by different organizations, but some of the common labels include the following:

- **White hats:** These people are nonmalicious; for example, an IT person who attempts to “hack” into a computer system before it goes live to test the system. Generally, the person attempting the hack has a contractual agreement with the owner of the resource to be hacked. White hats often are involved in something known as ethical hacking. An **ethical hacker** is an expert at breaking into systems and can attack systems on behalf of the system’s owner and with the owner’s consent. The ethical hacker uses penetration testing and intrusion testing to attempt to gain access to a target network or system.
- **Black hats:** These are malicious individuals who attempt to break into computers and computer networks *without* authorization. Black hats are the ones who attempt identity theft, piracy, credit card fraud, and so on. Penalties for this type of activity are severe, and black hats know it; keep this in mind if and when you come into contact with one of these seedy individuals—they can be brutal, especially when cornered. Of course, many vendors try to make the term “black hat” into something cuter and less dangerous. But for the purposes of this book and your job security, we need to speak plainly, so here we will consider a black hat to be a malicious individual.
- **Gray hats:** These are possibly the most inexplicable people on the planet. They are individuals who do not have any affiliation with a company but risk breaking the law by attempting to hack a system and then notify the administrator of the system that they were successful in doing so—just to let them know! Not to do anything malicious (other than breaking in...). Some gray hats offer to fix security vulnerabilities at a price, but these types are also known as green hats or mercenaries.
- **Blue hats:** These are individuals who are asked to attempt to hack into a system by an organization, but the organization does not employ them. The organization relies on the fact that the person simply enjoys hacking into systems. Usually, this type of scenario occurs when testing systems.
- **Elite:** Elite hackers are the ones who first find out about vulnerabilities. Only 1 out of an estimated 10,000 hackers wears the Elite hat—and I say that figuratively. The credit for their discoveries is usually appropriated by someone else more interested in fame. Many of these types of individuals don’t usually

Key Topic

care about “credit due” and are more interested in anonymity—perhaps a wise choice. You do not want to get on an Elite hacker’s bad side; they could crumple most networks and programs within hours if they so desired.

I mentioned before that no system is truly secure (and I use the term “system” loosely). Hackers know this and count on it. There’s always a way to circumnavigate a defense. It’s a constant battle in which administrators and attackers are consistently building and breaking down better and better mouse traps. The scales are always tipping back and forth; a hacker develops a way to break into a system, then an administrator finds a way to block that attack, then the hacker looks for an alternative method, and so on. This seems to reek of the chicken and the egg—which came first? Answer: You have to take it on a case-by-case basis. The last few sentences of banter are there for one reason—to convince you that you need to be on your toes; that you need to review logs often; that you need to employ as many security precautions as possible; that you need to keep abreast of the latest attacks and ways to mitigate risk; and that you must never underestimate the power and resilience of a hacker.

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 1-1 lists a reference of these key topics and the page number on which each is found.

Table 1-1 Key Topics for Chapter 1

Key Topic Element	Description	Page Number
Figure 1-1	The CIA of computer security	4
Bulleted list	Definitions of confidentiality, integrity, and availability	4
Bulleted list	Definitions of authentication, authorization, and accounting	5
Bulleted list	Definitions of the different types of hacker “hats”	9

Define Key Terms

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

Information security, confidentiality, integrity, availability, authentication, authorization, accounting, non-repudiation, defense in depth, white hat, ethical hacker, black hat

Review Questions

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

1. In information security, what are the three main goals? (Select the three best answers.)
 - A. Auditing
 - B. Integrity
 - C. Non-repudiation
 - D. Confidentiality
 - E. Risk Assessment
 - F. Availability
2. To protect against malicious attacks, what should you think like?
 - A. Hacker
 - B. Network admin
 - C. Spoofers
 - D. Auditor
3. Tom sends out many e-mails containing secure information to other companies. What concept should be implemented to prove that Tom did indeed send the e-mails?
 - A. Authenticity
 - B. Non-repudiation
 - C. Confidentiality
 - D. Integrity

4. Which of the following does the A in CIA stand for when it comes to IT security? Select the best answer.
 - A. Accountability
 - B. Assessment
 - C. Availability
 - D. Auditing
5. Which of the following is the greatest risk when it comes to removable storage?
 - A. Integrity of data
 - B. Availability of data
 - C. Confidentiality of data
 - D. Accountability of data
6. When it comes to information security, what is the I in CIA?
 - A. Insurrection
 - B. Information
 - C. Indigestion
 - D. Integrity
7. You are developing a security plan for your organization. Which of the following is an example of a physical control?
 - A. Password
 - B. DRP
 - C. ID card
 - D. Encryption
8. A user receives an e-mail but the e-mail client software says that the digital signature is invalid and the sender of the e-mail cannot be verified. The would-be recipient is concerned about which of the following concepts?
 - A. Confidentiality
 - B. Integrity
 - C. Remediation
 - D. Availability

9. Cloud environments often reuse the same physical hardware (such as hard drives) for multiple customers. These hard drives are used and reused when customer virtual machines are created and deleted over time. What security concern does this bring up implications for?
- A. Availability of virtual machines
 - B. Integrity of data
 - C. Data confidentiality
 - D. Hardware integrity
10. When is a system completely secure?
- A. When it is updated
 - B. When it is assessed for vulnerabilities
 - C. When all anomalies have been removed
 - D. Never

Answers and Explanations

1. **B., D., and F.** Confidentiality, integrity, and availability (known as CIA, the CIA triad, and the security triangle) are the three main goals when it comes to information security. Another goal within information security is accountability.
2. **A.** To protect against malicious attacks, think like a hacker. Then, protect and secure like a network security administrator.
3. **B.** You should use non-repudiation to prevent Tom from denying that he sent the e-mails.
4. **C.** Availability is what the A in CIA stands for, as in “the availability of data.” Together the acronym stands for confidentiality, integrity, and availability. Although accountability is important and is often included as a fourth component of the CIA triad, it is not the best answer. Assessment and auditing are both important concepts when checking for vulnerabilities and reviewing and logging, but they are not considered to be part of the CIA triad.
5. **C.** For removable storage, the confidentiality of data is the greatest risk because removable storage can easily be removed from the building and shared with others. Although the other factors of the CIA triad are important, any theft of removable storage can destroy the confidentiality of data, and that makes it the greatest risk.

6. **D.** The I in CIA stands for integrity. Together CIA stands for confidentiality, integrity, and availability. Accountability is also a core principle of information security.
7. **C.** An ID card is an example of a physical security control. Passwords and encryption are examples of technical controls. A disaster recovery plan (DRP) is an example of an administrative control.
8. **B.** The recipient should be concerned about the integrity of the message. If the e-mail client application cannot verify the digital signature of the sender of the e-mail, then there is a chance that the e-mail either was intercepted or is coming from a separate dangerous source. Remember, integrity means the reliability of the data, and whether or not it has been modified or compromised by a third party before arriving at its final destination.
9. **C.** There is a concern about data confidentiality with cloud computing because multiple customers are sharing physical hard drive space. A good portion of customers run their cloud-based systems in virtual machines. Some virtual machines could run on the very same hard drive (or very same array of hard drives). If one of the customers had the notion, they could attempt to break through the barriers between virtual machines, which if not secured properly, would not be very difficult to do.
10. **D.** A system can never truly be completely secure. The scales are always tipping back and forth; a hacker develops a way to break into a system, then an administrator finds a way to block that attack, and then the hacker looks for an alternative method. It goes on and on; be ready to wage the eternal battle!

This page intentionally left blank



This chapter covers the following subjects:

- **Computer Systems Security Threats:** This portion of Chapter 2 helps you to differentiate between the various computer security threats you should be aware of for the exam, including malware in all its forms, botnets, spam, privilege escalation, and more. Then we discuss how to defend against those threats in a proactive way, and how to fix problems that do occur in the case that threats have already manifested themselves. This is the most important section of this chapter; study it carefully!
- **Implementing Security Applications:** In this section, you learn how to select, install, and configure security applications such as personal firewalls, antivirus programs, and host-based intrusion detection systems. You'll be able to distinguish between the various tools and decide which is best for the different situations you'll see in the field.
- **Securing Computer Hardware, Peripherals, and Mobile Devices:** Here we delve into the physical: how to protect a computer's hardware, BIOS, and peripherals such as USB devices. We also discuss how to protect mobile devices such as smartphones and tablet computers.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 2.1, 2.3, 3.1, 3.2, 4.2, and 4.3.

Computer Systems Security

Simply stated, the most important part of a computer is the data. The data must be available, yet secured in such a way so that it can't be tampered with. Computer systems security is all about the security threats that can compromise an operating system and the data held within. Threats such as viruses, Trojans, spyware, and other malicious software are extremely prevalent in today's society. They are a big part of this chapter, and this chapter is an important part of the book. But it doesn't stop there; your computer can be accessed in other ways, including via the BIOS and by external devices. And "computer" doesn't just mean that desktop computer at a user's desk. It also means laptops, tablets, and smartphones—actually any other devices that have processing power and an operating system. These threats can be eliminated by implementing security applications on every one of your client computers on the network. Applications that can help to secure your computers against malware threats include antivirus programs, anti-spyware applications, personal firewalls, and host-based intrusion detection systems.

By implementing these security applications and ensuring that they are updated regularly, you can stave off the majority of malicious attacks that can target a computer system.

Foundation Topics

Computer Systems Security Threats

To combat the various security threats that can occur on a computer system, we first need to classify them. Then we need to define how these threats can be delivered to the target computer. Afterward we can discuss how to prevent security threats from happening and troubleshoot them if they do occur. Let's start with the most common computer threat and probably the most deadly—malicious software.

Malicious Software

Malicious software, or **malware**, is software designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent. Malware is a broad term used by computer professionals to include viruses, worms, Trojan horses, spyware, rootkits, adware, and other types of undesirable software.

Of course, we don't want malware to infect our computer system, but to defend against it we first need to define it and categorize it. Then we can put preventative measures into place. It's also important to locate and remove/quarantine malware from a computer system in the case that it does manifest itself.

For the exam, you need to know about several types of malware. For the past several years, an emphasis shift from viruses to other types of malware, such as spyware and ransomware, has occurred. Most people know about viruses and have some kind of antivirus software running. However, many people are still confused about the various other types of malware, how they occur, and how to protect against them. Because of this, computer professionals spend a lot of time fixing malware issues (that are not virus related) and training users on how to protect against them in the future. However, viruses are still a valid foe; let's start by discussing them.

Viruses

A **virus** is code that runs on a computer without the user's knowledge; it infects the computer when the code is accessed and executed. For viruses to do their dirty work, they first need to be executed by the user in some way. A virus also has reproductive capability and can spread copies of itself throughout the computer as long as it is first executed by the user—the virus can't reproduce by itself. By infecting files accessed by other computers, the virus can spread to those other systems as well. The problem is that computers can't call in sick on Monday; they need to be up and running as much as possible, more than your average human.

One well-known example of a virus is the Love Bug. Originating in 2000, this virus would arrive by an e-mail titled "I love you" with an attachment named love-letter-for-you.txt.vbs, or one of several other permutations of this fictitious love. Some users would be tricked into thinking this was a text file, but the extension was actually .vbs, short for Visual Basic script. This virus deleted files, sent usernames and passwords to its creator, infected 15 million computers, and supposedly caused \$5 billion in damage. Educate your users on how to screen their e-mail!

You might encounter several different types of viruses:

- **Boot sector:** Initially loads into the first sector of the hard drive; when the computer boots, the virus then loads into memory.
- **Macro:** Usually placed in documents and e-mailed to users in the hopes that the users will open the document, thus executing the virus.
- **Program:** Infects executable files.
- **Polymorphic:** Can change every time it is executed in an attempt to avoid antivirus detection.
- **Stealth:** Uses various techniques to go unnoticed by antivirus programs.
- **Armored:** This protects itself from antivirus programs by tricking the program into thinking that it is located in a different place from where it actually resides. Essentially, it has a layer of protection that it can use against the person who tries to analyze it; it will thwart attempts by analysts to examine its code.
- **Multipartite:** A hybrid of boot and program viruses that attacks the boot sector or system files first and then attacks the other files on the system.

Worms

A **worm** is much like a virus except that it self-replicates, whereas a virus does not. Worms take advantage of security holes in operating systems and applications (including backdoors, which we discuss later). They look for other systems on the network or through the Internet that are running the same applications and replicate to those other systems. With worms, the user doesn't need to access and execute the malware. A virus needs some sort of carrier to get it where it wants to go and needs explicit instructions to be executed, or it must be executed by the user. The worm does not need this carrier or explicit instructions to be executed.

A well-known example of a worm is Nimda (admin backward), which propagated automatically through the Internet in 22 minutes in 2001, causing widespread damage. It propagated through network shares, mass e-mailing, and operating system vulnerabilities.

Many times, the worm does not carry a payload, meaning that in and of itself, it does not contain code that can harm a computer. It may or may not include other malware, but even if it doesn't, it can cause general disruption of network traffic and computer operations because of the very nature of its self-replicating abilities.

Trojan Horses

Trojan horses, or simply Trojans, appear to perform wanted functions but are actually performing malicious functions behind the scenes. These are not technically viruses and can easily be downloaded without being noticed. They can also be transferred to a computer by way of removable media, especially USB flash drives. One example of a Trojan is a file that is contained within a downloaded program such as a key generator (known as a “keygen” used with pirated software) or other executable. If a user complains about slow system performance and numerous antivirus alerts, and they recently installed a questionable program from the Internet or from a USB flash drive, their computer could be infected by a Trojan.

Remote access Trojans (RATs) are the most common type of Trojan, for example Back Orifice, NetBus, or SubSeven (now deprecated); their capability to allow an attacker higher administration privileges than those of the owner of the system makes them quite dangerous. The software effectively acts as a remote administration tool (another name for the RAT acronym). These programs have the capability to scan for unprotected hosts and make all kinds of changes to a host when connected. A program like this was not *necessarily* designed to be used maliciously, but programs like these are easy for an average person to download and manipulate computers with. Worse, when a target computer is controlled by an attacker, it could easily become a robot (or simply a *bot*), carrying out the plans of the attacker on command. We'll discuss bots later in this chapter.

RATs can also be coded in PHP (or other languages) to allow remote access to websites. An example of this is the web shell, which has many permutations. It allows an attacker to remotely configure a web server without the user's consent. Quite often, the attacker will have cracked the FTP password in order to upload the RAT.

RATs are often used to persistently target a specific entity such as a government or a specific corporation. One example of this is the Plugx RAT. Malicious software such as this is known as an advanced persistent threat (APT). Groups that have vast resources at their disposal might make use of these APTs to carry out objectives against large-scale adversaries. APT groups could take the form of large hacker factions, and even some corporations and governments around the globe.

Ransomware

Some less than reputable persons use a particularly devious malware known as **ransomware**—a type of malware that restricts access to a computer system and demands that a ransom be paid. It locks the system in one of several ways, and informs the user that in order to unlock the computer and regain access to files, a payment would have to be made to one of several banking services, often overseas. It often

propagates as a Trojan or worm, and can make use of encryption to make the user's files inaccessible. This usage of encryption is also known as cryptoviral extortion. One example of this is CryptoLocker. This ransomware Trojan encrypts certain files on the computer's drives using an RSA public key. (The counterpart private key is stored on the malware creator's server.) Though the Trojan can be easily defeated by being either quarantined or removed, the files remain encrypted, and are nearly impossible to decrypt (given the strength of the RSA key). Payment is often required in voucher form, or in the form of a cryptocurrency such as Bitcoin. Ransomware attacks grew steadily for several years until 2013 when CryptoLocker (and other similar ransomware Trojans) appeared—now hundreds of thousands of computers worldwide are affected each year.

NOTE Sometimes a user will inadvertently access a fraudulent website (or pop-up site) that says that all the user's files have been encrypted and payment is required to decrypt them; some imposing government-like logo will accompany the statement. But many of these sites don't actually encrypt the user's files. In this case we have plain old extortion with no real damage done to the computer or files. These types of sites can be blocked by pop-up blockers, phishing filters, and the user's common sense when clicking searched-for links.

Spyware

Spyware is a type of malicious software either downloaded unwittingly from a website or installed along with some other third-party software. Usually, this malware collects information about the user without the user's consent. Spyware could be as simple as a piece of code that logs what websites you access, or go as far as a program that records your keystrokes (known as keyloggers). Spyware is also associated with advertising (those pop-ups that just won't go away!), and is sometimes related to malicious advertising, or *malvertising*—the use of Internet-based advertising (legitimate and illegitimate) to distribute malicious software.

Spyware can possibly change the computer configuration without any user interaction; for example, redirecting a browser to access websites other than those wanted.

Adware usually falls into the realm of spyware because it pops up advertisements based on what it has learned from spying on the user. **Grayware** is another general term that describes applications that are behaving improperly but without serious consequences. It is associated with spyware, adware, and joke programs. Very funny...not. One example (of many) of spyware is the Internet Optimizer, which redirects IE error pages out to other websites' advertising pages. Spyware can even be taken to the next level and be coded in such a way to hijack a person's computer.

Rootkits

A **rootkit** is a type of software designed to gain administrator-level control over a computer system without being detected. The term is a combination of the words “root” (meaning the root user in a Unix/Linux system or administrator in a Windows system) and “kit” (meaning software kit). Usually, the purpose of a rootkit is to perform malicious operations on a target computer at a later date without the knowledge of the administrators or users of that computer. A rootkit is a variation on the virus that attempts to dig in to the lower levels of the operating system—components of the OS that start up before any anti-malware services come into play. Rootkits can target the BIOS, boot loader, kernel, and more. An example of a boot loader rootkit is the Evil Maid Attack; this attack can extract the encryption keys of a full disk encryption system, which we discuss more later. Another (more current) example is the Alureon rootkit, which affects the master boot record (MBR) and low-level system drivers (such as atapi.sys). This particular rootkit was distributed by a botnet, and affected over 200,000 (known) Microsoft operating systems.

Rootkits are difficult to detect because they are activated before the operating system has fully booted. A rootkit might install hidden files, hidden processes, and hidden user accounts. Because rootkits can be installed in hardware or software, they can intercept data from network connections, keyboards, and so on.

Spam

Have you ever received an e-mail asking you to send money to some strange person in some faraway country? Or an e-mail offering extremely cheap Rolex watches? Or the next best penny stock? All of these are examples of spam. **Spam** is the abuse of electronic messaging systems such as e-mail, texting, social media, broadcast media, instant messaging, and so on. Spammers send unsolicited bulk messages indiscriminately, usually without benefit to the actual spammer, because the majority of spam is either deflected or ignored. Companies with questionable ethics condone this type of marketing (usually set up as a pyramid scheme) so that the people at the top of the marketing chain can benefit; however, it’s usually not worthwhile for the actual person who sends out spam.

The most common form of spam is e-mail spam, which is one of the worst banes of network administrators. Spam can clog up resources and possibly cause a type of denial-of-service to an e-mail server if there is enough of it. It can also mislead users, in an attempt at social engineering. And the bulk of network-based viruses are transferred through spam e-mails. Yikes! The worst type of spamming is when a person uses another organization’s e-mail server to send the spam. Obviously illegal, it could also create legal issues for the organization that owns the e-mail server. Just about

everyone has seen a spam e-mail, and in the rare case that you haven't, check out this link for some pretty horrific examples:
www.antespam.co.uk/spam-resource/

A derivative of spam, called *spim*, is the abuse of instant messaging systems, chat rooms, and chat functions in games specifically. It is also known as messaging spam, or IM spam.

Summary of Malware Threats

Table 2-1 summarizes the malware threats discussed up to this point.

Table 2-1 Summary of Malware Threats

Key Topic

Malware Threat	Definition	Example
Virus	Code that runs on a computer without the user's knowledge; it infects the computer when the code is accessed and executed.	Love Bug virus Ex: love-letter-for-you.txt.vbs
Worm	Similar to viruses except that it self-replicates, whereas a virus does not.	Nimda Propagated through network shares and mass e-mailing
Trojan horse	Appears to perform desired functions but actually is performing malicious functions behind the scenes.	Remote access Trojan Ex: Plugx
Ransomware	Malware that restricts access to computer files and demands a ransom be paid by the user.	Often propagated via a Trojan Ex: CryptoLocker
Spyware	Malicious software either downloaded unwittingly from a website or installed along with some other third-party software.	Internet Optimizer (aka DyFuCA)
Rootkit	Software designed to gain administrator-level control over a computer system without being detected.	Boot loader rootkits Ex: Evil Maid Attack, Alureon
Spam	The abuse of electronic messaging systems such as e-mail, broadcast media, and instant messaging.	Identity theft e-mails (phishing) Lottery scam e-mails

Ways to Deliver Malicious Software

Malware is not sentient (...not yet) and can't just appear out of thin air; it needs to be transported and delivered to a computer or installed on a computer system in some manner. This can be done in several ways. The simplest way would be for attackers to gain physical access to an unprotected computer and perform their malicious work locally. But because it can be difficult to obtain physical access, this can be done in several other ways, as shown in the upcoming sections. Some of the methods listed next can also be used by an attacker to simply gain access to a computer, make modifications, and so on, in addition to delivering the malware.

The method that a threat uses to access a target is known as a **threat vector**. Collectively, the means by which an attacker gains access to a computer in order to deliver malicious software is known as an **attack vector**. Probably the most common attack vector is via software.

Via Software, Messaging, and Media

Malware can be delivered via software in many different ways. A person who e-mails a zipped file might not even know that malware also exists in that file. The recipients of the e-mail will have no idea that the extra malware exists unless they have software to scan their e-mail attachments for it. Malware could also be delivered via FTP. Because FTP servers are inherently insecure, it's easier than you might think to upload insidious files and other software. Malware is often found among peer-to-peer (P2P) networks and bit torrents. Great care should be taken by users who use these technologies. Malware can also be embedded within, and distributed by, websites through the use of corrupting code or bad downloads. Malware can even be distributed by advertisements. And of course, removable media can victimize a computer as well. Optical discs and USB flash drives can easily be manipulated to automatically run malware when they are inserted into the computer. (This is when AutoRun is not your friend!) The removable media could also have hidden viruses or worms and possibly logic bombs (discussed later) configured to set that malware off at specific times.

Potential attackers also rely on user error. For example, if a user is attempting to access a website but types the incorrect domain name by mistake, the user could be redirected to an altogether unwanted website, possibly malicious in nature. This type of attack is known as **typosquatting** or URL hijacking. URL stands for uniform resource locator, which is the web address that begins with http or www. The potential attacker counts on the fact that millions of typos are performed in web browsers every day. These attackers "squat" on similar (but not exact) domain names. Once the user is at the new and incorrect site, the system becomes an easy target for spyware and other forms of malware. Some browsers come with built-in security such

as anti-phishing tools and the ability to auto-check websites that are entered, but the best way to protect against this is to train users to be careful when typing domain names.

NOTE Speaking of what a user types, some attackers will make use of a keylogger to record everything that the user types on the keyboard. This tool could be hardware or software-based, and is often used by security professionals as well. More about keyloggers appears in Chapter 12, “Monitoring and Auditing.”

Between the years 2008 and 2013, the distribution of malware grew exponentially. This is in large part due to automation, and the use of web attack-based software “kits.” This automating of cyber-crime, and the software used to do so, is collectively referred to as crimeware. One example of a web attack kit is the Blackhole exploit kit. This is used (and purchased) by potential attackers in order to distribute malware to computers that meet particular criteria, while the entire process is logged and documented. Kits such as this one account for the largest percentage of web threats, and are the most common software-based method of distributing malware.

Botnets and Zombies

I know what you are thinking—the names of these attacks and delivery methods are getting a bit ridiculous. But bear with me; they make sense and are deadly serious. Allow me to explain—malware can be distributed throughout the Internet by a group of compromised computers, known as a **botnet**, and controlled by a master computer (where the attacker resides). The individual compromised computers in the botnet are called **zombies**. This is because they are unaware of the malware that has been installed on them. This can occur in several ways, including automated distribution of the malware from one zombie computer to another. Now imagine if all the zombie computers had a specific virus or other type of attack loaded, and a logic bomb (defined a bit later) was also installed, ready to set off the malware at a specific time. If this were done to hundreds or thousands of computers, a synchronized attack of great proportions could be enacted on just about any target. Often, this is known as a distributed denial-of-service, or DDoS, attack, and is usually perpetrated on a particularly popular server, one that serves many requests. If a computer on your network is continually scanning other systems on the network, is communicating with an unknown IRC server or other unknown master server, and/or has hundreds of outbound connections to various websites, chances are the computer is part of a botnet.

But botnets can be used for more than just taking down a single target. They can also be used to fraudulently obtain wealth. One example of this type of botnet is the ZeroAccess botnet. It is based on Trojan malware that affects various Microsoft operating systems, and is used to mine Bitcoins or perpetuate click fraud. It is hidden from many antivirus programs through the use of a rootkit (infecting the MBR). In 2012 it was estimated that the botnet consisted of up to 10 million computers. You can imagine the sheer power of a botnet such as this, and the amount of revenue it can bring in per month. Every couple of months you can read about another botnet mastermind who has been brought to justice—only to be replaced by another entrepreneur.

Active Interception

Active interception normally includes a computer placed between the sender and the receiver in an effort to capture and possibly modify information. If a person can eavesdrop on your computer's data session, then that data can be stolen, modified, or exploited in other ways. Examples of this include session theft and man-in-the-middle (MITM) attacks. For more information on these attacks, see the section titled "Malicious Attacks" in Chapter 6, "Networking Protocols and Threats."

Privilege Escalation

Privilege escalation is the act of exploiting a bug or design flaw in a software or firmware application to gain access to resources that normally would've been protected from an application or user. This results in a user gaining additional privileges, more than were originally intended by the developer of the application; for example, if a regular user gains administrative control, or if a particular user can read another user's e-mail without authorization.

Backdoors

Backdoors are used in computer programs to bypass normal authentication and other security mechanisms in place. Originally, backdoors were used by developers as a legitimate way of accessing an application, but soon after they were implemented by attackers who would use backdoors to make changes to operating systems, websites, and network devices. Or the attacker would create a completely new application that would act as a backdoor, for example Back Orifice, which enables a user to control a Windows computer from a remote location. Often, it is installed via a Trojan horse; this particular one is known as a remote access Trojan, or RAT, as previously mentioned. Some worms install backdoors on computers so that remote spammers can send junk e-mail from the infected computers, or so

an attacker can attempt privilege escalation. Unfortunately, there isn't much that can be done about backdoors aside from updating or patching the system infected and keeping on top of updates. However, if network administrators were to find out about a new backdoor, they should inform the manufacturer of the device or the application as soon as possible. Backdoors are less common nowadays, because their practice is usually discouraged by software manufacturers and by makers of network devices.

Logic Bombs

A **logic bomb** is code that has, in some way, been inserted into software; it is meant to initiate one of many types of malicious functions when specific criteria are met. Logic bombs blur the line between malware and a malware delivery system. They are indeed unwanted software but are intended to activate viruses, worms, or Trojans at a specific time. Trojans set off on a certain date are also referred to as **time bombs**. The logic bomb ticks away until the correct time, date, and other parameters have been met. So, some of the worst bombs do not incorporate an explosion whatsoever. The logic bomb could be contained within a virus or loaded separately. Logic bombs are more common in the movies than they are in real life, but they do happen, and with grave consequences; but more often than not, they are detected before they are set off. If you, as a systems administrator, suspect that you have found a logic bomb, or a portion of the code of a logic bomb, you should notify your superior immediately and check your organization's policies to see if you should take any other actions. Action could include placing network disaster recovery processes on standby; notifying the software vendor; and closely managing usage of the software, including, perhaps, withdrawing it from service until the threat is mitigated. Logic bombs are the evil cousin of the Easter egg.

Easter eggs historically have been a platonic extra that was added to an OS or application as a sort of joke; often, it was missed by quality control and subsequently released by the manufacturer of the software. An older example of an Easter egg is the capability to force a win in Windows XP's Solitaire by pressing the ALT+Shift+2 keys simultaneously. Easter eggs are not normally documented (being tossed in last minute by humorous programmers) and are meant to be harmless, but nowadays they are not allowed by responsible software companies and are thoroughly scanned for. Because an Easter egg (and who knows what else) can possibly slip past quality control, and because of the growing concerns about malware in general, many companies have adopted the idea of Trustworthy Computing, which is a newer concept that sets standards for how software is designed, coded, and checked for quality control. Sadly, as far as software goes, the Easter egg's day has passed.

Preventing and Troubleshooting Malware

Now that we know the types of malware, and the ways that they can be delivered to a computer, let's talk about how to stop them before they happen, and how to troubleshoot them if they do happen. Unfortunately, given the number of computers you will work on, they *will* happen.

If a system is affected by malware, it might be sluggish in its response time or display unwanted pop-ups and incorrect home pages; or applications (and maybe even the whole system) could lock up or shut down unexpectedly. Often, malware uses CPU and memory resources directly or behind the scenes, causing the system to run slower than usual. In general, a technician should look for erratic behavior from the computer, as if it had a mind of its own! Let's go over viruses and spyware, look at how to prevent them, and finally discuss how to troubleshoot them if they do occur.

Preventing and Troubleshooting Viruses

We can do several things to protect a computer system from viruses. First, every computer should have antivirus software running on it. Kaspersky, McAfee, and Norton are examples of manufacturers of antivirus (AV) software, but there are many others, plus manufacturers of operating systems often bundle AV software with the OS or offer free downloads. Second, the AV software should be updated, which means that the software requires a current license; this is renewed yearly with most providers. When updating, be sure to update the AV engine *and* the definitions if you are doing it manually. Otherwise, set the AV software to automatically update at periodic intervals, for example, every day or every week. It's a good idea to schedule regular full scans of the system within the AV software.

As long as the definitions have been updated, antivirus systems usually locate viruses along with other malware such as worms and Trojans. However, these systems usually do not locate logic bombs, rootkits, and botnet activity. In lieu of this, keep in mind that AV software is important, but it is not a cure-all.

Next, we want to make sure that the computer has the latest service packs and updates available. This goes for the operating system and applications such as Microsoft Office. Backdoors into operating systems and other applications are not uncommon, and the OS manufacturers often release fixes for these breaches of security. Windows offers the Windows Update program. This should be enabled, and you should either check for updates periodically or set the system to check for updates automatically. It might be that your organization has rules governing how Windows Update functions. If so, configure Automatic Updates according to your company's policy. For example, in Windows 7 you can check whether your computer is up to date by going to Start > All Programs > Windows Update.

It's also important to make sure that a firewall is available, enabled, and updated. A firewall closes all the inbound ports to your computer (or network) in an attempt to block intruders. For instance, Windows Firewall (available in the Control Panel) is a built-in software-based feature included in most versions of Windows. This is illustrated in Figure 2-1. You can see that the firewall in the figure is enabled for private and public networks.

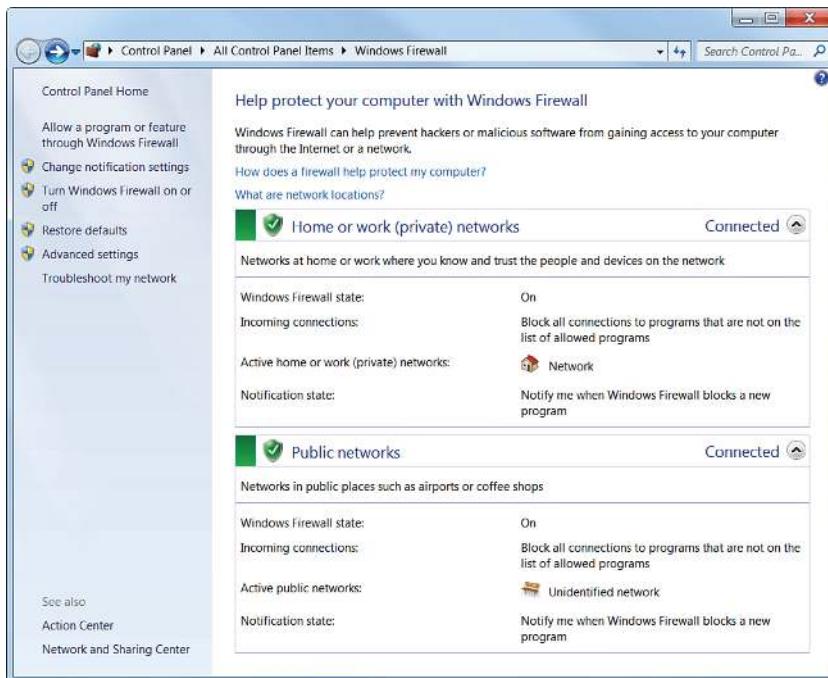


Figure 2-1 Windows Firewall in Windows 7

You might also have a hardware-based firewall; for example, one that is included in a small office/home office (SOHO) router. By using both, you have two layers of protection from various attacks that might include a payload with malware. Keep in mind that you might need to set exceptions for programs that need to access the Internet. This can be done by the program, or the port used by the protocol, and can be configured to enable specific applications to communicate through the firewall while keeping the rest of the ports closed.

Another way to help prevent viruses is to use what I call “separation of OS and data” (similar to the term “separation of church and state” in concept but not in content!). This method calls for two hard drives. The operating system is installed to the C: drive, and the data is stored on the D: drive (or whatever letter you use for the second drive). This compartmentalizes the system and data, making it more difficult

for viruses to spread and easier to isolate them when scanning. It also enables easy reinstallation without having to back up data! You can accomplish a similar scenario by using two partitions on the same drive.

NOTE There are viruses that can affect other types of operating systems as well. Android, iOS, and other desktop systems such as OS X and Linux are all susceptible, although not as commonly targeted as Windows systems.

Encryption is one excellent way to protect data that would otherwise be compromised (or lost) due to virus activity on a computer. Windows operating systems make use of the Encrypting File System (EFS), which can encrypt files on an individual basis. When a file is encrypted in this manner, the filename shows up green in color within Windows Explorer or File Explorer. It prevents clear-text access, and defies modification in most cases. Encryption of this type probably won't prevent viruses from occurring, but it can help to protect individual files from being compromised. We'll talk more about encryption later in this chapter and in Chapter 13, "Encryption and Hashing Concepts," and Chapter 14, "PKI and Encryption Protocols."

Finally, educate users as to how viruses can infect a system. Instruct them on how to screen their e-mails, and tell them not to open unknown attachments. Show them how to scan removable media before copying files to their computer, or set up the computer to scan removable media automatically. Sometimes user education works; sometimes it doesn't. One way to make user education more effective is to have a technical trainer educate your users, instead of doing it yourself. Or, consider creating interactive online learning tutorials. These methods can provide for a more engaging learning environment.

By using all of these techniques, virus infection can be severely reduced. However, if a computer is infected by a virus, you want to know what to look for so that you can "cure" the computer.

Here are some typical symptoms of viruses:

- Computer runs slower than usual.
- Computer locks up frequently or stops responding altogether.
- Computer restarts on its own or crashes frequently.
- Hard drives, optical drive, and applications are not accessible or don't work properly.

- Strange sounds occur.
- You receive unusual error messages.
- Display or print distortion occurs.
- New icons appear or old icons (and applications) disappear.
- There is a double extension on a file attached to an e-mail that was opened; for example: .txt.vbs or .txt.exe.
- Antivirus programs will not run or can't be installed.
- Files have been corrupted or folders are created automatically.
- System Restore capabilities are removed or disabled.

Before making any changes to the computer, make sure that you back up critical data and verify that the latest updates have been installed to the OS and the AV software. Then perform a thorough scan of the system using the AV software's scan utility; if allowed by the software, run the scan in Safe Mode. Another option is to move the affected drive to a "clean machine," a computer that is not connected to any network, and is used solely for the purpose of scanning for malware. This can be done by using a USB converter kit or a removable drive system, or by slaving the affected drive to an SATA, eSATA, or IDE port of the other computer. Then, run the AV software on that clean machine to scan that drive. PC repair shops use this isolated clean machine concept.

Hopefully, the AV software finds and quarantines the virus on the system. In the case that the AV software's scan does not find the issue, or if the AV software has been infected and won't run, you can try using a free online scanner such as Trend Micro's HouseCall:

<http://housecall.trendmicro.com/>

or download Microsoft's Malicious Software Removal Tool:
www.microsoft.com/security/pc-security/malware-removal.aspx

In rare cases, you might need to delete individual files and remove Registry entries. This might be the only solution when a new virus has infected a system and there is no antivirus definition released. Instructions on how to remove viruses in this manner can be found on AV software manufacturers' websites.

When it comes to boot sector viruses, your AV software is still the best bet. The AV software might use a boot disc (or bootable USB flash drive) to accomplish scanning of the boot sector, or it might have boot shielding built in. Some BIOS programs have the capability to scan the boot sector of the hard drive at startup; this might need to be enabled in the BIOS setup first. You can use the command-line to repair the boot sector. Windows versions starting with Vista offer the `bootrec /fixmbr` command from within the System Recovery Options Command Prompt (part of the

Windows Recovery Environment, aka WinRE). Windows XP and older versions of Windows offer the `FIXMBR` command available from the Recovery Console.

NOTE It is also possible to use older commands such as the DOS `sys` command to restore the first sector, or the `FDISK/MBR` command to repair the master boot record within the boot sector, but DOS-based bootable media of some kind is necessary to do this; it needs to be created on a DOS-based computer or downloaded from the Internet.

Another possibility is to use freely downloadable Linux-based tools such as Knoppix, which can be used to boot and repair the computer. That can be downloaded from: <http://knoppix.net/>

Keep in mind that the Recovery Console, System Recovery Options Command Prompt, and other command-line methods might not fix the problem; they might render the hard drive inoperable depending on the type of virus. So, it is best to use the AV software's various utilities that you have purchased for the system.

Preventing and Troubleshooting Worms and Trojans

Worms and Trojans can be prevented and troubleshooted in the same manner as viruses. There are free online scanners for Trojans, but in most cases, standard AV software scans for worms and Trojans in addition to viruses (and perhaps other malware as well). Usually, AV software can easily detect remote access Trojans, which were mentioned previously in the chapter, either by detecting the attacker's actual application or by detecting any .exe files that are part of the application and are used at the victim computer.

Prevention is a matter of maintenance, and careful user interaction with the computer. Keeping the AV software up to date is important once again, but even more important becomes the user's ability to use the computer properly—to navigate only to legitimate websites and to screen e-mail carefully.

Troubleshooting these types of malware is done in basically the same way as with viruses. The malware should be quarantined and/or removed if at all possible with AV software or with advanced techniques mentioned in the previous section. The same prevention and troubleshooting techniques apply to ransomware because it is often delivered in the form of a Trojan.

Preventing and Troubleshooting Spyware

Preventing spyware works in much the same manner as preventing viruses when it comes to updating the operating system and using a firewall. Also, because spyware is as common as viruses, antivirus companies and OS manufacturers add anti-spyware components to their software. Here are a few more things you can do to protect your computer in the hopes of preventing spyware:

- Use (or download) and update built-in anti-spyware programs such as Windows Defender or Microsoft Security Essentials. Be sure to keep the anti-spyware software updated.
- Adjust web browser security settings. For example, disable (or limit) cookies, create and configure trusted zones, turn on phishing filters, restrict unwanted websites, turn on automatic website checking, disable scripting (such as Java-Script and ActiveX), and have the browser clear all cache on exit. All of these things can help to filter out fraudulent online requests for usernames, passwords, and credit card information, which is also known as web-page spoofing. Higher security settings can also help to fend off session hijacking, which is the act of taking control of a user session after obtaining or generating an authentication ID. We'll talk more about web browser security in Chapter 4, "Application Security."
- Uninstall unnecessary applications and turn off superfluous services (for example, Remote Desktop services or FTP if they are not used).
- Educate users on how to surf the web safely. User education is actually the number one method of preventing malware! Access only sites believed to be safe, and download only programs from reputable websites. Don't click OK or Agree to close a window; instead press Alt+F4 on the keyboard to close that window. Be wary of file-sharing websites and the content stored on those sites. Be careful of e-mails with links to downloadable software that could be malicious.
- Consider technologies that discourage spyware. For example, use a browser that is less susceptible to spyware. Consider running a browser within a virtual machine, or take it to the next level and run the entire operating system in a virtual machine!

Here are some common symptoms of spyware:

- The web browser's default home page has been modified.
- A particular website comes up every time you perform a search.
- Excessive pop-up windows appear.

- The network adapter's activity LED blinks frequently when the computer shouldn't be transmitting data.
- The firewall and antivirus programs turn off automatically.
- New programs, icons, and favorites appear.
- Odd problems occur within windows (slow system, applications behaving strangely, and such).
- The Java console appears randomly.

To troubleshoot and repair systems infected with spyware, first disconnect the system from the Internet (or simply from the local area network). Then, try uninstalling the program from the Control Panel or Settings area of the operating system. Some of the less malicious spyware programs can be fully uninstalled without any residual damage. Be sure to reboot the computer afterward and verify that the spyware was actually uninstalled! Next, scan your system with the AV software to remove any viruses that might have infested the system, which might get in the way of a successful spyware removal. Again, in Windows, do this in Safe Mode if the AV software offers that option.

NOTE In some cases, Safe Mode is not enough, and you need to boot off of a disc with a bootable OS or kernel (Knoppix, for example) and then rerun the scans.

Next, scan the computer with the anti-spyware software of your choice in an attempt to quarantine and remove the spyware. You can use other programs, such as HijackThis, in an attempt to remove malware, but be careful with these programs because you will probably need to modify the Registry. Remove only that which is part of the infection.

Finally, you need to make sure that the malware will not re-emerge on your system. To do this, check your home page setting in your browser, verify that your HOSTS file hasn't been hijacked (located in C:\WINDOWS\system32\drivers\etc), and make sure that unwanted websites haven't been added to the Trusted Sites within the browser.

Badware

Viruses, spyware, and other types of malware are sometimes lumped into the term *badware*. Although all the aforementioned attacks are indeed malicious, some types of badware are not malicious in their intent, but the user loses a certain amount of control when they utilize them. An example of this is a shopping toolbar that aids in the shopping process, but simultaneously records where the person was shopping and what was bought, and sends that information back to the badware's main server without the user's knowledge or consent. Another example is where a user installs a particular program that is legitimate except for the fact that it installs another program (possibly spyware or scareware) without the user's consent. In a nutshell, badware is software that does things you do not want it to do, often without your consent. The best way for a user to protect against badware in general is to be careful what is installed on the computer, and to only install software from legitimate, authentic entities, while being wary of any unknown removable media before connecting it to the computer.

Preventing and Troubleshooting Rootkits

A successfully installed rootkit enables unauthorized users to gain access to a system and act as the root or administrator user. Rootkits are copied to a computer as a binary file; this binary file can be detected by signature-based and heuristic-based antivirus programs, which we discuss later in this chapter in the “Host-Based Intrusion Detection Systems” section. However, after the rootkit is executed, it can be difficult to detect. This is because most rootkits are collections of programs working together that can make many modifications to the system. When subversion of the operating system takes place, the OS can't be trusted, and it is difficult to tell if your antivirus programs run properly, or if any of your other efforts have any effect. Although security software manufacturers are attempting to detect running rootkits, it is doubtful that they will be successful. The best way to identify a rootkit is to use removable media (a USB flash drive or a special rescue CD-ROM) to boot the computer. This way, the operating system is not running, and therefore the rootkit is not running, making it much easier to detect by the external media. Programs that can be used to detect rootkits include the following:

- **GMER:** <http://www.gmer.net/>
- **TDSSKiller:** <http://support.kaspersky.com/viruses/disinfection/5350>
- **Microsoft Sysinternals Rootkit Revealer:**
<http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx> (for older Windows systems)
- **chkrootkit:** www.chkrootkit.org/ (for Linux/OS X systems)

Sometimes, rootkits will hide in the MBR. Often, operating system manufacturers recommend scrubbing the MBR (rewriting it, for example, within System Recovery Options or with the Windows Recovery Console) and then scanning with antivirus software. This depends on the type of rootkit.

Unfortunately, because of the difficulty involved in removing a rootkit, the best way to combat rootkits is to reinstall all software (or re-image the system). Generally, a PC technician, upon detecting a rootkit, will do just that, because it usually takes less time than attempting to fix all the rootkit issues, plus it can verify that the rootkit has been removed completely.

Preventing and Troubleshooting Spam

The Internet needs to be conserved, just like our environment. Might sound crazy, but it's true. There is only so much space to store information, and only so much bandwidth that can be used to transfer data. It is estimated that spam causes billions of dollars in fraud, damage, lost productivity, and so on every year; besides botnets and P2P networks, it's one of the biggest gobblers of Internet resources. The worst part is that most spammers do not bear the burden of the costs involved; someone else usually does. So the key is to block as much spam as possible, report those who do it, and train your users. Here are several ways to implement anti-spam security controls and, hopefully, reduce spam:

- **Use a spam firewall/filter:** This can be purchased as software for the server or as an appliance. One example of an appliance is the Barracuda Spam Firewall (www.barracuda.com). Barracuda monitors spam activity and creates and updates whitelists and blacklists, all of which can be downloaded to the appliance automatically. Network administrators should also block any e-mails that include attachments that do not comply with company rules. For example, some companies enable only .zip, .txt, .doc, and .docx to go through their e-mail attachment filter (or .zips only). If your company uses a web-hosting company for its website and for e-mail, that company likely has many spam filtering options. And on the client side, you can configure Outlook and other mail programs to a higher level of security against spam; this is usually in the Junk E-mail Options area, as shown in Figure 2-2. Spam filters can also be installed on individual clients. Many popular antivirus suites have built-in spam filtering. Make sure it is enabled! Just as an example, my personal e-mail account (which I try to keep private) has a filter at the web hosting company, plus my antivirus software package filters the e-mails, and Outlook is set to High in the Junk E-mail Options page, and of course, I still get at least several spams to my inbox every single day!

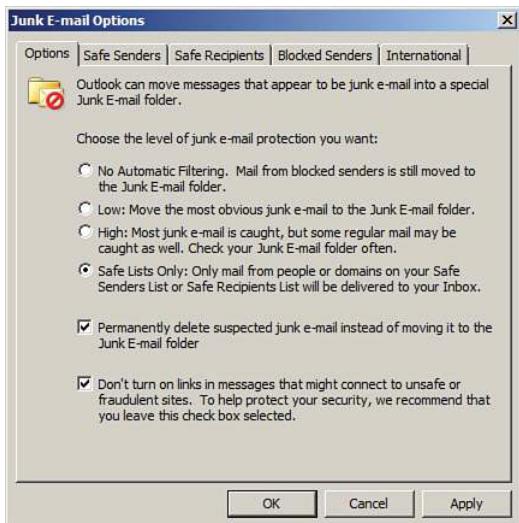


Figure 2-2 Outlook Junk E-mail Options Set at Highest Level of Security

- **Close open mail relays:** SMTP servers can be configured as **open mail relays**, which enables anyone on the Internet to send e-mail through the SMTP server. Although this is desirable to customers of the company that runs the SMTP server, it is not desirable to the company to have a completely open mail relay. So, open mail relays should either be closed or configured in such a way that only customers and properly authenticated users can use them. Open mail relays are also known as *SMTP open relays*.
- **Remove e-mail address links from the company website:** Replace these with online forms (secure PHP or CGI forms) that enable a person to contact the company but not see any company e-mail addresses. Use a separate advertising e-mail address for any literature or ads. Consider changing this often; marketing people might already do this as a form of tracking leads. Taking it to the next level, consider an e-mail service.
- **Use whitelists and blacklists:** Whitelists are lists of e-mail addresses or entire e-mail domains that are trusted, whereas blacklists are lists of e-mail addresses or e-mail domains that are not trusted. These lists can be set up on e-mail servers, e-mail appliances, and within mail client programs such as Outlook.
- **Train your users:** Have them create and use a free e-mail address whenever they post to forums, tech support portals, and newsgroups, and instruct them not to use their company e-mail for anything except company-related purposes. Make sure that they screen their e-mail carefully; this is also known as e-mail vetting. E-mail with attachments should be considered volatile unless

the user knows exactly where it comes from. Train your employees never to make a purchase from an unsolicited e-mail. Also, explain the reasoning behind using blind carbon copy (BCC) when sending an e-mail to multiple users. Let's not beat around the bush; we all know that this is the most difficult thing to ask of a company and its employees who have more important things to do. However, some companies enforce this as policy and monitor users' e-mail habits. Some companies have a policy in place in which users must create a "safe" list. This means that only the addresses on that list can send e-mail to the user and have it show up in the inbox.

You Can't Save Every Computer from Malware!

On a final and sad note, sometimes computers become so infected with malware that they cannot be saved. In this case, the data should be backed up (if necessary by removing the hard drive and slaving it to another system), and the operating system and applications reinstalled. The BIOS of the computer should also be flashed. After the reinstall, the system should be thoroughly checked to make sure that there were no residual effects and that the system's hard drive performs properly.

Summary of Malware Prevention Techniques

Table 2-2 summarizes the malware prevention techniques discussed up to this point.



Table 2-2 Summary of Malware Prevention Techniques

Malware Threat	Prevention Techniques
Virus	Run and update antivirus software. Scan the entire system periodically. Update the operating system. Use a firewall.
Worm	Run and update antivirus software. Scan the entire system periodically.
Trojan horse	Run and update antivirus software. Scan the entire system periodically. Run a Trojan scan periodically.
Spyware	Run and update anti-spyware software. Scan the entire system periodically. Adjust web browser settings. Consider technologies that discourage spyware.

Malware Threat	Prevention Techniques
Rootkit	Run and update antivirus software. Use rootkit detector programs.
Spam	Use a spam filter. Configure whitelists and blacklists. Close open mail relays. Train your users.

Implementing Security Applications

In the preceding section, we discussed antivirus suites such as McAfee, Norton, and so on. These application suites usually have antivirus, anti-spyware, and anti-spam components. Often, they also have a built-in firewall, known as a personal firewall. And perhaps the application suite also has a built-in *intrusion detection system (IDS)*, a piece of software that monitors and analyzes the system in an attempt to detect malicious activities. The type of IDS that a client computer would have is a **host-based intrusion detection system (HIDS)**. But there are other types of standalone software firewalls and HIDSs; we cover these in just a bit. Another type of built-in security is the pop-up blocker. Integrated into web browsers and web browser add-ons, pop-up blockers help users avoid websites that could be malicious. Let's discuss these security applications in a little more depth, starting with personal firewalls.

Personal Software Firewalls

Personal firewalls are applications that protect an individual computer from unwanted Internet traffic. They do so by way of a set of rules and policies. Some personal firewalls (also known as host-based firewalls) prompt the user for permission to enable particular applications to access the Internet. In addition, some personal firewalls now also have the capability to detect intrusions to a computer and block that intrusion; this is a basic form of a HIDS that we talk more about in the next section.

Examples of software-based personal firewalls include the following:

- **Windows Firewall:** Built into Windows, the basic version is accessible from the Control Panel in Windows Vista and newer, and from the network adapter's Properties window in Windows XP and older. The advanced version, Windows Firewall with Advanced Security, can be accessed (for example, in Windows 7) by typing `wf.msc` in the Run prompt or Command Prompt. This advanced version enables a user to perform more in-depth configurations such as custom rules.

NOTE For a quick tutorial on using Windows Firewall with Advanced Security, see the following link:
<http://www.davidlprowse.com/articles/?p=896>

- **ZoneAlarm:** Originally a free product that is still available (see the following link), this was purchased by Check Point and is now also offered as part of a suite of security applications. Go to www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm
- **ipfirewall (ipfw):** Built into some versions of FreeBSD, and OS X (newer OS X versions are also graphical, titled “Firewall”).
- **iptables:** Built into Linux systems. Can be extended upon using various configuration tools and third-party add-ons.

Antivirus application suites from Norton, McAfee, Kaspersky, and so on include personal firewalls as well. This has become a common trend over the past few years, and you can expect to see personal firewall applications built into most antivirus application suites in the future.

Because they are software, and because of the ever-increasing level of Internet attacks, personal firewalls should be updated often, and in many cases it is preferable to have them auto-update, although this depends on your organization’s policies.

As software, a personal firewall can utilize some of the computer’s resources. In the late 1990s and early 2000s, there were some complaints that particular antivirus suites used too much CPU power and RAM, sometimes to the point of crashing the computer; in some cases this was because of the resources used by the firewall. Today, some antivirus suites still run better than others, depending on the scenario. So a smart systems administrator selects an application suite that has a small footprint, and one that works best with the organization’s platforms and applications. Some organizations opt not to use personal firewalls on client computers and instead focus more on network-based firewalls and other security precautions. The choice of whether to use personal firewalls, network-based firewalls, or both can vary but careful analysis should be performed before a decision is made. For example, take an organization that accepts credit card payments over the phone and performs the transactions over the Internet. The individual computers that are used to carry out the transactions need to have a personal firewall installed with the proper ports filtered in order to comply with financial regulations.

Personal firewalls (like any software application) can also be the victim of attack. If worms or other malware compromise a system, the firewall could be affected. This just reinforces the concept that antivirus suites should be updated often; daily updates would be the optimal solution.

A common scenario for security in small offices and home offices is to have a four-port SOHO router/firewall protecting the network and updated personal firewalls on every client computer. This combination provides two levels of protection for the average user, which is usually adequate. But larger networks usually concentrate more on the network firewall(s) and network-based IDS(s) than on personal firewalls, although it is common to see both levels of firewall security in larger networks as well.

Host-Based Intrusion Detection Systems

Let's start by talking about intrusion detection systems (IDSs) in general. An IDS is used to monitor an individual computer system or a network, or a portion of a network, and analyze data that passes through to identify incidents, attacks, and so forth. You should be aware of two types of IDSs for the exam:

- **Host-based intrusion detection system (HIDS):** Loaded on an individual computer, it analyzes and monitors what happens inside that computer—for example, whether any changes have been made to file integrity. A HIDS is installed directly within an operating system, so it is not considered to be an “inline” device, unlike other network-based IDS solutions. One of the advantages of using a HIDS is that it can interpret encrypted traffic. Disadvantages include its purchase price, its resource-intensive operation, and its default local storage of the HIDS object database; if something happens to the computer, the database will be unavailable.
- **Network intrusion detection system (NIDS):** Can be loaded on the computer, or can be a standalone appliance, but it checks all the packets that pass through the network interfaces, enabling it to “see” more than just one computer; because of this, a NIDS is considered to be an “inline” device. Advantages include the fact that it is less expensive and less resource intensive, and an entire network can be scanned for malicious activity as opposed to just one computer. Of course, the disadvantage is that a NIDS cannot monitor for things that happen within an operating system. For more information about NIDS solutions, see the section “NIDS Versus NIPS” in Chapter 7, “Network Perimeter Security.”

Following are two main types of monitoring that an IDS can carry out:

- **Statistical anomaly:** It establishes a performance baseline based on normal network traffic evaluations, and then compares current network traffic activity with the baseline to detect whether it is within baseline parameters. If the sampled traffic is outside baseline parameters, an alarm is triggered and sent to the administrator.

- **Signature-based:** Network traffic is analyzed for predetermined attack patterns, which are known as *signatures*. These signatures are stored in a database that must be updated regularly to have effect. Many attacks today have their own distinct signatures. However, only the specific attack that matches the signature will be detected. Malicious activity with a slightly different signature might be missed.

For more information about the various types of monitoring methodologies, see the section “Monitoring Methodologies” in Chapter 12, “Monitoring and Auditing.”

IDS solutions need to be accurate and updated often to avoid the misidentification of legitimate traffic or, worse, the misidentification of attacks. Following are two main types of misidentification you need to know for the exam:

- **False positive:** The IDS identifies legitimate activity as something malicious.
- **False negative:** The IDS identifies an attack as legitimate activity. For example, if the IDS does not have a particular attack’s signature in its database, the IDS will most likely not detect the attack, believing it to be legitimate, and the attack will run its course without any IDS warnings. More information about false positives, false negatives, and other IDS terminology can be found in Chapter 9, “Physical Security and Authentication Models.”

Some antivirus application suites have basic HIDS functionality, but true HIDS solutions are individual and separate applications that monitor log files, check for file integrity, monitor policies, detect rootkits, and alert the administrator in real time of any changes to the host. This is all done in an effort to detect malicious activity such as spamming, zombie/botnet activity, identity theft, keystroke logging, and so on. Three examples of HIDS applications include the following:

- **Trend Micro OSSEC** (www.ossec.net): A free solution with versions for Windows, OS X, Linux, and Unix
- **Verisys** (www.ionx.co.uk/products/verisys): A commercial HIDS solution for Windows
- **Tripwire** (<http://www.tripwire.com/it-security-software/scm/file-integrity-monitoring/>): Another commercial HIDS solution

There are several compliance regulations that require the type of file integrity monitoring that a HIDS can provide, including PCI DSS and NIST 800-53. When selecting a HIDS, make sure it meets the criteria of any compliance regulations that your organization must adhere to.

It is important to protect the HIDS database because this can be a target for attackers. It should either be encrypted, stored on some sort of read-only memory, or stored outside the system.

If an IDS observes an incident, it notifies the systems or network administrator so that she might quarantine and fix the problem. However, over time, the need for prevention has become more desirable, and so *intrusion prevention systems* (IPs) and intrusion detection and prevention systems (IDPs) were developed. These not only detect incidents and attacks, but also attempt to prevent them from doing any real damage to the computer or to the network. Once again, typical companies such as McAfee and Norton (and the aforementioned HIDS providers) offer host-based intrusion prevention systems. There are also downloadable implementations for Linux that prevent malicious code from executing, such as Security-Enhanced Linux (SELinux). It is a set of kernel modifications originally developed by the National Security Agency (NSA) but was released to the open source community for download. We talk more about this in Chapter 10, “Access Control Methods and Models.”

A security administrator can review the logs of a host-based IDS at any time. However, if the computer has been shut down, the administrator will not be able to review information pertaining to system processes and network processes, nor information stored in memory, because all those items are volatile. HIDS logs that refer to archived storage, the MBR, the system disk, e-mail, and so on will still be available for review. By reviewing the logs of a HIDS, a security administrator can find out if the computer has been compromised by malware, or if it is communicating with a botnet.

Pop-Up Blockers

For a website to generate revenue, a webmaster often advertises other products and services, charging fees to the organization that creates these products and services. The only way that an organization can continually advertise on the website is if it is positive it will get a certain amount of click-through response for its ads. However, web users quickly learn to define which windows are advertisements and which aren't. So advertisers need to constantly create new and exciting ways to advertise their products. The traditional JavaScript-based pop-up window doesn't do as good of a job as it used to because many web browsers have built-in pop-up blockers, but you still see tons of them on the Internet, perhaps in other formats such as Flash. They can take their toll on user productivity—and can be detrimental to the user's computer. For example, some pop-up ads, if clicked, force the user to go to one or more separate websites that could have harmful code. Or worse yet, the pop-up itself could have malicious code built in; perhaps the Close button within the ad launches some other process altogether.

Some attackers create entire websites with malicious pop-ups just to infect as many computers as they can. You might ask: “Why take advantage of users?” Some attackers might answer: “Because they are there to be taken advantage of!” Not that I condone this behavior, but this mentality is infectious, making pop-ups and all their

cousins common; so systems administrators should try their best to block pop-ups. One way to do this is with a **pop-up blocker**. Following are some examples of web browsers that have built-in pop-up blocking functionality, and web browser add-on pop-up blocking tools:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Google Toolbar (add-on); <http://www.google.com/toolbar/ie/index.html>
- Adblock Plus (add-on); <https://adblockplus.org/en/chrome>
- Safari

One of the problems with pop-up blocking is that it might block content that is not an advertisement but instead is integral to the actual website. For example, I used to run a bulletin board system that has the capability to let users know that they have new private messages from other users; one of the options is for this alert to show up as a pop-up window. Because so many users do not see this alert, and instead get a message from the browser that says “Pop-up blocked” or something similar, which can look sort of suspicious to the user, I decided to turn off that functionality and instead let the main login page of the website (and e-mails) notify the user of new messages. This type of philosophy should be taken into account by webmasters when they define what the purpose of their website will be. Proper website functionality should be integrated directly into the actual web page, because most users ignore pop-ups or consider them malicious and attempt to close them, or block them, if they weren’t otherwise blocked automatically by their browser.

When dealing with the previously listed applications and add-ons, pop-up blocking is known as **ad filtering**, but this can be taken to another level, known as content filtering. **Content filters** block external files that use JavaScript or images from loading into the browser. Content filtering continues to become more and more important as advertisers become more and more clever. Most newer web browser versions offer some kind of filtering. For example, Internet Explorer version 8 and higher has built-in content filtering, and Adblock Plus can provide the same functionality for Mozilla Firefox (on versions that don’t already have it), plus proxy-based programs such as Squid can filter content (among other things) for multiple computers. For more about proxy servers, see the section “Firewalls and Network Security” in Chapter 7.

Of course, advertisers have devised some new tricks in an attempt to get past the pop-up blockers and content filters: flash-based pop-ups, pop-under ads, dynamic HTML (DHTML) hover ads, and so on. Advertisers continue to battle for ad space

with smart new ad types, so systems administrators should be prepared to update their clients' web browsers and browser add-ons on a regular basis.

Data Loss Prevention Systems

Data loss prevention (DLP) is a concept that refers to the monitoring of data in use, data in motion, and data at rest. A DLP system performs content inspection and is designed to prevent unauthorized use of data as well as prevent the leakage of data outside the computer (or network) that it resides in. DLP systems can be software- or hardware-based solutions and come in three varieties:

- **Endpoint DLP systems:** These systems run on an individual computer and are usually software-based. They monitor data in use, such as e-mail communications, and can control what information flows between various users. These systems can also be used to inspect the content of USB-based mass-storage devices.
- **Network DLP systems:** These can be software- or hardware-based solutions and are often installed on the perimeter of the network. They inspect data that is in motion.
- **Storage DLP systems:** These are typically installed in data centers or server rooms as software that inspects data at rest.

As with HIDS solutions, DLP solutions must be accurate and updated to reduce the amount of false positives and false negatives. Most systems alert the security administrator in the case that there was a possibility of data leakage. However, it is up to the administrator to determine whether the threat was real.

Securing Computer Hardware, Peripherals, and Mobile Devices

Now that the operating system is better secured, let's talk about securing other types of computer hardware, BIOS, external peripheral devices, and mobile devices.

Although it's important to secure PCs, Macs, servers, and other hosts on the network, we can't forget about wireless devices such as laptops, tablets, and smartphones, nor the plethora of devices that can be connected to a computer system, such as USB flash drives, external SATA hard drives, and optical discs. When smaller, portable devices are not in use, the best way to protect them is to put them in a locking cabinet... and lock it! Of course there are other ways to protect those devices, including encryption, proper handling, GPS tracking, and so on. But the simple physical solution of locking them up, or putting them in a safe, is often overlooked in our high-tech society. Desktop computers and servers, on the other hand,

are too cumbersome to be locked in a cabinet. However, there are many options when securing those computers, including physical solutions such as cable locks. But what if you want to stop people from using USB connections and other devices on the computer? Well, there's the underlying firmware without which our computer could not run; I'm speaking of the BIOS, which can secure these ports and devices. However, the BIOS must be secured as well!

Securing the BIOS

The BIOS can be the victim of malicious attacks; for mischievous persons it can also act as the gateway to the rest of the system. Protect it! Or your computer just might not boot. Following are a few ways to do so:

- **Use a BIOS password:** The password that blocks unwanted persons from gaining access to the BIOS is the supervisor password. Don't confuse it with the user password (or power-on password) employed so that the BIOS can verify a user's identity before accessing the operating system. Both of these are shown in Figure 2-3. Because BIOS passwords are relatively weak compared to other types of passwords, organizations often use one password for the BIOS on every computer in the network; in this scenario, there is all the more reason to change the password at regular intervals. Because some computers' BIOS password can be cleared by opening the computer (and either removing the battery or changing the BIOS jumper), some organizations opt to use locking cables or a similar locking device that deters a person from opening the computer.

Key Topic



Figure 2-3 BIOS and Drive Lock Passwords

On a semi-related note, many laptops come equipped with *drive lock* technology; this might simply be referred to as an HDD password. If enabled, it prompts the user to enter a password for the hard drive when the computer is first booted. If the user of the computer doesn't know the password for the hard drive, the drive locks and the OS does not boot. An eight-digit or similar hard drive ID usually associates the laptop with the hard drive installed (refer to Figure 2-3). On most systems this password is clear by default, but if the password is set and forgotten, it can usually be reset within the BIOS. Some laptops come with documentation clearly stating the BIOS and drive lock passwords.

- **Flash the BIOS:** *Flashing* describes the updating of the BIOS. By updating the BIOS to the latest version, you can avoid possible exploits and BIOS errors that might occur. All new motherboards issue at least one new BIOS version within the first six months of the motherboard's release.
- **Configure the BIOS:** Set up the BIOS to reduce the risk of infiltration. For example, change the BIOS boot order (boot device priority) so that it looks for a hard drive first and not any type of removable media. Also, if a company policy requires it, disable removable media including the optical drives, floppy drives, eSATA ports, and USB ports.

Securing Storage Devices

The storage device is known to be a common failure point because many storage devices have moving parts or use removable media. Storage devices also can pose security risks because usually they are external from a computer system and are possibly located in an insecure area. Also, keeping track of removable media can be difficult. Some of the solutions to this include physical security, encryption, and policies that govern the use and storage of removable media. This section discusses removable storage devices, such as discs and external USB drives, network attached storage (NAS), and whole disk encryption such as BitLocker. Hardware security modules take hardware-based encryption to the next level—we also discuss the basics of how these HSMs operate.

Removable Storage

Removable storage, or removable media, includes optical discs, USB devices, eSATA devices, and even floppy disks in some cases. A network administrator can prevent access to removable media from within the BIOS and within the operating system policies. In many companies, all removable media is blocked except for specifically necessary devices, which are approved on a case-by-case basis. Users should be trained on the proper usage of removable media and should *not* be allowed to take any data home with them. Users who sometimes work from home

should do so via a virtual private network (VPN) connection to keep the data confidential, yet accessible.

USB devices must be carefully considered. They are small but can transport a lot of data. These devices can be the victim of attacks and can act as the delivery mechanism for attacks to a computer. For example, a USB flash drive might have data files or entire virtual operating systems that can be exploited by viruses and worms. Also, an attacker can install a special type of virus or worm onto the flash drive that is executed when the flash drive is connected to the computer; in this scenario the computer is the target for the malware. Organizations must decide whether to allow USB devices to be used. Organizational policies should state that USB sticks should not be carried from one department to another without proper security procedures in place. Operating system group policies can be implemented to enforce which users are allowed to use USB devices. As mentioned earlier, the BIOS can also disable the use of USB devices on a local computer. Finally, the data on a USB device can be encrypted with various programs—for example, Windows BitLocker—on the software side, or you might opt to purchase a secure USB flash drive, such as one by Ironkey (<http://www.ironkey.com/en-US/>).

Network Attached Storage

Network attached storage (NAS) is a storage device that connects directly to your Ethernet network. Basic home and office NAS devices usually contain two hard drives, enabling you to set up **RAID 1** mirroring, which protects your data if one drive fails. A more advanced example of NAS would be a device that looks more like a computer and might house up to 32 drives and contain terabytes of data. Possibly hot-swappable, these drives can be physically replaced, and the data can be rebuilt in a short amount of time. A NAS device might be part of a larger storage area network (SAN); therefore, network security should also be considered when implementing any type of NAS. For more information on network security, see Chapters 5 through 8. To protect a single NAS device, consider data encryption, authentication, and constant secure logging of the device.

Whole Disk Encryption

Encryption is a huge component of today's computer security. By encrypting information, the data is rearranged in such a way that only the persons with proper authentication can read it. To encrypt an entire hard drive, you need some kind of full disk encryption software. ("Disk", though not accurate in some cases, is the commonly used term here.) Several are currently available on the market; one developed by Microsoft is called BitLocker—available in the elite editions of several newer versions of Windows. This software can encrypt the entire disk, which, after complete, is transparent to the user. Following are some requirements for this:

- Trusted platform module (TPM)—A chip residing on the motherboard that actually stores the encrypted keys.
- or
- An external USB key to store the encrypted keys.
- and
- A hard drive with two volumes, preferably created during the installation of Windows. One volume is for the operating system (most likely C:) that will be encrypted; the other is the active volume that remains unencrypted so that the computer can boot. If a second volume needs to be created, the BitLocker Drive Preparation Tool can be of assistance and can be downloaded from the Microsoft Download Center.

BitLocker software is based on the Advanced Encryption Standard (AES) and can use 128-bit and 256-bit keys. Keep in mind that a drive encrypted with BitLocker usually suffers in performance compared to a nonencrypted drive and could have a shorter shelf life as well.

In the appropriate Windows version/edition, BitLocker security settings can be accessed via the following steps:

Step 1. Navigate to the Run prompt.

Step 2. Type `gpedit.msc` and press Enter.

Step 3. In the Group Policy Editor window, navigate to Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption.

Figure 2-4 shows the BitLocker configuration screen.

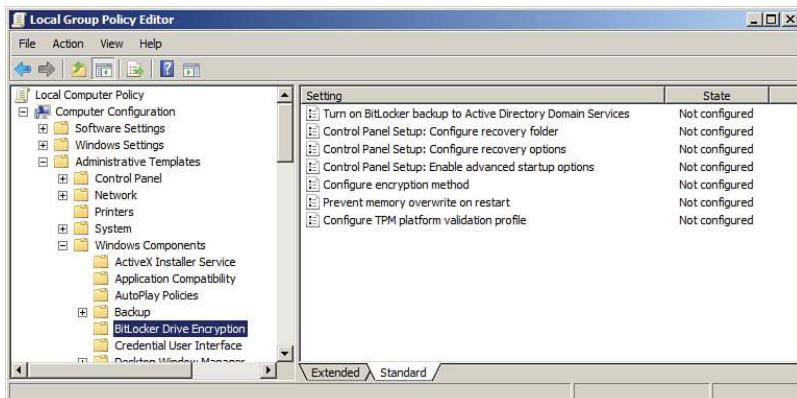


Figure 2-4 BitLocker Configuration Screen

NOTE For more information about BitLocker and how to use it, see the following links:

<http://windows.microsoft.com/en-us/windows-8/bitlocker-drive-encryption>

[http://technet.microsoft.com/en-us/library/cc766295\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc766295(WS.10).aspx)

Though it can be a lot of work to implement, double encryption can be a very successful technique when it comes to securing files. For example, a hard drive encrypted with BitLocker could also use EFS to encrypt individual files. This way, files that are copied to external media will remain encrypted, even though they don't reside on the drive using whole disk encryption.

Hardware Security Modules

Hardware security modules (HSMs) are physical devices that act as secure coprocessors. This means that they are used for encryption during secure login/authentication processes, during digital signings of data, and for payment security systems. The beauty of a hardware-based encryption device such as an HSM (or a TPM) is that it is faster than software encryption.

HSMs can be found in adapter card form, as devices that plug into a computer via USB, and as network-attached devices. They are generally tamper-proof, giving a high level of physical security. They can also be used in high-availability clustered environments because they work independently of other computer systems and are used solely to calculate the data required for encryption keys. However, many of these devices require some kind of management software to be installed on the computer they are connected to. Some manufacturers offer this software as part of the purchase, but others do not, forcing the purchaser to build the management software themselves. Due to this lack of management software, and the cost involved in general, HSMs have seen slower deployment with some organizations. This concept also holds true for hardware-based drive encryption solutions.

Often, HSMs are involved in the generation, storage, and archiving of encrypted key pairs such as the ones used in Secure Sockets Layer (SSL) sessions online, public key cryptography, and public key infrastructures (PKIs), which we discuss more in Chapter 13 and Chapter 14.

Securing Mobile Devices

Unfortunately, smartphones and tablets (and other mobile devices) can be the victims of attack as well. Attackers might choose to abuse your service or use your

device as part of a larger scale attack, and possibly to gain access to your account information. Though mobile devices can be considered “computers,” and most of the information mentioned in this chapter applies to them as well, there are some other things we should consider specifically for the mobile device.

Users of mobile devices should be careful who they give their phone number to, and should avoid listing their phone number on any websites, especially when purchasing products. Train your users not to follow any links sent by e-mail or by text messages if these are unsolicited. (If there is any doubt in the user’s mind, then it is best to ignore the communication.) Explain the issues with much of the downloadable software, such as games and ringtones, to your users. Use a locking code/password/gesture that’s hard to guess; this locks the mobile device after a specific amount of time has lapsed. Use complex passwords when necessary.

In general, mobile operating system software must be updated just like desktop computer software; keep these devices up to date, and there will be less of a chance that they will be affected by viruses and other malware. You can encrypt data in several ways, and some organizations have policies that specify how data will be encrypted. More good general tips are available at the following National Cyber Awareness System (NCAS) and U.S. Computer Emergency Readiness Team (US-CERT) website links:

- <https://www.us-cert.gov/ncas>
- www.us-cert.gov/ncas/tips/ST05-017.html
- www.us-cert.gov/ncas/tips/ST04-020.html

Let’s discuss some of the attacks and other concerns for mobile devices, as well as ways to prevent these things from happening, and how to recover from them if they do occur.

Malware

It’s not just Windows that you have to worry about when it comes to malware. Every operating system is vulnerable, some less than others. Historically, in the mobile device marketplace, Android has proven to be somewhat of a stomping ground for malware; for example, the GinMaster Trojan steals confidential information from the Android device and sends it to a remote website. Viruses, worms, rootkits, and other types of malware are commonly found in the Android OS, and are sometimes found in iOS and other mobile device operating systems.

As with desktop operating systems, mobile operating systems should be updated to the newest version possible (or the point release for the version installed). AV software can also be used. Newer models of mobile devices come with built-in security

programs such as Lookout Security and Antivirus for Android. These programs should be updated regularly, and configured for optimal security. Care should be taken when tapping links within e-mails, texts, or social media networks. Personal or organizational information should never be shared on social networks, and should usually not be stored on the mobile device.

NOTE Social engineering attacks are also quite common on mobile devices. Techniques such as hoaxes, pretexting, phishing, and many more are commonplace. We'll discuss how to combat social engineering in general within Chapter 16, "Policies, Procedures, and People."

Botnet Activity

Mobile devices can be (and are) part of botnets as well. Because they are more easily accessible than desktop computers at this point, they make up a big part of some of today's botnets. A mobile device can take part in the launching of distributed denial-of-service (DDoS) attacks, or inadvertently join in with a click fraud outfit, or could be part of a scam to get users of other mobile devices to send premium-rate Short Message Service (SMS) messages. And that's just the beginning. Methods for preventing a mobile device from joining a botnet (without the user's knowledge) are similar to those mentioned previously concerning malware. Great care should be taken when downloading applications. The user should make sure the apps are from a legitimate source. Also, rooting (or jailbreaking) the mobile device is not recommended. The programs used in conjunction with rooting the device are often malicious, or are closely aligned with other malicious programs. If it appears that a device has become part of a botnet, that device should be wiped, either by a hard reset or other means.

SIM Cloning

Another attack on smartphones is SIM cloning (also known as phone cloning), which allows two phones to utilize the same service and allows an attacker to gain access to all phone data. V1 SIM cards had a weak algorithm that made SIM cloning possible (with some expertise). However, V2 cards and higher are much more difficult (if not impossible) to clone due to a stronger algorithm on the chip. Users and administrators should be aware of the version of SIM card being used and update it (or the entire smartphone) if necessary.

Wireless Attacks

Anytime a cell phone or smartphone connects, it uses some type of wireless service. Whether it's 4G, 3G, GSM, Wi-Fi, infrared, RFID, or Bluetooth, security implications exist. To minimize risks, the best solution is to turn off the particular service when not in use, or simply turn the mobile device off altogether if it is not being used.

Bluetooth is especially vulnerable to virus attacks, as well as bluejacking and bluesnarfing.

Bluejacking is the sending of unsolicited messages to Bluetooth-enabled devices such as mobile phones. Bluejacking can be stopped by setting the affected Bluetooth device to “undiscoverable” or by turning off Bluetooth altogether.

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection. Generally, bluesnarfing is the theft of data (calendar information, phonebook contacts, and so on). Ways of discouraging bluesnarfing include using a pairing key that is not easy to guess; for example, stay away from 0000 or similar default Bluetooth pairing keys! Otherwise, Bluetooth devices should be set to “undiscoverable” (only after legitimate Bluetooth devices have been set up, of course), or Bluetooth can be turned off altogether.

For more information about Bluetooth vulnerabilities (and other wireless attacks in general), see the section “Securing Wireless Networks” in Chapter 8, “Securing Network Media and Devices.”

Theft

Over 100 mobile devices end up missing (often stolen) every minute. Let me repeat—every minute! You can imagine the variety of reasons why this is. The worst attack that can be perpetuated on a smartphone or tablet is theft. The theft of a mobile device means the possible loss of important data and personal information. There are a few ways to protect against this loss of data, and recover from the theft of a mobile device if it does happen.

First, mobile devices in an organization should utilize data encryption. The stronger the encryption, the more difficult it is for a thief to decode and use the data on the device. If at all possible, use *full device encryption*, similar to Windows BitLocker. The actual conversations on phones can also be encrypted. Voice encryption can protect the confidentiality of spoken conversations and can be implemented with a special microSD chip (preferably) or with software.

Mobile devices should also be set up for GPS tracking so that they can be tracked if they are lost or stolen. The quicker a device can be located, the less risk of data loss, especially if it is encrypted. However, GPS tracking can also be a security vulnerability if an attacker knows how to track the phone.

The beauty of mobile devices is in their inherent portability—that and the ability to track SIM cards. Administrators of mobile devices should consider remote *lock-out* programs. If a device is lost or stolen, the admin can lock the device, disallowing a would-be attacker access. In addition, the device can be configured to use the “three strikes and you’re out” rule, meaning that if a user tries to be authenticated to the device and is unsuccessful after three attempts, the user is locked out. Taking it to the next level, if the data is extremely sensitive, you might want to consider a remote wipe program. If the mobile device is reported as lost or stolen, these programs can remove all data from the phone in a bit by bit process, making it difficult (if not impossible) to recover. This is known as *sanitizing* the phone remotely. Of course, a solid backup strategy should be in place before a remote wipe solution is implemented.

Screen locks, complex passwords, and taking care when connecting to wireless networks are also important. Though a screen lock won’t deter the knowledgeable hacker, it will usually deter the average person who, for example, finds a stray phone sitting in a coffee shop, mall, or other public location. User training should be implemented when users first receive their device. Though many organizations don’t take the time to do this, it is a great way to show users how to secure their device, and also check whether their encryption, GPS tracking, and other features are working properly. They can also be trained on how to inform your organization and local law enforcement in the case that a device is lost or stolen, effectively reducing the risk of data loss by allowing you to find the device faster or mitigate the problem in other ways.

NOTE In the case of theft, the two best ways to protect against the loss of confidential or sensitive information are encryption and a remote wipe program.

Application Security

Let’s speak more about the applications’ security on mobile devices. We’ve already mentioned that applications should (usually) be updated to the latest version, and discussed the importance of proper user interaction; but let’s delve a bit deeper and talk about ways to encrypt data that is transferred through applications.

Encryption is one of the best ways to ensure that data is secured and that applications work properly without interference from potential attackers. However, a security administrator should consider whole device encryption, which encrypts the internal memory and any removable (SD) cards. Sometimes an admin might forget about one or the other. Then there is data in transit; data that is on the move between a

client and a server. Most applications for mobile devices communicate with a server of some sort; for example, when a person uses a web browser, an e-mail client, a contacts database, or actual “apps” that work independently of a browser, but operate in a similar manner, meaning that they ultimately connect to a server. Weather apps, games, social media apps, and so on all fall into this category.

Let’s consider the web browser, for instance. A mobile device will connect to websites in a very similar manner as a desktop computer. Basic websites will use a Hypertext Transfer Protocol (HTTP) connection. But websites that require any type of personally identifiable information (PII) will use HTTP Secure (HTTPS). This can then utilize one of several types of encryption, such as Transport Layer Security (TLS).

NOTE We’ll discuss HTTPS, TLS, and many other security protocols in more depth within Chapter 13.

Whatever the security protocol, the important point here is that the server connected to makes use of some kind of database that stores encryption keys. The key (or a portion thereof) is sent to the client device and is agreed upon (handshaking occurs) so that the transfer of data, especially private information, is encrypted and protected. Often, HTTPS pages are used to aid in the process of authentication—the confirmation of a person’s (or computer’s) identity, typically with the help of a username/password combination. Examples of this include when you log in to your account with a bank or with a shopping portal.

One of the important roles for the server is key management—the creation, storage, usage, and retirement of encryption keys. Proper key management (and the regular updating of keys) is a security administrator’s primary concern. Generally, an organization will purchase a master key algorithm from a third-party company such as VeriSign. That company informs the organization if a key has become compromised and needs to be revoked. These third parties might also take part in credential management (the managing of usernames, passwords, PINs, and other passcodes, usually stored within a secure database) to make things a bit easier for the security administrator. It depends on the size of the organization and its budget. This gets quite in-depth, as you can imagine. For now, realize that a mobile device is an easy target. Therefore, applications (especially third-party apps) should be scrutinized to make sure they are using a solid encryption plan when personal information is transferred back and forth. Of course, we’ll get more into encryption and key management within Chapters 13 and 14.

Authentication to servers and other networks (and all of their applications) can get even more complicated when the concept of transitive trust is implemented. Effectively, a transitive trust is when two networks (or more) have a relationship such that users logging in to one network get access to data on the other. In days gone by, these types of trusts were created automatically between different sections of networks. However, it was quickly realized that this type of transitivity was insecure, allowing users (and potential attackers) access to other networks that they shouldn't have had access to in the first place. There's a larger looming threat here as well. The transitive trust is based on the transitive property in mathematics, which states that if A is equal to B, and B is equal to C, then A is automatically equal to C. Put into computer terms: if the New York network trusts the California network, and the California network trusts the Hong Kong network, then the New York network automatically trusts the Hong Kong network. You can imagine the security concerns here, as well as the domino effect that could occur. So, organizations will usually prefer the non-transitive trust, where users need to be authenticated to each network separately, and therefore are limited to the applications (and data) they have access to on a per-network basis.

To further restrict users, and increase application security, **application whitelisting** is often used. This means that a list of approved applications is created by the administrator and that the user can work with those applications only, and no others. This is often done within a computer policy and can be made more manageable by utilizing a mobile device management system (which we will detail a bit later). Users often only need access to several apps: phone, e-mail, contacts, and web browser. These applications would make up the whitelist, and if a user tried to use other apps, they would be denied, or at the very least, would be prompted for additional user credentials. If a user needed access to another app, such as the camera, the security administrator would weigh the security concerns (GPS, links to social media, and so on) and decide whether or not to add the app to the whitelist. Contrast this with blacklisting, which is the common method used when working with e-mail, and by antivirus and HIDS programs.

Geotagging (also written as geo-tagging) is another application concern. Photos, videos, websites, messages, and much more can be geotagged. Geotagging is the adding of data to the content in question, helping users to gather location-specific information. For example, if a user wanted to take a picture of their favorite store at the mall and help friends to find it, the user could geotag the picture. However, this requires that the smartphone (or other mobile device) have GPS installed and running. This then means that the user's smartphone can be physically located and tracked. Depending on the applications running, this could pose a security threat. In a corporate environment, the security administrator will often choose to disable geotagging features. There are several privacy implications when it comes to geotagging. One of the most dangerous is the fact that many users don't even know

that they are geotagging their media when they do so—some of the applications are that transparent. For people in the company such as executives (who might carry a wealth of confidential information), this is the type of feature that should be disabled. If a potential attacker can track an executive, then the attacker can find out where the executive lives, determine when the executive is in the office, and determine the location of clients, all of which can help the attacker to commit corporate espionage. When it comes down to it, the usage of GPS in general should be examined carefully, weighing the benefits against the possible vulnerabilities. Many executives and other employees use their mobile devices at work, which brings up many security concerns besides GPS. Collectively these are known as BYOD concerns and are described in the following section.

BYOD Concerns

Around 2011, organizations began to allow employees to bring their own mobile devices into work and connect them to the organization’s network (for work purposes only, of course). This “bring your own device” concept has since grown into a more popular method of computing for many organizations. It is enticing from a budgeting standpoint, but can be very difficult on the security administrator, and possibly on the user as well.

In order to have a successful BYOD implementation, the key is to implement **storage segmentation**—a clear separation of organizational and personal information, applications, and other content. It must be unmistakable where the data ownership line occurs. For networks with a lot of users, consider third-party offerings from companies that make use of **mobile device management (MDM)** platforms. These are centralized software solutions that can control, configure, update, and secure remote mobile devices such as Android, iOS, BlackBerry, and so on, all from one administrative console. The MDM software can be run from a server within the organization, or administered within the cloud. It makes the job of a mobile IT security administrator at least manageable. From the central location, the security administrator can implement patch management (more on that in Chapter 3, “OS Hardening and Virtualization”) and antivirus management such as updates to the virus definitions. The admin can also set up more secure levels of mobile device access control. *Access control* is the methodology used to allow access to computer systems. (More on access control in Chapter 10, “Access Control Methods and Models.”) For larger organizations, MDM software makes it easy for an admin to view inventory control, such as how many devices are active for each of the mobile operating systems used. It also makes it simpler to track assets, such as the devices themselves, and the types of data each contains. In addition, MDM software makes it less complicated to disable unused features on multiple devices at once, thereby increasing the efficiency of the devices, reducing their footprint, and ultimately making them more secure. For

instance, an employee who happens to have both a smartphone and a tablet capable of making cellular calls doesn't necessarily need the latter. The admin could disable the tablet's cellular capability, which would increase battery efficiency as well as security for that device. Finally, application control becomes easier as well. Applications can be installed, uninstalled, updated, and secured from that central location. Even devices' removable storage (often USB-based) can be manipulated—as long as the removable storage is currently connected to the device.

User acceptance of BYOD is mixed in its reactions. Some employees like the idea of using their own device (which they might not have been allowed to use at work previously) and not having to train on a separate work computer. However, some employees believe that BYOD is just a way to move computing costs from the company to the user, and the level of trust is low. Around 2013, studies showed that the *perception* of BYOD (and MDM solutions) varied. Approximately 40 percent of users believe that their employer can see personal information on their mobile devices. This brings up a variety of legal concerns, such as the right to privacy. Companies that offer BYOD MDM solutions counter this by drawing a clear line in the sand, defining exactly what employers can see (for example, corporate e-mail) and what they can't see (such as personal texts). In general, these companies try to protect the privacy of the individual. Many organizations will write clear privacy policies that define, if necessary, selective wipes of secure corporate data while protecting personal data. As of the writing of this book, the technology is not perfect, and there will be some debate over time as to its long-term viability.

Part of the debate includes some additional concerns; for example, additional legal concerns exist about such things as employee misconduct and fraud. As of the writing of this book, legal precedents are being set, and the general consensus is gravitating toward a separation of personal and organizational data. Anything found that could possibly implicate an employee of wrongdoing would have to be found in the organizational portion of the data. From a forensics point of view, however, and because the device can't be split in two, if any potential wrongdoing is investigated, the device would need to be confiscated for analysis.

Most employees (of all age groups) are also concerned with how on-board devices (such as the on-board camera) can be used against them with or without their knowledge. Companies that offer BYOD solutions tend to refer to the camera (and photos/video taken) as part of the personal area of the device. However, those same companies will include GPS location as something the company can see, but this can be linked to a corporate login, with GPS tracking the user only when the user is logged in. On-boarding and off-boarding in general are another concern. Essentially, on-boarding is when the security administrator takes control of the device temporarily to configure it, update it, and perhaps monitor it, and off-boarding is when the security administrator relinquishes control of the device when finished

with it. It brings up some questions for the employee: When does it happen? How long does it last? How will my device be affected? Are there any architectural/infrastructural concerns? For example, will the BYOD solution change the core files of my device? Will an update done by a person when at home render the device inactive the next day at work? That's just the tip of the iceberg when it comes to questions and concerns about BYOD. The best course of action is for an organization to set firm policies about all of these topics.

Policies that need to be instituted include an acceptable use policy, a data ownership policy, and a support ownership policy. In essence, these define what a user is allowed to do with the device (during work hours), who owns what data and how that data is separated, and under what scenarios the organization takes care of technical support for the device as opposed to the user. We'll talk more about policies such as these in Chapter 16.

To help secure the mobile devices in a BYOD enterprise environment, some third-party providers offer: embedded certificate authority for managing devices and user identify; sophisticated posture monitoring and automated policy workflow so non-compliant devices do not get enterprise access; and certificate-based security to secure e-mail and reduce the chance of data loss.

Table 2-3 summarizes the mobile security techniques we covered in this section. With a mixture of user adherence to corporate policies, the workplace respecting the user's right to privacy, and a strong security plan, BYOD can be a success.

Table 2-3 Summary of Mobile Device Security

Key Topic

Mobile Device Security Topic	Countermeasure
Malware	Update device to latest version (or point release for the current version). Use security suites and AV software. Enable them if preloaded on the device and update regularly. Train users to carefully screen e-mail and selectively access websites. Be careful of social networks and third-party apps.
Botnets & DDoS	Download apps from a legitimate source. If BYOD is in place, use company-approved apps. Refrain from “rooting” or “jailbreaking” the device. Have data backed up in case the device becomes part of a botnet and has to be wiped.
SIM cloning	Use V2 and newer cards with strong encryption algorithms.

Mobile Device Security Topic	Countermeasure
Wireless attacks	Use a strong password for the wireless network.
	Turn off unnecessary wireless features such as mobile hotspot, tethering, and so on.
	Disable Bluetooth if not in use for long periods of time (also conserves battery).
	Set device to undetectable.
Theft	Utilize data and voice encryption (especially in BYOD implementations).
	Implement lockout, remote locator, and remote wipe programs.
	Limit the amount of confidential information stored on the device.
	Use screen locks and complex passwords.
Application security	Use encryption from reputable providers.
	Utilize non-transitive trusts between networks and apps.
	White-list applications.
	Disable geotagging.
BYOD concerns	Implement storage segmentation.
	Utilize an MDM solution.
	Create and implement clear policies that the organization and user must adhere to.

Chapter Summary

Computer systems of all kinds require an in-depth security plan. This is due to the plethora of security threats to, and vulnerabilities of, desktops, laptops, servers, and mobile devices. The primary threat is malicious software, or malware, including viruses, worms, Trojans, rootkits, spyware, ransomware, and spam. Any of these can turn a \$1000 computer into a pile of useless metal. The security administrator needs to understand what these threats are, how they can be delivered, how they manifest themselves, and how they can be prevented, or troubleshoot if they do occur.

Computer security threats can be delivered by way of software or within an e-mail, via zombie computers that are part of a botnet, and through backdoors and the act of privilege escalation. The idea is that the attacker wants to either render the computer useless or gain administrative access to it. The reason, more often than not,

is that the attacker wants confidential information; such as company secrets, credit card numbers, or even classified government information.

A good security administrator is proactive. Preventing these threats means updating systems and applications (and possibly redesigning networks and systems from the ground up). It also means using firewalls, host-based intrusion detection systems (HIDSs), and data loss prevention (DLP) systems. It requires in-depth configuration of applications, filtering, and secure policies. And of course, this all signifies a need for user training.

Software is not the only place to increase security. Hardware can be physically protected, and firmware such as the BIOS should be secured as well. We mentioned earlier that the most important thing to a company (technologically speaking) is its data. So, the securing of all types of storage devices, especially removable storage, is paramount. This can be done in a physical manner, and in a logical manner by utilizing hardware security modules (HSMs) and encryption.

A computer is a computer. It doesn't matter if it's a PC from 1986 or a mobile device from this year. All computers need to be secured using the same principles and policies. However, mobile devices tend to fall through the cracks. So, since 2011 or so, companies have really started gearing up the security for these devices. In most organizations it is not feasible to stop a person from bringing their smartphone into work. Some organizations have decided to embrace this practice and benefit from it with a policy of bringing in your own device (BYOD) to be used for work purposes in addition to personal. While this creates a whole slew of new security considerations, some organizations are implementing BYOD successfully by creating a well-defined demarcation point between the user's data and the organization's. By instituting this, along with a mobile device management (MDM) solution and strong policies for theft, wireless attacks, and application security, mobile devices can survive and thrive in the enterprise, and in the small office, just as they do in the home.

Many of the topics we discussed in this chapter, such as encryption and policies, will be covered in more depth as we progress throughout the book. You will find that later chapters tend to build upon this one. Be sure to review this chapter carefully.

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 2-4 lists a reference of these key topics and the page number on which each is found.

Table 2-4 Key Topics for Chapter 2

Key Topic Element	Description	Page Number
Bullet list	Types of viruses	19
Table 2-1	Summary of malware threats	23
Table 2-2	Summary of malware prevention techniques	38
Figure 2-3	BIOS and drive lock passwords	46
Table 2-3	Summary of mobile device security	59

Define Key Terms

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

malware, virus, worm, Trojan horse, ransomware, spyware, adware, grayware, rootkit, spam, threat vector, attack vector, typosquatting, botnet, zombie, active interception, privilege escalation, backdoors, logic bomb, time bomb, Easter egg, open mail relay, host-based intrusion detection system (HIDS), personal firewall, pop-up blocker, ad filtering, content filters, hardware security module, bluejacking, bluesnarfing, application white-listing, storage segmentation, mobile device management (MDM)

Review Questions

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

1. A group of compromised computers that have software installed by a worm or Trojan is known as which of the following?
 - A. Botnet
 - B. Virus
 - C. Honeypot
 - D. Zombie

2. What are some of the drawbacks to using a HIDS instead of a NIDS on a server? (Select the two best answers.)
 - A. A HIDS may use a lot of resources, which can slow server performance.
 - B. A HIDS cannot detect operating system attacks.
 - C. A HIDS has a low level of detection of operating system attacks.
 - D. A HIDS cannot detect network attacks.

3. Which of the following computer security threats can be updated automatically and remotely? (Select the best answer.)
 - A. Virus
 - B. Worm
 - C. Zombie
 - D. Malware

4. Which of the following is the best mode to use when scanning for viruses?
 - A. Safe Mode
 - B. Last Known Good Configuration
 - C. Command Prompt only
 - D. Boot into Windows normally

5. Which of the following is a common symptom of spyware?
 - A. Infected files
 - B. Computer shuts down
 - C. Applications freeze
 - D. Pop-up windows

- 6.** What are two ways to secure the computer within the BIOS? (Select the two best answers.)

 - A.** Configure a supervisor password.
 - B.** Turn on BIOS shadowing.
 - C.** Flash the BIOS.
 - D.** Set the hard drive first in the boot order.
- 7.** Dan is a network administrator. One day he notices that his DHCP server is flooded with information. He analyzes it and finds that the information is coming from more than 50 computers on the network. Which of the following is the most likely reason?

 - A.** Virus
 - B.** Worm
 - C.** Zombie
 - D.** PHP script
- 8.** Which of the following is not an example of malicious software?

 - A.** Rootkits
 - B.** Spyware
 - C.** Viruses
 - D.** Browser
- 9.** Which type of attack uses more than one computer?

 - A.** Virus
 - B.** DoS
 - C.** Worm
 - D.** DDoS
- 10.** What are the two ways in which you can stop employees from using USB flash drives? (Select the two best answers.)

 - A.** Utilize RBAC.
 - B.** Disable USB devices in the BIOS.
 - C.** Disable the USB root hub.
 - D.** Enable MAC filtering.

- 11.** Which of the following does not need updating?
- A.** HIDS
 - B.** Antivirus software
 - C.** Pop-up blockers
 - D.** Anti-spyware
- 12.** Which of the following are Bluetooth threats? (Select the two best answers.)
- A.** Bluesnarfing
 - B.** Blue bearding
 - C.** Bluejacking
 - D.** Distributed denial-of-service
- 13.** What is a malicious attack that executes at the same time every week?
- A.** Virus
 - B.** Worm
 - C.** Bluejacking
 - D.** Logic bomb
- 14.** Which of these is true for active interception?
- A.** When a computer is put between a sender and receiver
 - B.** When a person overhears a conversation
 - C.** When a person looks through files
 - D.** When a person hardens an operating system
- 15.** Tim believes that his computer has a worm. What is the best tool to use to remove that worm?
- A.** Antivirus software
 - B.** Anti-spyware software
 - C.** HIDS
 - D.** NIDS
- 16.** Which of the following types of scanners can locate a rootkit on a computer?
- A.** Image scanner
 - B.** Barcode scanner

- C. Malware scanner
 - D. Adware scanner
17. Which type of malware does not require a user to execute a program to distribute the software?
- A. Worm
 - B. Virus
 - C. Trojan horse
 - D. Stealth
18. Which of these is not considered to be an inline device?
- A. Firewall
 - B. Router
 - C. CSU/DSU
 - D. HIDS
19. Whitelisting, blacklisting, and closing open relays are all mitigation techniques addressing what kind of threat?
- A. Spyware
 - B. Spam
 - C. Viruses
 - D. Botnets
20. How do most network-based viruses spread?
- A. By optical disc
 - B. Through e-mail
 - C. By USB flash drive
 - D. By floppy disk
21. Which of the following defines the difference between a Trojan horse and a worm? (Select the best answer.)
- A. Worms self-replicate but Trojan horses do not.
 - B. The two are the same.
 - C. Worms are sent via e-mail; Trojan horses are not.
 - D. Trojan horses are malicious attacks; worms are not.

- 22.** Which of the following types of viruses hides its code to mask itself?
- A.** Stealth virus
 - B.** Polymorphic virus
 - C.** Worm
 - D.** Armored virus
- 23.** Which of the following types of malware appears to the user as legitimate but actually enables unauthorized access to the user's computer?
- A.** Worm
 - B.** Virus
 - C.** Trojan
 - D.** Spam
- 24.** Which of the following would be considered detrimental effects of a virus hoax? (Select the two best answers.)
- A.** Technical support resources are consumed by increased user calls.
 - B.** Users are at risk for identity theft.
 - C.** Users are tricked into changing the system configuration.
 - D.** The e-mail server capacity is consumed by message traffic.
- 25.** To mitigate risks when users access company e-mail with their smartphone, what security policy should be implemented?
- A.** Data connection capabilities should be disabled.
 - B.** A password should be set on the smartphone.
 - C.** Smartphone data should be encrypted.
 - D.** Smartphone should be only for company use.
- 26.** Your manager wants you to implement a type of intrusion detection system (IDS) that can be matched to certain types of traffic patterns. What kind of IDS is this?
- A.** Anomaly-based IDS
 - B.** Signature-based IDS
 - C.** Behavior-based IDS
 - D.** Heuristic-based IDS

- 27.** You are the security administrator for your organization. You want to ensure the confidentiality of data on mobile devices. What is the best solution?
- A.** Device encryption
 - B.** Remote wipe
 - C.** Screen locks
 - D.** AV software
- 28.** You are tasked with implementing a solution that encrypts the CEO's laptop. However, you are not allowed to purchase additional hardware or software. Which of the following solutions should you implement?
- A.** HSM
 - B.** TPM
 - C.** HIDS
 - D.** USB encryption
- 29.** One of your co-workers complains of very slow system performance and says that a lot of antivirus messages are being displayed. The user admits to recently installing pirated software and downloading and installing an illegal keygen to activate the software. What type of malware has affected the user's computer?
- A.** Worm
 - B.** Logic bomb
 - C.** Spyware
 - D.** Trojan
- 30.** A smartphone has been lost. You need to ensure 100% that no data can be retrieved from it. What should you do?
- A.** Remote wipe
 - B.** GPS tracking
 - C.** Implement encryption
 - D.** Turn on screen locks
- 31.** A user complains that they were browsing the Internet when the computer started acting erratically and crashed. You reboot the computer and notice that performance is very slow. In addition, after running a netstat command you notice literally hundreds of outbound connections to various websites, many of which are well-known sites. Which of the following has happened?

- A. The computer is infected with spyware.
 - B. The computer is infected with a virus.
 - C. The computer is now part of a botnet.
 - D. The computer is now infected with a rootkit.
32. Which of the following is a concern based on a user taking pictures with a smartphone?
- A. Application whitelisting
 - B. Geotagging
 - C. BYOD
 - D. MDM
33. A smartphone is an easy target for theft. Which of the following are the *best* methods to protect the confidential data on the device? (Select the two best answers.)
- A. Remote wipe
 - B. E-mail password
 - C. GPS
 - D. Tethering
 - E. Encryption
 - F. Screen lock
34. Which of the following should Carl, a security administrator, include when encrypting a smartphone? (Select the two best answers.)
- A. Public keys
 - B. Internal memory
 - C. Master boot record (MBR)
 - D. Steganographic images
 - E. Removable memory cards
35. Which of the following is an advantage of implementing individual file encryption on a hard drive that already uses whole disk encryption?
- A. Individually encrypted files will remain encrypted if they are copied to external drives.
 - B. It reduces the processing overhead necessary to access encrypted files.

- C. NTFS permissions remain intact when files are copied to an external drive.
 - D. Double encryption doubles the bit strength of the encrypted file.
- 36. You are in charge of compliance with financial regulations for credit card transactions. You need to block out certain ports on the individual computers that do these transactions. What should you implement to best achieve your goal?
 - A. HIPS
 - B. Antivirus updates
 - C. Host-based firewall
 - D. NIDS
- 37. One of your users was not being careful when browsing the Internet. The user was redirected to a warez site where a number of pop-ups appeared. After clicking one pop-up by accident, a drive-by download of unwanted software occurred. What does the download most likely contain?
 - A. Spyware
 - B. DDoS
 - C. Smurf
 - D. Backdoor
 - E. Logic bomb
- 38. You are the network administrator for a small organization without much in the way of security policies. While analyzing your servers' performance you find various chain messages have been received by the company. Which type of security control should you implement to fix the problem?
 - A. Antivirus
 - B. Anti-spyware
 - C. Host-based firewalls
 - D. Anti-spam
- 39. Which of the following would most likely be considered for DLP?
 - A. Proxy server
 - B. Print server
 - C. USB mass storage device
 - D. Application server content

40. You are the security administrator for your organization and have just completed a routine server audit. You did not notice any abnormal activity. However, another network security analyst finds connections to unauthorized ports from outside the organization’s network. Using security tools, the analyst finds hidden processes that are running on the server. Which of the following has most likely been installed on the server?
- A. Spam
 - B. Rootkit
 - C. Backdoor
 - D. Logic bomb
 - E. Ransomware

Answers and Explanations

1. **A.** A botnet is a group of compromised computers, usually working together, with malware that was installed by a worm or a Trojan horse. An individual computer within a botnet is referred to as a zombie (among other things). A virus is code that can infect a computer’s files. A honeypot is a computer that is used to lure attackers and quarantine their attack so that it can be analyzed, and so that it does not spread to the rest of the network.
2. **A. and D.** Host-based intrusion detection systems (HIDSs) run within the operating system of a computer. Because of this, they can slow a computer’s performance. Most HIDS do not detect network attacks well (if at all). However, a HIDS can detect operating system attacks and will usually have a high level of detection for those attacks.
3. **C.** Zombies (also known as zombie computers) are systems that have been compromised without the knowledge of the owner. A prerequisite is the computer must be connected to the Internet so that the hacker or malicious attack can make its way to the computer and be controlled remotely. Multiple zombies working in concert often form a botnet. See the section “Computer Systems Security Threats” earlier in this chapter for more information.
4. **A.** Safe Mode should be used (if your AV software supports it) when scanning for viruses.
5. **D.** Pop-up windows are common to spyware. The rest of the answers are more common symptoms of viruses.

6. **A.** and **D.** Configuring a supervisor password in the BIOS disallows any other user to enter the BIOS and make changes. Setting the hard drive first in the BIOS boot order disables any other devices from being booted off, including floppy drives, optical drives, and USB flash drives. BIOS shadowing doesn't have anything to do with computer security, and although flashing the BIOS may include some security updates, it's not the best answer.
7. **B.** A worm is most likely the reason that the server is being bombarded with information by the clients; perhaps it is perpetuated by a botnet. Because worms self-replicate, the damage can quickly become critical.
8. **D.** A web browser (for example, Internet Explorer) is the only one listed that is not an example of malicious software. Although a browser can be compromised in a variety of ways by malicious software, the application itself is not the malware.
9. **D.** A DDoS, or distributed denial-of-service, attack uses multiple computers to make its attack, usually perpetuated on a server. None of the other answers use multiple computers.
10. **B.** and **C.** By disabling all USB devices in the BIOS, a user cannot use his flash drive. Also, the user cannot use the device if you disable the USB root hub within the operating system. RBAC, which stands for role-based access control, defines access to networks by the person's role in the organization (we will cover this more later in the book). MAC filtering is a method of filtering out computers when they attempt to access the network (using the MAC addresses of those computers).
11. **C.** Pop-up blockers do not require updating to be accurate. However, host-based intrusion detection systems, antivirus software, and anti-spyware all need to be updated to be accurate.
12. **A.** and **C.** Bluesnarfing and bluejacking are the names of a couple of Bluetooth threats. Another attack could be aimed at a Bluetooth device's discovery mode. To date there is no such thing as blue bearding, and a distributed denial-of-service attack uses multiple computers to attack one host.
13. **D.** A logic bomb is a malicious attack that executes at a specific time. Viruses normally execute when a user inadvertently runs them. Worms can self-replicate at will. And bluejacking deals with Bluetooth devices.
14. **A.** Active interception normally includes a computer placed between the sender and the receiver to capture information.
15. **A.** Antivirus software is the best option when removing a worm. It may be necessary to boot into Safe Mode to remove this worm when using antivirus software.

16. **C.** Malware scanners can locate rootkits and other types of malware. These types of scanners are often found in anti-malware software from manufacturers such as McAfee, Norton, and so on. Adware scanners (often free) can scan for only adware. Always have some kind of anti-malware software running on live client computers!
17. **A.** Worms self-replicate and do not require a user to execute a program to distribute the software across networks. All the other answers do require user intervention. Stealth refers to a type of virus.
18. **D.** HIDSs, or host-based intrusion detection systems, are not considered to be an inline device. This is because they run on an individual computer. Firewalls, routers, and CSU/DSUs are inline devices.
19. **B.** Closing open relays, whitelisting, and blacklisting are all mitigation techniques that address spam. Spam e-mail is a serious problem for all companies and must be filtered as much as possible.
20. **B.** E-mail is the number one reason why network-based viruses spread. All a person needs to do is double-click the attachment within the e-mail, and the virus will do its thing, which is most likely to spread through the user's address book. Removable media such as optical discs, USB flash drives, and floppy disks can spread viruses but are not nearly as common as e-mail.
21. **A.** The primary difference between a Trojan horse and a worm is that worms will self-replicate without any user intervention; Trojan horses do not self-replicate.
22. **D.** An armored virus attempts to make disassembly difficult for an antivirus software program. It thwarts attempts at code examination. Stealth viruses attempt to avoid detection by antivirus software altogether. Polymorphic viruses change every time they run. Worms are not viruses.
23. **C.** A Trojan, or a Trojan horse, appears to be legitimate and looks like it'll perform desirable functions, but in reality it is designed to enable unauthorized access to the user's computer.
24. **A. and C.** Because a virus can affect many users, technical support resources can be consumed by an increase in user phone calls. This can be detrimental to the company because all companies have a limited number of technical support personnel. Another detrimental effect is that unwitting users may be tricked into changing some of their computer system configurations. The key term in the question is "virus hoax." The technical support team might also be inundated by support e-mails from users, but not to the point where the e-mail server capacity is consumed. If the e-mail server is consumed by message traffic, that would be a detrimental effect caused by the person who sent the virus and

by the virus itself but not necessarily by the hoax. Although users may be at risk for identity theft, it is not one of the most detrimental effects of the virus hoax.

25. **B.** A password should be set on the phone, and the phone should lock after a set period of time. When the user wants to use the phone again, the user should be prompted for a password. Disabling the data connection altogether would make access to e-mail impossible on the smartphone. Smartphone encryption of data is possible, but it could use a lot of processing power that may make it unfeasible. Whether the smartphone is used only for company use is up to the policies of the company.
26. **B.** When using an IDS, particular types of traffic patterns refer to signature-based IDS.
27. **A.** Device encryption is the best solution listed to protect the confidentiality of data. By encrypting the data, it makes it much more difficult for a malicious person to make use of the data. Screen locks are a good idea but are much easier to get past than encryption. Antivirus software will not stop an attacker from getting to the data once the mobile device has been stolen. Remote sanitization (remote wipe) doesn't keep the data confidential; it removes it altogether! While this could be considered a type of confidentiality, it would only be so if a good backup plan was instituted. Regardless, the best answer with confidentiality in mind is encryption. For example, if the device was simply lost, and was later found, it could be reused (as long as it wasn't tampered with). But if the device was sanitized, it would have to be reloaded and reconfigured before being used again.
28. **B.** A TPM, or trusted platform module, is a chip that resides on the motherboard of the laptop. It generates cryptographic keys that allow the entire disk to be encrypted, as in full disk encryption (FDE). Hardware security modules (HSMs) and USB encryption require additional hardware. A host-based intrusion detection system requires either additional software or hardware.
29. **D.** A Trojan was probably installed (unknown to the user) as part of the keygen package. Illegal downloads often contain malware of this nature. At this point, the computer is compromised. Not only is it infected, but malicious individuals might be able to remotely access it.
30. **A.** If the device has been lost and you need to be 100% sure that data cannot be retrieved from it, then you should remotely sanitize (or remotely "wipe") the device. This removes all data to the point where it cannot be reconstructed by normal means. GPS tracking might find the device, but as time is spent tracking and acquiring the device, the data could be stolen. Encryption is a good idea, but over time encryption can be deciphered. Screen locks can be easily circumvented.

31. C. The computer is probably now part of a botnet. The reason the system is running slowly is probably due to the fact that there are hundreds of outbound connections to various websites. This is a solid sign of a computer that has become part of a botnet. Spyware, viruses, and rootkits might make the computer run slowly, but they will not create hundreds of outbound connections.
32. B. Geotagging is a concern based on a user taking pictures with a mobile device such as a smartphone. This is because the act of geotagging utilizes GPS, which can give away the location of the user. Application whitelisting is when there is an approved list of applications for use by mobile devices. Usually implemented as a policy, if the mobile device attempts to open an app that is not on the list, the process will fail, or the system will ask for proof of administrative identity. BYOD stands for bring your own device, a technological concept where organizations allow employees to bring their personal mobile devices to work and use them for work purposes. MDM stands for mobile device management, a system that enables a security administrator to configure, update, and secure multiple mobile devices from a central location.
33. A. and E. Remote wipe and encryption are the best methods to protect a stolen device's confidential or sensitive information. GPS can help to locate a device, but it can also be a security vulnerability in general; this will depend on the scenario in which the mobile device is used. Passwords should never be e-mailed and should not be associated with e-mail. Tethering is when a mobile device is connected to another computer (usually via USB) so that the other computer can share Internet access, or other similar sharing functionality in one direction or the other. This is great as far as functionality goes, but more often than not can be a security vulnerability. Screen locks are a decent method of reducing the chance of login by the average person, but they are not much of a deterrent for the persistent attacker.
34. B. and E. When encrypting a smartphone, the security administrator should encrypt internal memory and any long-term storage such as removable media cards. The admin must remember that data can be stored on both. Public keys are already encrypted; it is part of their inherent nature. Smartphones don't necessarily use an MBR the way Windows computers do, but regardless, if the internal memory has been encrypted, any boot sector should be secured. Images based on steganography, by their very nature, are encrypted through obfuscation. It is different from typical data encryption, but it's a type of cryptography nonetheless.
35. A. By implementing individual file encryption (such as EFS) on files that are stored on a disk encrypted with whole disk encryption, the files will remain encrypted (through EFS) even if they are copied to a separate drive that does not use whole disk encryption. However, running two types of encryption will

usually *increase* processing overhead, not reduce it. NTFS permissions aren't relevant here; however, if files are copied to an external drive, those files by default lose their NTFS permissions and inherit new permissions from the parent folder on the new drive. We'll discuss NTFS permissions more in Chapter 10. We shouldn't call this *double* encryption—rather, the files are encrypted twice separately. The bit strength is not cumulative in this example, but there are two layers of encryption, which is an example of defense in depth and security layering.

36. **C.** To meet regulations, a properly configured host-based firewall will be required on the computers that will be transacting business by credit card over the Internet. All of the other answers—antivirus updates, NIDS, and HIPS—are good ideas to secure the system (and/or network), but they do not address the core issue of filtering ports, which is the primary purpose of the firewall. Also, a network-based firewall will often not be secure enough to meet regulations, thus the need for the extra layer of protection on the individual computers.
37. **A.** Of the answers listed, the download most likely contains spyware. It could contain other types of malware as well, such as viruses, Trojans, worms, and so on. The rest of the answers are types of network attacks and methods of accessing the computer to drop a malware payload. A DDoS is a distributed denial-of-service attack, which uses many computers to attack a single target. Smurf is an example of a DDoS. We'll talk more about these in Chapter 6. Backdoors are vulnerabilities in code that can allow a hacker (or even the programmer) administrative access to an operating system. Logic bombs are ways of delivering malware; they are based on timing.
38. **D.** The chain messages are e-mails (similar to the archaic chain *letter*) that are being spammed on the network. Therefore, anti-spam security controls need to be implemented. This would be a type of preventive control. Antivirus programs find and quarantine viruses, worms, and Trojans, but unless they are part of an AV suite of software, they will not check e-mail. Anti-spyware tools will attempt to prevent spyware from being installed on the computer. Host-based firewalls block attacks from coming through specific ports, but will not catch spam messages. However, a HIDS could possibly detect spam, and a HIPS (host-based intrusion prevention system) might even prevent or quarantine it.
39. **C.** Of the answers listed, the USB mass storage device would be the most likely asset to be considered for data loss prevention (DLP). It's the only device listed in the answers that should have any real organizational data! A proxy server temporarily caches such data as HTTP and FTP. A print server forwards printed documents to the correct printer (again the data is usually

held temporarily). An application server contains programs, but usually doesn't store organizational data files. It's the devices and computers that store actual company data files that we are primarily concerned with.

- 40. B.** Most likely, a rootkit was installed. These can evade many routine scans, so there is no fault here. It's just that more in-depth analysis was required to find the rootkit. The hidden processes are the main indicator of the rootkit. Spam is simply harassment by e-mail (and other messaging systems), to put it nicely. Backdoors are programmed ways to bypass security of an operating system. A logic bomb is code that defines when a particular type of malware will execute. Ransomware is when a computer is operationally held hostage; files are not retrievable by the user (because they have been encrypted) until a ransom is paid. It's important to run in-depth scans periodically. They can be time consuming, but they can uncover many threats and vulnerabilities that would otherwise go unnoticed. We'll discuss these types of scans more during Chapters 11 and 12.

Case Studies for Chapter 2

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

Case Study 2-1: Using Free Malware Scanning Programs

Scenario: As a security administrator, your task is to select a free malware scanning program and scan a computer system.

An anti-malware solution is extremely important when securing a computer's operating system. There are plenty to choose from that will have a price tag attached, but a good security person should also be able to use free tools online. Plus, using a free tool provides us with an easy way to practice without expending any hard-earned capital.

You can select from the following list or search for an alternative using your favorite search engine. These could be programs that are downloadable; if so, be sure that you are downloading the files from a reputable source. There are also online scanners that run directly from within a website. In this case, make sure that the website is secured via some kind of website scanning system. Keep in mind that links may change over time, and software that is free (at the writing of this book) may incur a charge as time goes by.

Once you have selected a tool, scan your computer for malware. This is best done on a test computer if you have one available. Write down the results of your scans.

- Malicious Software Removal Tool
<http://www.microsoft.com/security/pc-security/malware-removal.aspx>
- Trend Micro HouseCall <http://housecall.trendmicro.com/>
- Malwarebytes Anti-Malware <http://www.malwarebytes.org/>
- Microsoft Safety Scanner
<http://www.microsoft.com/security/scanner/en-us/default.aspx>
- Spybot Search & Destroy <http://www.safer-networking.org/private/>
- Combofix <http://www.combofix.org/>

Case Study 2-2: Securing the BIOS

Scenario: Your boss asks you to secure the BIOS on a desktop computer. Your job is to modify the BIOS boot order, disable unnecessary devices such as floppy drives, and configure a supervisory password.

The BIOS boots before the operating system. It can be configured to boot from optical discs and removable media. This change is fairly simple to make as long as a person can log in to the BIOS setup program. If no password is configured, this is even easier. You can imagine the amount of havoc that can be wreaked upon a machine if a malicious individual were to gain access to the BIOS.

Try securing the BIOS program on a test computer, or try securing the virtual BIOS that is included within virtual machine software such as Virtual PC 2007, Windows Virtual PC, or VirtualBox. When you are finished, return all settings back to normal.

Case Study 2-3: Securing Mobile Devices

Scenario: You have purchased a couple of different mobile devices and are concerned about their out-of-the-box level of security. Implement some basic security measures on the devices.

Take a look at the mobile device(s) that you own or attempt to borrow one. What kind of security measures could you take (or have already taken) to make the device(s) less vulnerable. If you can't get access to one, use the content in this chapter to help with some ideas for security measures that you can implement. Write down your list of security implementations and compare them with the case study solution.

Case Study 2-4: Filtering and Screening E-mail

Scenario: You are the security administrator for a midsized organization. One of your many tasks is to train users to filter and/or screen their e-mails.

E-mail vetting (screening) has become increasingly necessary over the past decade. This is due to the amount of spam that dominates the Internet. Imagine how you might reduce the amount of spam (which everyone gets at some point) within Outlook e-mail accounts and within free web-based e-mail accounts such as Gmail.

Write down your answers and compare with the case study solution.

Case Study Solutions

Case Study 2-1 Solution

In this example solution we use the free Trend Micro HouseCall scanning program to analyze a computer for viruses. This should be performed on a test computer, but a virtual machine is also acceptable. The steps are as follows:

- Step 1.** Download Trend Micro's HouseCall software from
<http://housecall.trendmicro.com/>
- Step 2.** When it finishes downloading, install the program.
- Step 3.** The program should run automatically; use it to scan your computer for malware. You can click settings to select different partitions or folders. If you find any malware, quarantine it!
- Step 4.** Consider downloading and utilizing other tools in the list to get a firmer understanding of how these type of scanning tools operate.
- Step 5.** When you finish working with the free malware scanning programs, uninstall each of them from the computer and clear the cache on the system.

Video Solution: Watch the video solution “2-1: Using Free Malware Scanning Programs” on the accompanying disc.

Simulation: Complete the simulation “2-1: Identifying Malware Types.”

Case Study 2-2 Solution

For this example solution we use the virtual BIOS in Microsoft Virtual PC 2007 to make some configuration changes, thus securing the BIOS. The steps are as follows:

- Step 1.** Download and install Microsoft Virtual PC 2007.
- Step 2.** Run the Virtual PC program; this should display the Virtual PC console.
- Step 3.** Create a new virtual machine.
- Step 4.** Access the VM BIOS.
- Step 5.** Change the Boot device priority order.
- Step 6.** Disable the floppy drive.
- Step 7.** Configure a complex supervisor password.
- Step 8.** Return the virtual BIOS settings to normal.

Video Solution: Watch the video solution “2-2: Securing the BIOS” on the accompanying disc for in-depth details of each step.

Simulation: Complete the simulation “2-2: Securing the BIOS.”

Case Study 2-3 Solution

Some of the security measures you can implement on a mobile device include: configuring screen locks utilizing either a password, PIN, or gesture; installing (or simply configuring) antivirus software; disabling wireless and GPS; using encryption; and installing/configuring backup and remote wipe programs.

Video Solution: Watch the video solution “2-3: Securing Mobile Devices” on the accompanying disc.

Case Study 2-4 Solution

Spam and other junk mail is very prevalent in today's e-mail communications. There are so many sources of this junk mail that it is impossible to stop altogether. However, through filtering and user education (screening of e-mail) it can be reduced to a level that is manageable.

One of the ways to do this is to increase the level of security for junk e-mail. E-mail applications such as Outlook offer this feature. Another way is to set up filters either through third-party software locally, at the e-mail server (be it in-house or on the Internet), or by using a filtering appliance, such as the Barracuda devices mentioned earlier in the chapter. The use of blacklisting (and/or whitelisting) can help with reoccurring spam. But the best method is to train users to scan their e-mails carefully, deleting any that appear suspicious, and by all means to not open any attachments from an unknown source. While deleting the e-mail, the domain it came from can be marked as blacklisted as well. So any e-mails originating from that domain (any e-mail address on that domain) will be automatically blocked.

Simulation: Complete the simulation “2-4: Filtering E-mails.”



This chapter covers the following subjects:

- **Hardening Operating Systems:** Service packs, patches, hotfixes—This section details what you need to know to make your operating system strong as steel. Group policies, security templates, and baselining put on the finishing touches to attain that bullet-proof system.
- **Virtualization Technology:** This section delves into virtual machines and other virtual implementations with an eye on applying real-world virtualization scenarios.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 3.6, 4.1, and 4.3.

OS Hardening and Virtualization

Imagine a computer with a freshly installed server operating system (OS) placed on the Internet or on a DMZ that went live without any updating, service packs, or hotfixes. How long do you think it would take for this computer to be compromised? A week? Sooner? It depends on the size and popularity of the organization, but it won't take long for a nonhardened server to be compromised. And it's not just servers! Workstations, routers, switches: You name it; they all need to be updated regularly, or they *will* fall victim to attack. By updating systems frequently and by employing other methods such as group policies and baselining, we are *hardening* the system, making it tough enough to withstand the pounding that it will probably take from today's technology...and society.

Another way to create a secure environment is to run operating systems *virtually*. Virtual systems allow for a high degree of security, portability, and ease of use. However, they are resource-intensive, so a balance needs to be found, and virtualization needs to be used according to the level of resources in an organization. Of course, these systems need to be maintained and updated (hardened) as well.

By utilizing virtualization properly and by implementing an intelligent update plan, operating systems, and the relationships between operating systems, can be more secure and last a long time.

Foundation Topics

Hardening Operating Systems

An operating system, or OS, that has been installed out-of-the-box is inherently insecure. This can be attributed to several things, including initial code issues and backdoors, the age of the product, and the fact that most systems start off with a basic and insecure set of rules and policies. How many times have you heard of a default OS installation where the controlling user account was easily accessible and had no password? Although these types of oversights are constantly being improved upon, making an out-of-the-box experience more pleasant, new applications and new technologies offer new security implications as

well. So regardless of the product, we must try to protect it after the installation is complete.

Hardening of the OS is the act of configuring an OS securely, updating it, creating rules and policies to help govern the system in a secure manner, and removing unnecessary applications and services. This is done to minimize OS exposure to threats and to mitigate possible risk. Although it is impossible to reduce risk to zero, I'll show some tips and tricks that can enable you to diminish current and future risk to an acceptable level.

This section demonstrates how to harden the OS through the use of service packs, patches and patch management, hotfixes, group policies, security templates, and configuration baselines. We then discuss a little bit about how to secure the file system and hard drives. But first, let's discuss how to analyze the system and decide which applications and services are unnecessary, and then remove them.

Removing Unnecessary Applications and Services

Unnecessary applications and services use valuable hard drive space and processing power. Plus, they can be vulnerabilities to an operating system.

For example, instant messaging programs might be fun for a user but usually are not productive in the workplace (to put it nicely); plus, they often have backdoors that are easily accessible to attackers. They should be discouraged or disallowed by rules and policies. Be proactive when it comes to these types of programs. If users can't install an IM program on their computer, you will never have to remove it from the system. But if you do have to remove an application like this, be sure to remove all traces that it ever existed. Make sure that related services are turned off and disabled. Then verify that their inbound ports are no longer functional, and that they are closed and secured. For example, AOL Instant Messenger (AIM) uses inbound port 5190, which is well known to attackers, as are other inbound ports of other IM programs, such as ICQ or Trillian. Confirm that any shares created by an application are disabled as well. Basically, remove all instances of the application or, if necessary, re-image the computer! That is just one example of many, but it can be applied to most superfluous programs. Another type of program you should watch out for are remote control programs. Applications that enable remote control of a computer should be avoided if possible.

Personally, I use a *lot* of programs. But over time, some of them fall by the wayside and are replaced by better programs. The best procedure is to check a system periodically for any unnecessary programs. For example, in Windows 7 we can look at the list of installed programs by going to the Control Panel > Programs > Programs and Features, as shown in Figure 3-1.

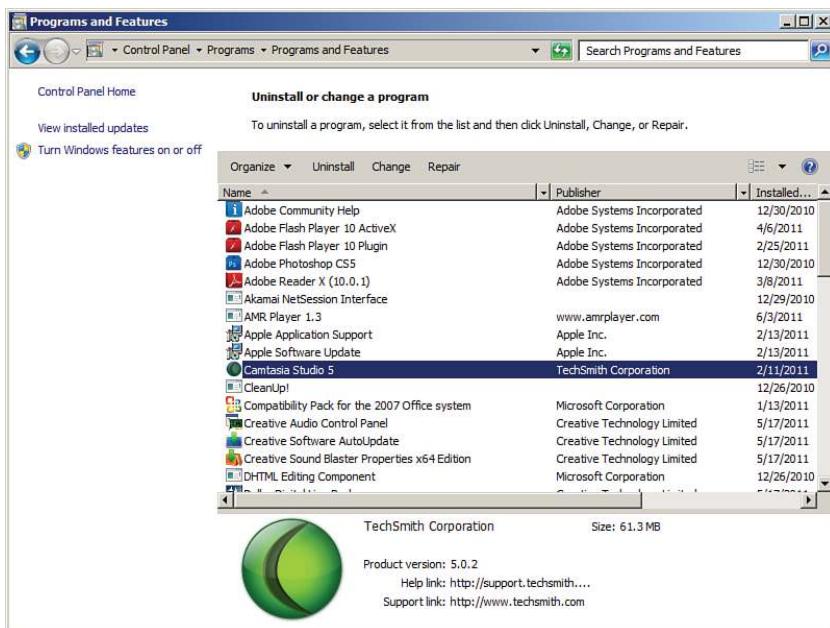


Figure 3-1 Windows 7 Programs and Features Window

Notice in the figure that Camtasia Studio 5 is installed. This is an older version of the program. If in the future I decide to install the latest version of Camtasia, or use another program, such as Adobe Captivate or something similar, and Camtasia 5 is no longer necessary, then it should be removed. This can be done by right-clicking the application and selecting Uninstall. Or an application might have an uninstall feature built into the Start menu that you can use. Programs such as this can use up to 50 MB, 100 MB, and possibly much more, so it makes sense to remove them to conserve hard drive space. This becomes more important when you deal with audio/video departments that would use an application such as Camtasia, and most likely many others like it. The applications are always battling for hard drive space, and it can get ugly! Not only that, but many applications place a piece of themselves in the Notification Area in Windows. So, a part of the program is actually running behind the scenes using processor/RAM resources. If the application is necessary, there are often ways to eliminate it from the Notification Area, either by right-clicking it and accessing its properties, or by turning it off with a configuration program such as the System Configuration Utility in Windows (which can be executed by going to Start > Run and typing `msconfig`).

Consider also that apps like this might also attempt to communicate with the Internet in an attempt to download updates, or for other reasons. It makes this issue not only a resource problem, but also a security concern, so it should be removed if it is unused. Only software deemed necessary should be installed in the future.

Now, uninstalling applications on a few computers is feasible, but what if you have a larger network? Say, one with 1,000 computers? You can't expect yourself or your computer techs to go to each and every computer locally and remove applications. That's when centrally administered management systems come into play. Examples of these include Microsoft's System Center Configuration Manager (SCCM), and the variety of mobile device management suites available. These programs allow a security administrator to manage lots of computers' software, configurations, and policies, all from the local workstation.

Of course, it can still be difficult to remove all the superfluous applications from every end-user computer on the network. What's important to realize here is that applications are at their most dangerous when actually being used by a person. Given this mindset, you should consider the concept of application whitelisting and blacklisting. Application whitelisting, as mentioned in Chapter 2, "Computer Systems Security," is when you set a policy that allows only certain applications to run on client computers (such as Microsoft Word and Internet Explorer). Any other application will be denied to the user. This works well in that it eliminates any possibility (excluding hacking) of another program being opened by an end user, but it can cause productivity problems. When an end user really *needs* another application, an exception would have to be made to the rule for that user, which takes time, and possibly permission from management. **Application blacklisting**, on the other hand, is when individual applications are disallowed. This can be a more useful (and more efficient) solution if your end users work with, and frequently add, a lot of applications. In this scenario, an individual application (say a social media or chat program) is disabled across the network. This and whitelisting are often performed from centralized management systems mentioned previously, and through the use of policies, which we discuss more later in this chapter (and later in the book).

Services are used by applications and the OS. They too can be a burden on system resources and pose security concerns. Examine Figure 3-2 and note the highlighted service.

Key Topic

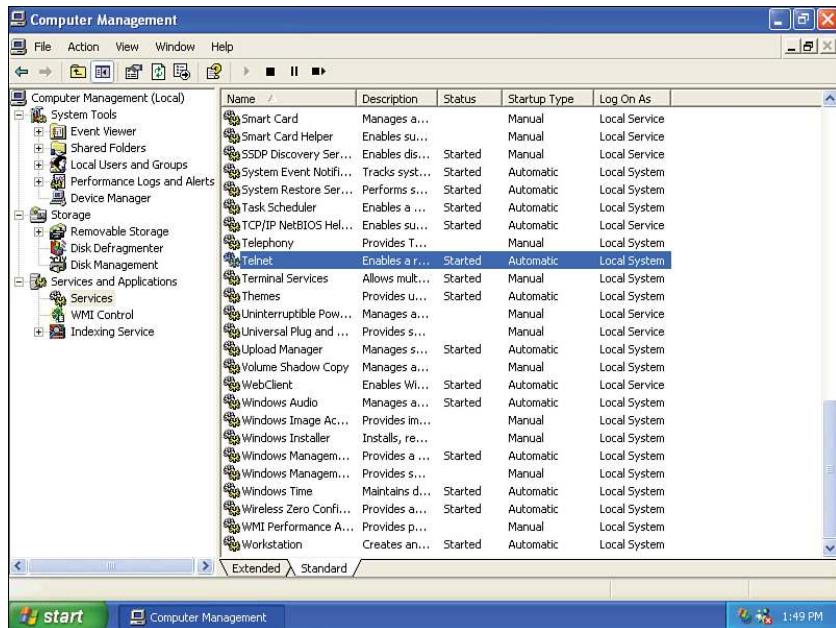


Figure 3-2 Services Window in Windows XP

The OS shown in Figure 3-2 is Windows XP. Normally, I wouldn't use Windows XP as an example given its age (and the fact that Microsoft will not support it anymore), but in this case I must because of the insecure nature of Telnet and the numerous systems that will probably continue to run Windows XP for some time. Windows XP was the last Microsoft OS to have Telnet installed by default, even though it was already well known that Telnet was a security risk. This is an example of an out-of-the-box security risk. But to make matters worse, the Telnet service in the figure is started! Instead of using Telnet, a more secure application/protocol should be utilized such as SSH. Then Telnet should be stopped and disabled. To do so, just right-click the service, select Properties, click the Stop button, and change the Startup Type drop-down menu to the Disabled option, as shown in Figure 3-3.

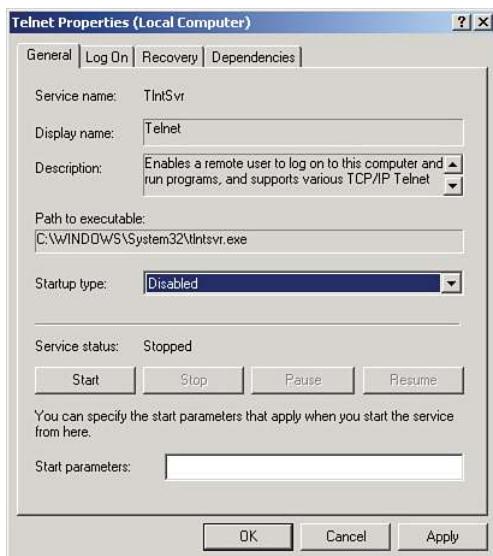
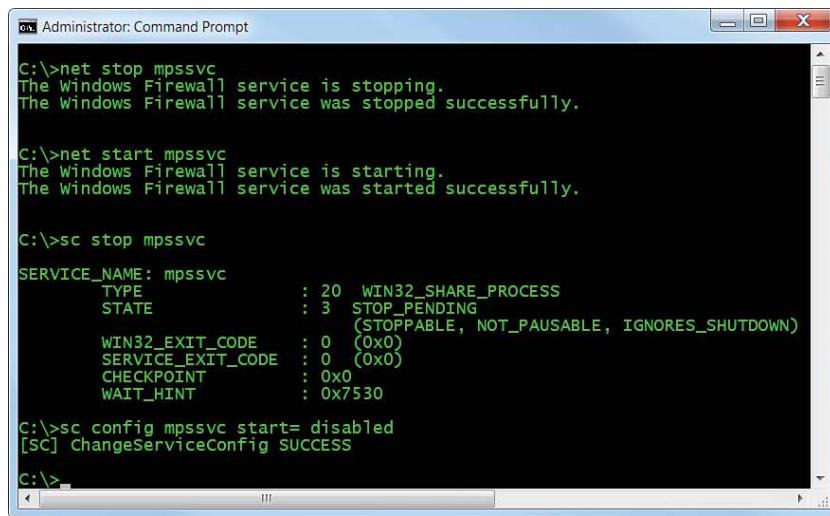


Figure 3-3 Telnet Properties Dialog Box

This should be done for all unnecessary services, for example, the Trivial File Transfer Protocol (TFTP). By disabling services such as this one, we can reduce the risk of attacker access to the computer and we trim the amount of resources used. This is especially important on Windows servers, because they run a lot more services and are a more common target. By disabling unnecessary services, we *reduce the size of the attack surface*.

Services can be started and stopped in the Windows Command Prompt with the `net start` and `net stop` commands, as well as by using the `sc` command. Examples of this are shown in Figure 3-4.

Key TopicA screenshot of a Windows 7 Command Prompt window titled "Administrator: Command Prompt". The window shows several commands being run:

```
C:\>net stop mpssvc
The Windows Firewall service is stopping.
The Windows Firewall service was stopped successfully.

C:\>net start mpssvc
The Windows Firewall service is starting.
The Windows Firewall service was started successfully.

C:\>sc stop mpssvc
SERVICE_NAME: mpssvc
    TYPE               : 20  WIN32_SHARE_PROCESS
    STATE              : 3   STOP_PENDING
                          (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0X7530

C:\>sc config mpssvc start= disabled
[SC] ChangeServiceConfig SUCCESS
C:\>
```

Figure 3-4 Stopping and Disabling a Service in the Windows 7 Command Prompt

NOTE You will need to run the Command Prompt in elevated mode (as an administrator) to execute these commands.

In Figure 3-4 we have stopped and started the Windows Firewall service (which uses the service name mpssvc) by invoking the `net stop` and `net start` commands. Then, we used the `sc` command to stop the same service with the `sc stop mpssvc` syntax. It shows that the service stoppage was pending, but as you can see from Figure 3-5, it indeed stopped (and right away, I might add). Finally, we used a derivative of the `sc` command to *disable* the service, so that it won't start again when the system is restarted. This syntax is

```
sc config mpssvc start= disabled
```

Note that there is a space after the equal sign, which is necessary for the command to work properly. Figure 3-5 shows the GUI representation of the Windows Firewall service.



Figure 3-5 Windows Firewall Properties Dialog Box

You can see in the figure that the service is disabled and stopped. This is a good place to find out the name of a service if you are not sure. Or, you could use the `sc query` command.

In Linux, you can start, stop, and restart services in a variety of ways. Because there are many variants of Linux, how you perform these actions varies in the different GUIs that are available. So, in this book I usually stick with the command-line, which is generally the same across the board. You'll probably want to display a list of services (and their status) in the command-line first. For example, in Ubuntu you can do this by typing the following:

```
service --status all
```

For a list of upstart jobs with their status, use the following syntax:

```
initctl list
```

NOTE In Linux, if you are not logged in as an administrator (and even sometimes if you are), you will need to type `sudo` before a command, and be prepared to enter an administrator password. Be ready to use `sudo` often.

Services can be stopped in the Linux command-line in a few ways:

- By typing the following syntax:

```
/etc/init.d/<service> stop
```

where <service> is the service name. For example, if you are running an Apache web server, you would type the following:

```
/etc/init.d/apache2 stop
```

Services can also be started and restarted by replacing `stop` with `start` or `restart`.

- By typing the following syntax in select versions:

```
service <service> stop
```

Some services require a different set of syntax. For example, Telnet can be deactivated in Red Hat by typing `chkconfig telnet off`. Check the MAN pages within the command-line or online for your particular version of Linux to obtain exact syntax and any previous commands that need to be issued. Or use a generic Linux online MAN page; for example: <http://linux.die.net/man/1/telnet>.

In OS X *Server*, services can be stopped in the command-line by using the following syntax:

```
sudo serveradmin stop <service>
```

However, this doesn't work on OS X *client*. In OS X client (for example, 10.9 Mavericks) you would simply quit processes either by using the Activity Monitor or by using the `kill` command in the Terminal.

NOTE Ending the underlying process is sometimes necessary in an OS when the service can't be stopped. To end processes in Windows, use the Task Manager or the `taskkill` command. The `taskkill` command can be used in conjunction with the executable name of the task or the process ID (PID) number. Numbers associated with processes can be found with the `tasklist` command. In Linux, use the `kill` command to end an individual process. To find out all process IDs currently running, use the syntax `ps aux | less`. (Ctrl+Z can break you out of commands such as this if necessary.) On mobile devices, the equivalent would be a force quit.

Table 3-1 summarizes the various ways to stop services in operating systems.

**Table 3-1** Summary of Ways to Stop Services

Operating System	Procedure to Stop Service
Windows	Access <code>services.msc</code> from the Run prompt.
	Use the <code>net stop <servicename></code> command in the Command Prompt.
	Use the <code>sc stop <servicename></code> command in the Command Prompt.
Linux	Use the syntax <code>/etc/init.d/<servicename> stop</code> .
	Use the syntax <code>service <servicename> stop</code> (in select versions).
	Use the syntax <code>chkconfig <servicename> off</code> (in select versions).
OS X	Use the <code>kill</code> command to end processes. Also works in Linux. In Windows, this is the <code>taskkill</code> command.

Don't confuse services with *service packs*. Although a service controls a specific function of an OS or application, a service pack is used to update a system. The service pack probably will update services as well, but the similarity in names is purely coincidental.

Service Packs

A **service pack (SP)** is a Microsoft-centric group of updates, bug fixes, updated drivers, and security fixes installed from one downloadable package or from one disc. When the number of patches for an OS reaches a certain limit, they are gathered together into an SP. This might take one to several months after the OS is released. Because organizations know an SP will follow an OS release, which implies that there will be security issues with a brand-new out-of-the-box OS, they will usually wait until the first SP is released before embracing a new OS.

SPs are numbered; for example SP1, SP2, and so on. An OS without an SP is referred to as SP0. Installing an SP is relatively easy and only asks a few basic questions. When those questions are answered, it takes several minutes or more to complete the update; then a restart is required. Although the SP is installed, it re-writes many files and copies new ones to the hard drive as well.

Historically, many SPs have been cumulative, meaning that they also contain previous SPs. But in some cases they have to be installed individually. For example, with Windows Vista, SP1 must be installed before updating to SP2. Before installing an SP, read the instructions that accompany it, or the instructions on the download page on the company's website.

To find out an OS's current SP level, click Start, right-click Computer, and select Properties, and the SP should be listed. If there is no SP installed, it will be blank. An example of Windows 7's System window is shown in Figure 3-6; it shows that SP1 is installed. Windows Server operating systems work in the same fashion.

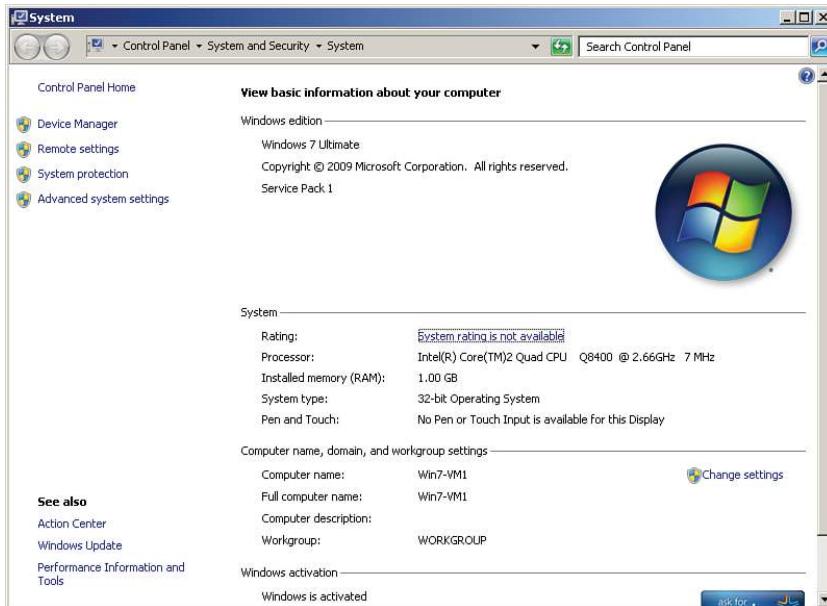


Figure 3-6 Windows 7 System Window

NOTE Newer versions of Windows, such as Windows 8 and Windows Server 2012, do not use service packs. Instead, they use update rollups, and new releases. For example, Windows 8 can be upgraded to 8.1, and Windows Server 2012 can be upgraded (for a fee) to Server 2012 R2 (release 2). However, you can find out the version information using the same techniques listed in this section.

You can also find out which service pack your operating system uses by opening the System Information tool (open the Run prompt and type `msinfo32.exe`). It will be listed directly in the system summary. In addition, you can use the `systeminfo` command in the Command Prompt (a GREAT information gatherer!).

Another tool you can use to find out the SP level besides `msinfo32.exe` is the `winver` command. This can be run in the Run prompt, in the search box, or in the Command Prompt. Either way, it will bring up the About Windows window. You can

also discern SP levels directly in the Command Prompt. For example, if you open the Command Prompt in Windows 7 and see on the top line Microsoft Windows [Version 6.1.7600], then no SP is installed. But if you do this on Windows 7 with SP1, you will see Microsoft Windows [Version 6.1.7601]. Note the difference in the last number. You can also see this by simply typing ver. You can also find out the OS name, version, and SP level with the following syntax:

```
systeminfo|findstr /B /C:"OS Name" /C:"OS Version"
```

Note the pipe symbol between `systeminfo` and `findstr`. Also, the text within the quotes is case sensitive.

In this example, the resulting output on a Windows 7 Ultimate OS with SP1 installed would be

```
OS Name: Microsoft Windows 7 Ultimate  
OS Version: 6.1.7601 Service Pack 1 Build 7601
```

For the Version/SP level only, omit the following:

```
/C:"OS Name"
```

To find out which SP a particular version of Office is running, click Help on the menu bar and select About Microsoft Office <Application Name>, where the application name could be Outlook, Word, and so on, depending on what app you use. Service packs are also used by Windows Server products and add-on products to Windows Server such as Microsoft Exchange Server.

SPs can be acquired through Windows Update, at www.microsoft.com, on disc, and through a Microsoft Developer Network (MSDN) subscription. An SP might also have been incorporated into the original OS distribution disc. This is known as *slipstreaming*. This method enables the user to install the OS and the SP at the same time in a seamless manner. System administrators can create slipstreamed images for simplified over-the-network installations of the OS and SP.

NOTE Some companies choose to stay with an older SP so that the OS in question can interoperate properly with specific applications. Though this is not recommended, you should check your organization's policies governing this subject.

If possible, the testing of service packs should be done offline (with physical media). Disconnect the computer from the network by disabling the network adapter before initiating the SP upgrade. Again, because brand-new operating systems are inherently insecure to some extent (no matter what a manufacturer might say), organiza-

tions usually wait for the release of the first SP before implementing the new OS on a live network. However, SPs are not the only type of updating you need to do to your computers. Microsoft operating systems require further patching with the Windows Update program, and other applications require their own patches and hotfixes.

Windows Update, Patches, and Hotfixes

To be considered secure, operating systems should have support for multilevel security, and be able to meet government requirements. An operating system that meets these criteria is known as a **Trusted Operating System (TOS)**. Examples of this include Windows 7, OS X 10.6, FreeBSD (with the TrustedBSD extensions), and Red Hat Enterprise Server. To be considered a TOS, the manufacturer of the system must have strong policies concerning updates and patching.

Even without being a TOS, operating systems should be updated regularly. For example, Microsoft recognizes the deficiencies in an OS, and possible exploits that could occur, and releases patches to increase OS performance and protect the system. After the latest SP has been installed, the next step is to see whether any additional updates are available for download.

For example, if you want to install additional updates for Windows 7 through Windows Update, choose Start > All Programs > Windows Update, and click Check for Updates in the left panel. The system then automatically scans for updates. Updates are divided into the following categories:

- **Critical updates and SPs:** Include the latest SP and other security and stability updates. Some updates must be installed individually; others can be installed as a group.
- **Windows updates:** Recommended updates to fix noncritical problems certain users might encounter; also adds features and updates to features bundled into Windows.
- **Driver updates:** Updated device drivers for installed hardware.

If your system is in need of updates, a shield (for the Windows Security Center) appears in the Notification Area. Double-clicking this brings up the Security Center window in which you can turn on automatic updates. To modify how you are alerted to updates, and how they are downloaded and installed in Windows 7, choose Start > All Programs > Windows Update and then click the Change Settings link.

NOTE Different Windows operating systems might require slightly different navigation. For all versions of Windows consider going to Run and typing `wuapp .exe`.

From here, there will be four options (in other operating systems, the options might be slightly different):

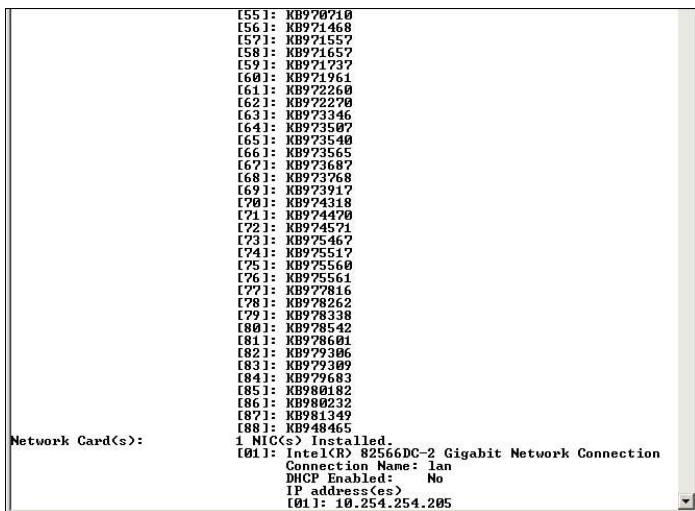
Key Topic

- **Install Updates Automatically:** This is the option recommended by Microsoft. You can schedule when and how often the updates should be downloaded and installed.
- **Download Updates but Let Me Choose Whether to Install Them:** This automatically downloads updates when they become available, but Windows prompts you to install them instead of installing them automatically. Each update has a checkbox, so you can select individual updates to install.
- **Check for Updates but Let Me Choose Whether to Download and Install Them:** This enables you to know when updates are available, but you are in control as to when they are downloaded and installed.
- **Never Check for Updates:** This is not recommended by Microsoft because it can be a security risk, but it might be necessary in some environments in which updates could cause conflicts over the network. In some networks, the administrator takes care of updates from a server and sets the local computers to this option.

Patches and Hotfixes

The best place to obtain patches and hotfixes is from the manufacturer's website. The terms *patches* and *hotfixes* are often used interchangeably. Windows Updates are made up of hotfixes. Originally, a **hotfix** was defined as a single problem-fixing patch to an individual OS or application installed live while the system was up and running and without a reboot necessary. However, this term has changed over time and varies from vendor to vendor. (Vendors may even use both terms to describe the same thing.) For example, if you run the `systeminfo` command in the Command Prompt of a Windows Vista computer, you see a list of Hotfix(es), similar to Figure 3-7. The figure doesn't show all of them because there are 88 in total. However, they can be identified with the letters KB followed by six numbers. Some of these are single patches to individual applications, but others affect the entire system, such as #88, which is called KB948465. This hotfix is actually Windows Vista Service Pack 2!—which includes program compatibility changes, additional hardware support, and general OS updates. And a Service Pack 2 installation definitely requires a restart.

Key Topic



```

[55]: KB9900710
[56]: KB991468
[57]: KB991455?
[58]: KB991657
[59]: KB991737
[60]: KB991961
[61]: KB992260
[62]: KB992270
[63]: KB997346
[64]: KB997356?
[65]: KB997359
[66]: KB9973655
[67]: KB9973687
[68]: KB9973768
[69]: KB9973917
[70]: KB9974318
[71]: KB9974470
[72]: KB9974571
[73]: KB9975467
[74]: KB9975517
[75]: KB9975560
[76]: KB9975561
[77]: KB9977816
[78]: KB9978262
[79]: KB9978338
[80]: KB9978542
[81]: KB9978681
[82]: KB9979386
[83]: KB9979389
[84]: KB9980182
[85]: KB9980182
[86]: KB9980232
[87]: KB9981349
[88]: KB9948465

Network Card(s):
1 NIC(s) Installed.
  01: Intel(R) 82566DC-2 Gigabit Network Connection
      Connection Name: lan
      DHCP Enabled: No
      IP address(es):
        01: 10.254.254.205
  
```

Figure 3-7 Running the systeminfo Command in Windows

On the other side of the spectrum, Blizzard Entertainment defines hotfixes in its World of Warcraft game as a “hot” change to the server with no downtime (or a quick world restart), and no client download is necessary. The organization releases these if they are critical, instead of waiting for a full patch version. The gaming world commonly uses the terms *patch version*, *point release*, or *maintenance release* to describe a group of file updates to a particular gaming version. For example, a game might start at version 1 and later release an update known as 1.17. The .17 is the point release. (This could be any number, depending on the amount of code re-writes.) Later, the game might release 1.32, in which .32 is the point release, again otherwise referred to as the patch version. This is common with other programs as well. For example, the aforementioned Camtasia program that is running on the computer shown in Figure 3-1 is version 5.0.2. The second dot (.2) represents very small changes to the program, whereas a patch version called 5.1 would be a larger change, and 6.0 would be a completely new version of the software. This concept also applies to blogging applications and forums (otherwise known as bulletin boards). As new threats are discovered (and they are extremely common in the blogging world), new patch versions are released. They should be downloaded by the administrator, tested, and installed without delay. Admins should keep in touch with their software manufacturers, either through phone or e-mail, or by frequenting their web pages. This keeps the admin “in the know” when it comes to the latest updates. And this applies to server and client operating systems, server add-ons such as Microsoft Exchange or SQL Server, Office programs, web browsers, and the plethora of third-party programs that an organization might use. Your job just got a bit busier!

Of course, we are usually not concerned with updating games in the working world; they should be removed from a computer if they are found (unless perhaps you work for a gaming company). But multimedia software such as Camtasia is prevalent in most companies, and web-based software such as bulletin-board systems are also common and susceptible to attack.

Patches generally carry the connotation of a small fix in the mind of the user or system administrator, so larger patches are often referred to as software updates, service packs, or something similar. However, if you were asked to fix a single security issue on a computer, a patch would be the solution you would want. For example, there are various Trojans that attack older versions of Microsoft Office for Mac. To counter these, Microsoft released a specific patch for those versions of Office for Mac that disallows remote access by the Trojans.

Before installing an individual patch, you should determine if it perhaps was already installed as part of a group update. For example, you might read that OS X 10.8 had a patch released for iTunes, and being an enthusiastic iTunes user, you might consider installing the patch. But you should first find out the version of the OS you are running. For example, Figure 3-8 shows a Mac that runs OS X version 10.9.1. That would most likely include the earlier patch for iTunes. To find this information, simply click the Apple menu and then click About This Mac.



Figure 3-8 OS X Version Number

Sometimes, patches are designed poorly, and although they might fix one problem, they could possibly create another, which is a form of software regression. Because you never know exactly what a patch to a system might do, or how it might react or interact with other systems, it is wise to incorporate patch management.

Patch Management

It is not wise to go running around the network randomly updating computers, not to say that you would do so! Patching, like any other process, should be managed properly. **Patch management** is the planning, testing, implementing, and auditing of patches. Now, these four steps are ones that I use; other companies might have a slightly different patch management strategy, but each of the four concepts should be included:

- **Planning:** Before actually doing anything, a plan should be set into motion. The first thing that needs to be decided is whether the patch is necessary and whether it is compatible with other systems. Microsoft Baseline Security Analyzer (MBSA) is one example of a program that can identify security misconfigurations on the computers in your network, letting you know whether patching is needed. If the patch is deemed necessary, the plan should consist of a way to test the patch in a “clean” network on clean systems, how and when the patch will be implemented, and how the patch will be checked after it is installed.
- **Testing:** Before automating the deployment of a patch among a thousand computers, it makes sense to test it on a single system or small group of systems first. These systems should be reserved for testing purposes only and should not be used by “civilians” or regular users on the network. I know, this is asking a lot, especially given the amount of resources some companies have. But the more you can push for at least a single testing system that is not a part of the main network, the less you will be to blame if a failure occurs!
- **Implementing:** If the test is successful, the patch should be deployed to all the necessary systems. In many cases this is done in the evening or over the weekend for larger updates. Patches can be deployed automatically using software such as Microsoft’s System Center Configuration Manager (SCCM) or the older Systems Management Server (SMS).
- **Auditing:** When the implementation is complete, the systems (or at least a sample of systems) should be audited; first, to make sure the patch has taken hold properly, and second, to check for any changes or failures due to the patch. SCCM, SMS, and other third-party tools can be used in this endeavor.

Key Topic

NOTE The concept of patch management, in combination with other application/OS hardening techniques, is collectively referred to as *configuration management*.

There are also Linux-based and Mac-based programs and services developed to help manage patching and the auditing of patches. Red Hat has services to help sys

admins with all the RPMs they need to download and install, which can become a mountain of work quickly! And for those people who run GPL Linux, there are third-party services as well. A network with a lot of mobile devices benefits greatly from the use of a mobile device management (MDM) platform. But even with all these tools at an organization's disposal, sometimes, patch management is just too much for one person, or for an entire IT department, and an organization might opt to contract that work out.

Group Policies, Security Templates, and Configuration Baselines

Although they are important tasks, removing applications, disabling services, patching, hotfixing, and installing service packs are not the only ways to harden an operating system. Administrative privileges should be used sparingly, and policies should be in place to enforce your organization's rules. A **Group Policy** is used in Microsoft and other computing environments to govern user and computer accounts through a set of rules. Built-in or administrator-designed security templates can be applied to these to configure many rules at one time. Afterward, configuration baselines should be created and used to measure server and network activity.

To access the Group Policy in Windows, go to the Run prompt and type `gpedit.msc`. This should display the Local Group Policy Editor console window. Figure 3-9 shows an example of this in Windows 7.

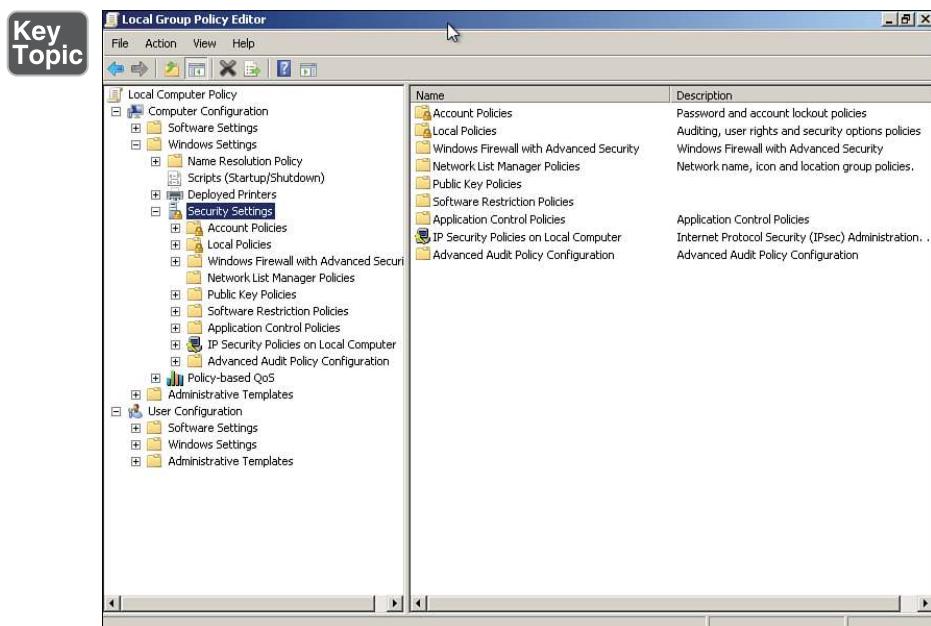


Figure 3-9 Local Group Policy Editor in Windows 7

Although there are many configuration changes you can make, this figure focuses on the computer's security settings that can be accessed by navigating to Local Computer Policy > Computer Configuration > Windows Settings > Security Settings. From here you can make changes to the password policies (for example, how long a password lasts before having to be changed), account lockout policies, public key policies, and so on. We talk about these different types of policies and the best way to apply them in future chapters. The Group Policy Editor in the figure is known as the Local Group Policy Editor and only governs that particular machine and the local users of that machine. It is a basic version of the Group Policy Editor used by Windows Server domain controllers that have Active Directory loaded.

It is also from here that you can add security templates as well. **Security templates** are groups of policies that can be loaded in one procedure; they are commonly used in corporate environments. Different security templates have different security levels. These can be installed by right-clicking Security Settings and selecting Import Policy. This brings up the Import Policy From window. This technique of adding a policy template becomes much more important on Windows Server computers. Figure 3-10 shows an example of the Import Policy From window in Windows Server 2012.

There are three main security templates in Server 2012/2008: defltbase.inf (uncommon), defltsv.inf (used on regular servers), and defldc.inf (used in domain controllers). By default, these templates are stored in %systemroot%\inf (among a lot of other .inf files).

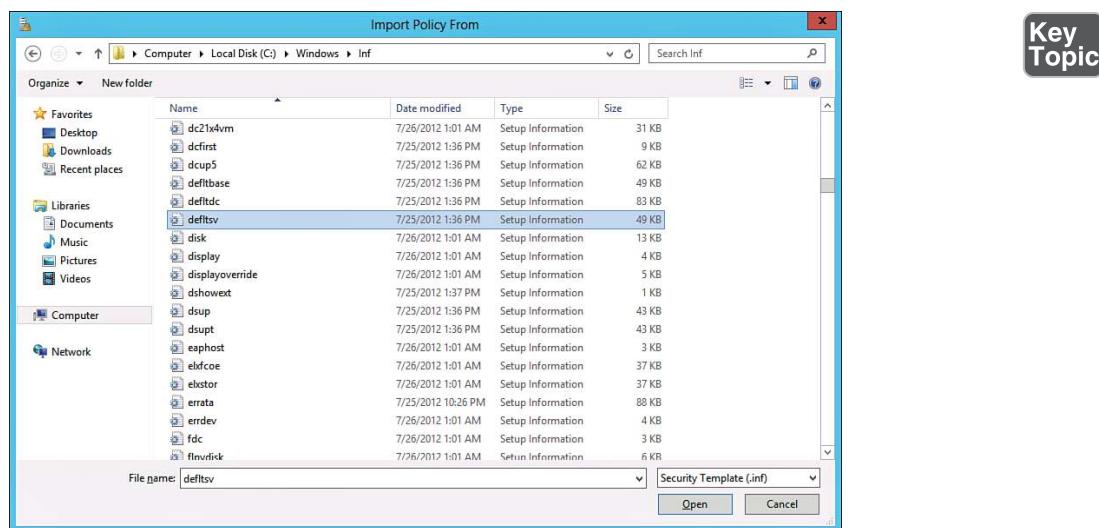


Figure 3-10 Windows Server 2012 Import Policy From Window

Select the policy you desire and click Open. That establishes the policy on the server. It's actually many policies that are written to many locations of the entire Local Security Policy window. Often, these policy templates are applied to organizational units on a domain controller. But they can be used for other types of systems and policies as well.

NOTE Policies are imported in the same manner in Server 2003, but the names are different. For example, the file securedc.inf is an information file filled with policy configurations more secure than the default you would find in a Windows Server 2003 domain controller that runs Active Directory. And hisecd.inf is even more secure, perhaps too secure and limiting for some organizations. Server Templates for Server 2003 are generally stored in %systemroot%\Security\templates.

In Server 2012 you can modify policies, and add templates, directly from Server Manager > Security Configuration Wizard as well. If you save templates here, they are saved as .xml files instead of .inf files.

Group Policies are loaded with different Group Policy objects (GPOs). By configuring as many of these GPOs as possible, you implement OS hardening, ultimately establishing host-based security for your organization's workstations.

Baselining is the process of measuring changes in networking, hardware, software, and so on. Creating a baseline consists of selecting something to measure and measuring it consistently for a period of time. For example, I might want to know what the average hourly data transfer is to and from a server. There are many ways to measure this, but I could possibly use a protocol analyzer to find out how many packets cross through the server's network adapter. This could be run for 1 hour (during business hours of course) every day for 2 weeks. Selecting different hours for each day would add more randomness to the final results. By averaging the results together, we get a baseline. Then we can compare future measurements of the server to the baseline. This can help us to define what the standard load of our server is and the requirements our server needs on a consistent basis. It can also help when installing additional computers on the network. The term *baselining* is most often used to refer to monitoring network performance, but it actually can be used to describe just about any type of performance monitoring. Baselining and benchmarking are extremely important when testing equipment and when monitoring already installed devices. We discuss this further in Chapter 12, "Monitoring and Auditing."

Hardening File Systems and Hard Drives

You want more? I promise *more*. The rest of the book constantly refers to more advanced and in-depth ways to harden a computer system. But for this chapter, let's conclude this section by giving a few tips on hardening a hard drive and the file system it houses.

First, the file system used dictates a certain level of security. On Microsoft computers, the best option is to use NTFS, which is more secure, enables logging (oh so important), supports encryption, and has support for a much larger maximum partition size and larger file sizes. Just about the only place where FAT32 and NTFS are on a level playing field is that they support the same amount of file formats. So, by far, NTFS is the best option. If a volume uses FAT or FAT32, it can be *converted* to NTFS using the following command:

```
convert volume /FS:NTFS
```

For example, if I want to convert a USB flash drive named M: to NTFS, the syntax would be

```
convert M: /FS:NTFS
```

There are additional options for the convert command. To see these, simply type convert /? in the Command Prompt. NTFS enables for file-level security and tracks permissions within access control lists (ACLs), which are a necessity in today's environment. Most systems today already use NTFS, but you never know about flash-based and other removable media. A quick chkdsk command in the Command Prompt or right-clicking the drive in the GUI and selecting Properties can tell you what type of file system it runs.

Generally, the best file system for Linux systems is ext4. It allows for the best and most configurable security. To find out the file system used by your version of Linux, use the fdisk -l command or df -T command.

System files and folders by default are hidden from view to protect a Windows system, but you never know. To permanently configure the system to not show hidden files and folders, navigate to Windows Explorer or File Explorer, click the Tools menu, and click Folder Options. Then select the View tab, and under Hidden Files and Folders select the Do Not Show Hidden Files and Folders radio button. Note that in newer versions of Windows, the menu bar can also be hidden; to view it, press Alt+T on the keyboard. To configure the system to hide protected system files, select the Hide Protected Operating System Files checkbox, located three lines below the radio button previously mentioned. This disables the ability to view such files and folders as bootmgr, boot, ntldr, and boot.ini. You might also need to secure a system by turning off file sharing. For example, this can be done in Windows 7

within the Network and Sharing Center, and within Windows XP in the Local Area Connection Properties dialog box.

In the past, I have made a bold statement: “Hard disks *will* fail.” But it’s all too true. It’s not a matter of *if*; it’s a matter of *when*. By maintaining and hardening the hard disk with various hard disk utilities, we attempt to stave off that dark day as long as possible. You can implement several things when maintaining and hardening a hard disk:

Key Topic

- **Remove temporary files:** Temporary files and older files can clog up a hard disk, cause a decrease in performance, and pose a security threat. It is recommended that Disk Cleanup or a similar program be used. Policies can be configured (or written) to run Disk Cleanup every day or at logoff for all the computers on the network.
- **Periodically check system files:** Every once in a while it’s a good idea to verify the integrity of operating system files. This can be done in the following ways:
 - With the `chkdsk` command in Windows. This checks the disk and fixes basic issues such as lost files, and some errors with the `/F` option.
 - With the `SFC` (System File Checker) command in Windows. This utility checks and, if necessary, replaces protected system files. It can be used to fix problems in the OS, and in other applications such as Internet Explorer. A typical command you might type is `SFC /scannow`. Use this if `chkdsk` is not successful at making repairs.
 - With the `fsck` command in Linux. This command is used to check and repair a Linux file system. The synopsis of the syntax is `fsck [-sAVRTNP] [-C [fd]] [-t fstype] [filesystem ...] [--] [fs-specific-options]`. More information about this command can be found at the corresponding MAN page for `fsck`. A derivative, `e2fsck`, is used to check a Linux ext2fs (second extended file system). Also, open source data integrity tools can be downloaded for Linux such as Tripwire.
- **Defragment drives:** Applications and files on hard drives become fragmented over time. For a server, this could be a disaster, because the server cannot serve requests in a timely fashion if the drive is too thoroughly fragmented. Defragmenting the drive can be done with Microsoft’s Disk Defragmenter, with the command-line `defrag` command, or with other third-party programs.
- **Back up data:** Backing up data is critical for a company. It is not enough to rely on a fault-tolerant array. Individual files or the entire system can be backed up to another set of hard drives, to optical discs, to tape, or to the cloud. Microsoft domain controllers’ Active Directory databases are particularly susceptible to

attack; the System State for these operating systems should be backed up, in case that the server fails and the Active Directory needs to be recovered in the future.

- **Use restoration techniques:** In Windows, restore points should be created on a regular basis for servers and workstations. The System Restore utility (rstrui.exe) can fix issues caused by defective hardware or software by reverting back to an earlier time. Registry changes made by hardware or software are reversed in an attempt to force the computer to work the way it did previously. Restore points can be created manually and are also created automatically by the OS before new applications, service packs, or hardware are installed. OS X uses the Time Machine utility, which works in a similar manner. Though there is no similar tool in Linux, a user can back up the ~/home directory to a separate partition. When these contents are decompressed to a new install, most of the Linux system and settings will have been restored. Another option in general is to use imaging (cloning) software such as Acronis True Image, Paragon Hard Disk Manager, or PowerISO. Remember that these techniques do not necessarily back up data, and that the data should be treated as a separate entity that needs to be backed up regularly.
- **Consider whole disk encryption:** Finally, whole disk encryption can be used to secure the contents of the drive, making it harder for attackers to obtain and interpret its contents.

A recommendation I give to all my students and readers is to separate the OS from the data physically. If you can have each on a separate hard drive, it can make things a bit easier just in case the OS is infected with malware (or otherwise fails). The hard drive that the OS inhabits can be completely wiped and reinstalled without worrying about data loss, and applications can always be reloaded. Of course, settings should be backed up (or stored on the second drive). If a second drive isn't available, consider configuring the one hard drive as two partitions, one for the OS (or system) and one for the data. By doing this, and keeping a well-maintained computer, you are effectively hardening the OS.

Key Topic

Keeping a Well-Maintained Computer

This is an excerpt of an article I wrote that I give to all my customers and students. By maintaining the workstation or server, you are hardening it as well. I break it down into six steps (and one optional step):

Step 1. Use a surge protector or UPS—Make sure the computer and other equipment connect to a surge protector, or better yet a UPS if you are concerned about power loss.

- Step 2. Update the BIOS and/or UEFI**—Flashing the BIOS isn't always necessary; check the manufacturer's website for your motherboard to see if an update is needed.
- Step 3. Update the OS**—For Windows, this includes the latest SPs and any Windows Updates beyond that, and setting Windows to alert if there are any new updates. For Linux and OS X, it means simply updating the system to the latest version and installing individual patches as necessary.
- Step 4. Update anti-malware**—This includes making sure that there is a current license for the anti-malware (antivirus and anti-spyware) and verifying that updates are turned on and the software is regularly scanning the system.
- Step 5. Update the firewall**—Be sure to have some kind of firewall installed and enabled; then update it. If it is Windows Firewall, updates should happen automatically through Windows Update. However, if you have a SOHO router with a built-in firewall, or other firewall device, you need to update the device's ROM by downloading the latest image from the manufacturer's website.
- Step 6. Maintain the disks**—This means running a disk cleanup program regularly and checking to see whether the hard disk needs to be defragmented from once a week to once a month depending on the amount of usage. It also means creating restore points, doing computer backups, or using third-party backup or drive imaging software.
- Step 7. (Optional) Create an image of the system**—After all your configurations and hardening of the OS are complete, you might consider creating an image of the system. Imaging the system is like taking a snapshot of the entire system partition. That information is saved as one large file, or a set of compressed files that can be saved anywhere. It's kind of like system restore but at another level. The beauty of this is that you can reinstall the entire image if your system fails or is compromised, quickly and efficiently, with very little configuration necessary—only the latest security and AV updates since the image was created need be applied. Of course, most imaging software has a price tag involved, but it can be well worth it if you are concerned about the time it would take to get your system back up and running in the event of a failure. This is the basis for standardized images in many organizations. By applying mandated security configurations, updates, and so on, and then taking an image of the system, you can create a snapshot in time that you can easily revert to if necessary, while being confident that a certain level of security is already embedded into the image.

NOTE To clean out a system regularly, consider re-imaging it, or if a mobile device, resetting it. This takes care of any pesky malware by deleting everything and reinstalling to the point in time of the image, or to factory condition. While you will have to do some reconfigurations, the system will also run much faster because it has been completely cleaned out.

Virtualization Technology

Let's define virtualization. **Virtualization** is the creation of a virtual entity, as opposed to a true or actual entity. The most common type of entity created through virtualization is the virtual machine—usually as an OS. In this section we discuss types of virtualization, identify their purposes, and define some of the various virtual applications.

Types of Virtualization and Their Purposes

Many types of virtualization exist, from network and storage to hardware and software. The CompTIA Security+ exam focuses mostly on virtual machine software. The **virtual machines (VMs)** created by this software run operating systems or individual applications. These virtual operating systems (also known as hosted operating systems or guests) are designed to run *inside* a real OS. So the beauty behind this is that you can run multiple various operating systems simultaneously from just one PC. This has great advantages for programmers, developers, and systems administrators, and can facilitate a great testing environment. Security researchers in particular utilize virtual machines so they can execute and test malware without risk to an actual OS and the hardware it resides on. Nowadays, many VMs are also used in live production environments. Plus, an entire OS can be dropped onto a DVD or even a flash drive and transported where you want to go.

Of course, there are drawbacks. Processor and RAM resources and hard drive space are eaten up by virtual machines. And hardware compatibility can pose some problems as well. Also, if the physical computer that houses the virtual OS fails, the virtual OS will go offline immediately. All other virtual computers that run on that physical system will also go offline. There is added administration as well. Some technicians forget that virtual machines need to be updated with the latest service packs and patches just like regular operating systems. Many organizations have policies that define standardized virtual images, especially for servers. As I alluded to earlier, the main benefit of having a standardized server image is that mandated security configurations will have been made to the OS from the beginning—creating a template, so to speak. This includes a defined set of security updates, service packs, patches, and so on, as dictated by organizational policy. So when you load up a new

instance of the image, a lot of the configuration work will already have been done, and just the latest updates to the OS and AV software need to be applied. This image can be used in a virtual environment, or copied to a physical hard drive as well. For example, you might have a server farm that includes two physical Windows Server systems and four virtual Windows Server systems, each running different tasks. It stands to reason that you will be working with new images from time to time as you need to replace servers or add them. By creating a standardized image once, and using it many times afterward, you can save yourself a lot of configuration time in the long run.

Virtual machines can be broken down into two categories:

- **System virtual machine:** A complete platform meant to take the place of an entire computer, enabling you to run an entire OS virtually.
- **Process virtual machine:** Designed to run a single application, such as a virtual web browser.

Whichever VM you select, the VM cannot cross the software boundaries set in place. For example, a virus might infect a computer when executed and spread to other files in the OS. However, a virus executed in a VM will spread through the VM but not affect the underlying *actual* OS. So this provides a secure platform to run tests, analyze malware, and so on...and creates an *isolated* system. If there are adverse effects to the VM, those effects (and the VM) can be compartmentalized to stop the spread of those effects. This is all because the virtual machine inhabits a separate area of the hard drive from the actual OS. This enables us to isolate network services and roles that a virtual server might play on the network.

Virtual machines are, for all intents and purposes, emulators. The terms *emulation*, *simulation*, and *virtualization* are often used interchangeably. Emulators can also be web-based; for example, an emulator of a SOHO router's firmware that you can access online. You might also have heard of much older emulators such as Basilisk, or the DOSBox, or a RAM drive, but nowadays, anything that runs an OS virtually is generally referred to as a virtual machine or virtual appliance.

A *virtual appliance* is a virtual machine image designed to run on virtualization platforms; it can refer to an entire OS image or an individual application image. Generally, companies such as VMware refer to the images as virtual appliances, and companies such as Microsoft refer to images as virtual machines. One example of a virtual appliance that runs a single app is a virtual browser. VMware developed a virtual browser appliance that protects the underlying OS from malware installations from malicious websites. If the website succeeds in its attempt to install the malware to the virtual browser, the browser can be deleted and either a new one can be created or an older saved version of the virtual browser can be brought online!

Other examples of virtualization include the virtual private network (VPN), which is covered in Chapter 9, “Physical Security and Authentication Models,” and the virtual local area network (VLAN), which is covered in Chapter 5, “Network Design Elements.”

Hypervisor

Most virtual machine software is designed specifically to host more than one VM. A byproduct is the intention that all VMs are able to communicate with each other quickly and efficiently. This concept is summed up by the term **hypervisor**. A hypervisor allows multiple virtual operating systems (guests) to run at the same time on a single computer. It is also known as a virtual machine manager (VMM). The term hypervisor is often used ambiguously. This is due to confusion concerning the two different types of hypervisors:

- **Type 1: Native**—The hypervisor runs directly on the host computer’s hardware. Because of this it is also known as “bare metal.” Examples of this include VMware vCenter and vSphere, Citrix XenServer, and Microsoft Hyper-V. Hyper-V can be installed as a standalone product, known as Microsoft Hyper-V Server, or it can be installed as a role within a standard installation of Windows Server 2008 (R2) or higher. Either way, the hypervisor runs independently and accesses hardware directly, making both versions of Windows Server Hyper-V Type 1 hypervisors.
- **Type 2: Hosted**—This means that the hypervisor runs within (or “on top of”) the operating system. Guest operating systems run within the hypervisor. Compared to Type 1, guests are one level removed from the hardware and therefore run less efficiently. Examples of this include Microsoft Virtual PC 2007, Windows Virtual PC (for Windows 7), Hyper-V (for Windows 8), VirtualBox, VMware Server, and VMware Workstation.

Key Topic

Generally, Type 1 is a much faster and much more efficient solution than Type 2. It is also more elastic, meaning that environments using Type 1 hypervisors can usually respond to quickly changing business needs by adjusting the supply of resources as necessary. Because of this elasticity and efficiency, Type 1 hypervisors are the kind used by web-hosting companies and by companies that offer cloud computing solutions such as infrastructure as a service (IaaS). It makes sense too. If you have ever run a powerful operating system such as Windows Server 2012/2008 within a Type 2 hypervisor such as Windows Virtual PC, you will have noticed that a ton of resources are being used that are taken from the hosting operating system. It is not nearly as efficient as running the hosted OS within a Type 1 environment. However, keep in mind that the hardware/software requirements for a Type 1 hypervisor

are more stringent and more costly. Because of this, some developing and testing environments use Type 2-based virtual software.

Securing Virtual Machines

In general, the security of a virtual machine operating system is the equivalent to that of a physical machine OS. The VM should be updated to the latest service pack. If you have multiple VMs, especially ones that will interact with each other, make sure they are updated in the same manner. This will help to ensure patch compatibility between the VMs. A VM should have the newest AV definitions, perhaps have a personal firewall, have strong passwords, and so on. However, there are several things to watch out for that, if not addressed, could cause all your work compartmentalizing operating systems to go down the drain. This includes considerations for the virtual machine OS as well as the controlling virtual machine software.

First, make sure you are using current and updated virtual machine software. Update to the latest patch for the software you are using (for example, the latest version of Oracle VirtualBox). Configure any applicable security settings or options in the virtual machine software. Once this is done, you can go ahead and create your virtual machines, keeping in mind the concept of standardized imaging mentioned earlier.

Next, keep an eye out for network shares and other connections between the virtual machine and the physical machine, or between two VMs. Normally, malicious software cannot travel between a VM and another VM or a physical machine as long as they are properly separated. But if active network shares are between the two, malware could easily spread from one system to the other. If a network share is needed, map it, use it, and then disconnect it when you are finished. If you need network shares between two VMs, document what they are and which systems (and users) connect to them. Review the shares often to see whether they are still necessary. Be careful with VMs that use a *bridged* or similar network connection, instead of network address translation (NAT). This method connects directly with other physical systems on the network, and can allow for malware and attacks to traverse the “bridge” so to speak. If a virtual host is attached to a network attached storage (NAS) device or to a storage area network (SAN), it is recommended to segment the storage devices off the LAN either physically or with a secure VLAN. Regardless of where the virtual host is located, secure it with a strong firewall and disallow unprotected file transfer protocols such as FTP and Telnet.

Consider disabling any unnecessary hardware from within the virtual machine such as optical drives, USB ports, and so on. If some type of removable media is necessary, enable the device, make use of it, and then disable it immediately after finishing. Also, devices can be disabled from the virtual machine software itself. The

boot priority in the virtual BIOS should also be configured so that the hard drive is booted from first, and not any removable media or network connection (unless necessary in your environment).

Due to the fact that VMs use a lot of physical resources of the computer, a compromised VM can be a threat in the form of a denial-of-service attack. To mitigate this, set a limit on the amount of resources any particular VM can utilize, and periodically monitor the usage of VMs. However, be careful of monitoring VMs. Most virtual software offers the ability to monitor the various VMs from the main host, but this feature can also be exploited. Be sure to limit monitoring, enable it only for authorized users, and disable it whenever not necessary.

Finally, be sure to protect the raw virtual disk file. A disaster on the raw virtual disk can be tantamount to physical disk disaster. Look into setting permissions as to who can access the folder where the VM files are stored. If your virtual machine software supports logging and/or auditing, consider implementing it so that you can see exactly who started and stopped the virtual machine, and when. Otherwise, you can audit the folder where the VM files are located. Finally, consider making a copy of the virtual machine or virtual disk file, also known as a *snapshot*, encrypting the VM disk file, and digitally signing the VM and validating that signature prior to usage.

NOTE Enterprise-level virtual software such as Hyper-V and VMware vCenter/vSphere takes security to a whole new level. Much more planning and configuration is necessary for these applications. It's not necessary to know for the Security+ exam, but if you want to gather more information on securing Hyper-V, see the following link:

<http://technet.microsoft.com/en-us/library/dd569113.aspx>

For more information on how to use and secure VMware, see the following link:

<http://www.vmware.com/products/vsphere/resources.html>

One last comment: A VM should be as secure as possible, but in general, because the hosting computer is in a controlling position, it is likely to be more easily exploited, and a compromise to the hosting computer probably means a compromise to any guest operating systems it contains. Therefore, if possible, the host should be even more secure than the VMs it controls. So harden your heart, harden the VM, and make the hosting OS solid as a rock.

Chapter Summary

This chapter focused on the hardening of operating systems and the securing of virtual operating systems. Out-of-the-box operating systems can often be insecure for a variety of reasons and need to be *hardened* to meet your organization’s policies, Trusted Operating System (TOS) compliance, and government regulations. But in general, they need to be hardened so that they are more difficult to compromise.

The process of hardening an operating system includes: removing unnecessary services and applications; whitelisting and blacklisting applications; using anti-malware applications; configuring personal software-based firewalls; updating to the latest patch or service pack (as well as managing those patches); using group policies, security templates, and baselining; utilizing a secure file system and performing preventive maintenance on hard drives; and in general, keeping a well-maintained computer.

Well, that’s a lot of work, especially for one person. That makes the use of *automation* very important. Automate your work whenever you can through the use of templates, the imaging of systems, and by using specific workflow methods. These things, in conjunction with well-written policies, can help you (or your team) to get work done faster and more efficiently.

One great way to be more efficient (and possibly more secure) is by using *virtualization*, the creation of a virtual machine or other emulator that runs in a virtual environment, instead of requiring its own physical computer. It renders dual-booting pretty much unnecessary, and can offer a lot of options when it comes to compartmentalization and portability. The virtual machine runs in a hypervisor—either Type 1, which is also known as bare metal, or Type 2, which is hosted. Type 1 is faster and more efficient, but usually more expensive and requires greater administrative skill. Regardless of the type you use, the hypervisor, and the virtual machines it contains, needs to be secured.

The hosting operating system, if there is one, should be hardened appropriately. The security administrator should update the virtual machine software to the latest version and configure applicable security settings for it. Individual virtual machines should have their virtual BIOS secured, and the virtual machine itself should be hardened the same way a regular, or *non-virtual*, operating system would be. (That clarification is important, because many organizations today have more virtual servers than non-virtual servers! The term “regular” becomes inaccurate in some scenarios.) Unnecessary hardware should be disabled, and network connections should be carefully planned and monitored. In addition, the administrator should consider setting limits on the resources a virtual machine can consume, monitor the virtual machine (and its files), and protect the virtual machine through file permissions and encryption. And of course, *all* virtual systems should be tested thoroughly before being placed into

production. It's the implementation of security control testing that will ensure compatibility between VMs and virtual hosting software, reduce the chances of exploitation, and offer greater efficiency and less downtime in the long run.

Chapter 3 builds on Chapter 2. Most of the methods mentioned during Chapter 2 are expected to be implemented in addition to the practices listed in this chapter. By combining them with the software protection techniques we will cover in Chapter 4, “Application Security,” you will end up with quite a secure computer system.

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 3-2 lists a reference of these key topics and the page number on which each is found.

Table 3-2 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
Figure 3-2	Services window in Windows XP	87
Figure 3-3	Telnet Properties dialog box	88
Figure 3-4	Stopping and disabling a service in the Windows 7 Command Prompt	89
Table 3-1	Summary of ways to stop services	92
Bullet list	Windows Update options	96
Figure 3-7	<code>systeminfo</code> command in Windows	97
Bulleted list	Patch management four steps	99
Figure 3-9	Local Group Policy Editor in Windows 7	100
Figure 3-10	Windows Server 2012 Import Policy From window	101
Bulleted list	Maintaining a hard disk	104
Numbered list	Keeping a well-maintained computer	105
Bulleted list	Types of hypervisors	109

Define Key Terms

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

hardening, application blacklisting, service pack (SP), Trusted Operating System (TOS), hotfix, patch, patch management, Group Policy, security template, baselining, virtualization, virtual machine, hypervisor

Review Questions

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

1. Virtualization technology is often implemented as operating systems and applications that run in software. Often, it is implemented as a virtual machine. Of the following, which can be a security benefit when using virtualization?
 - A. Patching a computer will patch all virtual machines running on the computer.
 - B. If one virtual machine is compromised, none of the other virtual machines can be compromised.
 - C. If a virtual machine is compromised, the adverse effects can be compartmentalized.
 - D. Virtual machines cannot be affected by hacking techniques.
2. Eric wants to install an isolated operating system. What is the best tool to use?
 - A. Virtualization
 - B. UAC
 - C. HIDS
 - D. NIDS
3. Where would you turn off file sharing in Windows 7?
 - A. Control Panel
 - B. Local Area Connection
 - C. Network and Sharing Center
 - D. Firewall properties
4. Which option enables you to hide ntldr?
 - A. Enable Hide Protected Operating System Files

- B.** Disable Show Hidden Files and Folders
 - C.** Disable Hide Protected Operating System Files
 - D.** Remove the -R Attribute
- 5. Which of the following should be implemented to harden an operating system? (Select the two best answers.)
 - A.** Install the latest service pack.
 - B.** Install Windows Defender.
 - C.** Install a virtual operating system.
 - D.** Execute PHP scripts.
- 6. What is the best (most secure) file system to use in Windows?
 - A.** FAT
 - B.** NTFS
 - C.** DFS
 - D.** FAT32
- 7. A customer's computer uses FAT16 as its file system. What file system can you upgrade it to when using the convert command?
 - A.** NTFS
 - B.** HPFS
 - C.** FAT32
 - D.** NFS
- 8. Which of the following is not an advantage of NTFS over FAT32?
 - A.** NTFS supports file encryption.
 - B.** NTFS supports larger file sizes.
 - C.** NTFS supports larger volumes.
 - D.** NTFS supports more file formats.
- 9. What is the deadliest risk of a virtual computer?
 - A.** If a virtual computer fails, all other virtual computers immediately go offline.
 - B.** If a virtual computer fails, the physical server goes offline.
 - C.** If the physical server fails, all other physical servers immediately go offline.

- D. If the physical server fails, all the virtual computers immediately go offline.
10. Virtualized browsers can protect the OS that they are installed within from which of the following?
- A. DDoS attacks against the underlying OS
 - B. Phishing and spam attacks
 - C. Man-in-the-middle attacks
 - D. Malware installation from Internet websites
11. Which of the following needs to be backed up on a domain controller to recover Active Directory?
- A. User data
 - B. System files
 - C. Operating system
 - D. System State
12. Which of the following should you implement to fix a single security issue on the computer?
- A. Service pack
 - B. Support website
 - C. Patch
 - D. Baseline
13. An administrator wants to reduce the size of the attack surface of a Windows Server. Which of the following is the best answer to accomplish this?
- A. Update antivirus software.
 - B. Install service packs.
 - C. Disable unnecessary services.
 - D. Install network intrusion detection systems.
14. You finished installing the operating system for a home user. What are three good methods to implement to secure that operating system? (Select the three best answers.)
- A. Install the latest service pack.
 - B. Install a hardware- or software-based firewall.

- C. Install the latest patches.
 - D. Install a remote desktop tech support program.
15. Which of the following is a security reason to implement virtualization in your network?
- A. To isolate network services and roles
 - B. To analyze network traffic
 - C. To add network services at lower costs
 - D. To centralize patch management
16. Which of the following is one example of verifying new software changes on a test system?
- A. Application hardening
 - B. Virtualization
 - C. Patch management
 - D. HIDS
17. You have been tasked with protecting an operating system from malicious software. What should you do? (Select the two best answers.)
- A. Disable the DLP.
 - B. Update the HIPS signatures.
 - C. Install a perimeter firewall.
 - D. Disable unused services.
 - E. Update the NIDS signatures.
18. You are attempting to establish host-based security for your organization's workstations. Which of the following is the *best* way to do this?
- A. Implement OS hardening by applying GPOs.
 - B. Implement database hardening by applying vendor guidelines.
 - C. Implement web server hardening by restricting service accounts.
 - D. Implement firewall rules to restrict access.
19. In Windows, which of the following commands will *not* show the version number?
- A. Systeminfo
 - B. Wf.msc

C. Winver

D. Msinfo32.exe

- 20.** During an audit of your servers, you have noticed that most servers have large amounts of free disk space and have low memory utilization. Which of the following statements will be correct if you migrate some of the servers to a virtual environment?
- A.** You might end up spending more on licensing, but less on hardware and equipment.
 - B.** You will need to deploy load balancing and clustering.
 - C.** Your baselining tasks will become simpler.
 - D.** Servers will encounter latency and lowered throughput issues.

Answers and Explanations

- 1. C.** By using a virtual machine (which is one example of a virtual instance), any ill effects can be compartmentalized to that particular virtual machine, usually without any ill effects to the main operating system on the computer. Patching a computer does not automatically patch virtual machines existing on the computer. Other virtual machines can be compromised, especially if nothing is done about the problem. Finally, virtual machines can definitely be affected by hacking techniques. Be sure to secure them!
- 2. A.** Virtualization enables a person to install operating systems (or applications) in an isolated area of the computer's hard drive, separate from the computer's main operating system.
- 3. C.** The Network and Sharing Center is where you can disable file sharing in Windows 7. It can be accessed indirectly from the Control Panel as well. By disabling file sharing, you disallow any (normal) connections to data on the computer. This can be very useful for computers with confidential information, such as an executive's laptop or a developer's computer.
- 4. A.** To hide ntldr you need to enable the Hide Protected Operating System Files checkbox. Keep in mind that you should have already enabled the Show Hidden Files and Folders radio button.
- 5. A. and B.** Two ways to harden an operating system include installing the latest service pack and installing Windows Defender. However, virtualization is a separate concept altogether; it can be used to create a compartmentalized OS, but needs to be secured and hardened just like any other OS. PHP scripts will

generally not be used to harden an operating system. In fact, they can be vulnerabilities to websites and other applications.

6. **B.** NTFS is the most secure file system for use with today's Windows. FAT and FAT32 are older file systems, and DFS is the distributed file system used in more advanced networking.
7. **A.** The convert command is used to upgrade FAT and FAT32 volumes to the more secure NTFS without loss of data. HPFS is the High Performance File System developed by IBM and is not used by Windows. NFS is the Network File System, something you would see in a storage area network.
8. **D.** NTFS and FAT32 support the same number of file formats, so this is not an advantage of NTFS. However, NTFS supports file encryption, larger file sizes, and larger volumes, making it more advantageous in general in comparison to FAT32, and is capable of higher levels of security, most especially down to the file level.
9. **D.** The biggest risk of running a virtual computer is that it will go offline immediately if the server that it is housed on fails. All other virtual computers on that particular server will also go offline immediately.
10. **D.** The beauty of a virtualized browser is that regardless of whether a virus or other malware damages it, the underlying operating system will remain unharmed. The virtual browser can be deleted and a new one can be created; or if the old virtual browser was backed up previous to the malware attack, it can be restored. This concept applies to entire virtual operating systems as well, if configured properly.
11. **D.** The System State needs to be backed up on a domain controller to recover the Active Directory database in the future. The System State includes user data and system files but does not include the entire operating system. If a server fails, the operating system would have to be reinstalled, and then the System State would need to be restored.
12. **C.** A patch can fix a single security issue on a computer. A service pack addresses many issues and rewrites many files on a computer; it may be overkill to use a service pack when only a patch is necessary. You might obtain the patch from a support website. A baseline can measure a server or a network and obtain averages of usage.
13. **C.** Often, operating system manufacturers such as Microsoft refer to the attack surface as all the services that run on the operating system. By conducting an analysis of which services are necessary and which are unnecessary, an administrator can find out which ones need to be disabled, thereby reducing the attack surface. Service packs, antivirus software, and network intrusion detection

systems (NIDSs) are good tools to use to secure an individual computer and the network but do not help to reduce the size of the attack surface of the operating system.

14. **A., B., and C.** After installing an operating system, it's important to install the latest service pack, patches, and a firewall. These three methods can help to secure the operating system. However, remote desktop support programs can actually make a computer less secure and should be installed only if the user requests that functionality.
15. **A.** Virtualization of computer servers enables a network administrator to isolate the various network services and roles that a server may play. Analyzing network traffic would have to do more with assessing risk and vulnerability and monitoring and auditing. Adding network services at lower costs deals more with budgeting than with virtualization, although, virtualization can be less expensive. Centralizing patch management has to do with hardening the operating systems on the network scale.
16. **C.** Patch management is an example of verifying any new changes in software on a test system (or live systems for that matter.) Verifying the changes (testing) is the second step of the standard patch management strategy. Application hardening might include updating systems, patching them, and so on, but to be accurate, this question is looking for that particular second step of patch management. Virtualization is the creating of logical OS images within a working operating system. HIDS stands for host-based intrusion detection system, which attempts to detect malicious activity on a computer.
17. **B. and D.** Updating the host-based intrusion prevention system is important. Without the latest signatures, the HIPS will not be at its best when it comes to protecting against malware. Also, disabling unused services will reduce the attack surface of the OS, which in turn makes it more difficult for attacks to access the system and run malicious code. Disabling the data leakage prevention device would not aid the situation, and it would probably cause data leakage from the computer. Installing a perimeter firewall won't block malicious software from entering the individual computer. A personal firewall would better reduce the attack surface of the computer, but it is still not meant as an anti-malware tool. Updating the NIDS signatures will help the entire network, but might not help the individual computer. In this question we want to focus in on the individual computer, not the network. In fact, given the scenario of the question, you do not even know if a network exists.
18. **A.** The best way to establish host-based security for your organization's workstations is to implement GPOs (Group Policy objects). When done properly from a server, this can harden the operating systems in your network, and you

can do it from a central location without having to configure each computer locally. It is the only answer that deals with the client operating systems. The other answers deal with database and web servers, and firewalls that protect the entire network.

19. **B.** Of the answers listed, the only one that will not show the version number is `wf.msc`. That brings up the Windows Firewall with Advanced Security. All of the other answers will display the version number in Windows.
20. **A.** If you migrate some of these low-resource servers to a virtual environment (a very smart thing to do), you could end up spending more on licensing, but less on hardware, due to the very nature of virtualization. In fact, the goal is to have the gains of hardware savings outweigh the losses of licensing. Load balancing and clustering deals with an OS utilizing the hardware of multiple servers. This will not be the case when you go virtual, nor would it have been the case anyway, because clustering and load balancing is used in environments where the server is very resource-intensive. Baseline, unfortunately, will remain the same; you should analyze all of your servers regularly, whether they are physical or virtual. These particular servers should not encounter latency or lowered throughput because they are low-resource servers in the first place. If, however, you considered placing into a virtual environment a Windows Server 2012 that supports 5,000 users, you should definitely expect latency.

Case Studies for Chapter 3

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

Case Study 3-1: Discerning and Updating the Service Pack Level

Scenario: You have been tasked with finding out the service pack level of a Windows 7 computer and updating it if necessary. You must also configure the Windows Update program in such a way that you will be notified of new updates but they will not be downloaded until you decide to do so, in keeping with your company's policies.

Usually an organization will choose to have the latest service packs installed for every Windows system, and the latest patches for other operating systems. It's important to be able to recognize whether a computer is up to date. Try and locate the service pack level for your version of Windows, and attempt to find out the version

numbers for any other computing devices you might possess. Enter your results in Table 3-3. Afterward, define how you would go about configuring Windows Update, and what option you would choose.

Table 3-3 Operating System and Version Responses

Operating System	Version
Example: Windows 7	Example: SP1 (version 6.1.7601)

Case Study 3-2: Securing a Virtual Machine

Scenario: Now that you have installed virtual machine software, and created a new VM, you are required to secure it. Your task is to disable unnecessary virtual hardware and secure the virtual BIOS.

Virtual machines that are contained within a Type 2 host are sort of like a computer within a computer. Consider writing down exactly what you are configuring. Try to do this in an illustrative nature. Or, consider using a network documentation program such as Visio. As you progress in the virtual world, you will be using more and more virtual computers, and will connect to them in a variety of remote ways. The more you document what it is that you are doing, the better you will understand your virtual environments.

Within your virtual software, disable the sound card, COM ports, LPT ports, and floppy disks (if any exist). This is done in the properties (or settings) of the virtual machine. Secure the BIOS by modifying the BIOS boot order, disabling unnecessary hardware, and setting an administrative (supervisor) password.

Case Study 3-3: Stopping Services in the Command-Line

Scenario: You have found that working in the GUI is good, but working in the command-line can be better. Besides, you almost always have a CLI (command-line interface) open, and you can type quickly, so it makes sense to use the CLI as often as possible. You know that unnecessary services can be vulnerabilities to your

systems, so you decide to reduce the size of the attack surface by stopping and disabling services—and do this from the CLI.

Demonstrate that you can stop services in the Windows Command Prompt (such as the Windows Firewall), as well as services in the Linux CLI (such as an Apache web server if installed). Specific commands and syntax will vary depending on the version of the operating system you are working in.

Case Study Solutions

Case Study 3-1 Solution

To find out the service pack level of Windows 7, navigate to Start, then right-click Computer and select Properties. This displays the System window and should show the Windows edition, as well as the service pack level. If no service pack is listed, then none is installed, and is known as service pack 0. Other versions of Windows use similar navigation to find out the service pack level. To update to the latest service pack for a given Windows operating system, go to <http://support.microsoft.com/> and search the relevant phrase, such as “Windows 7 SP1.” Latest service packs can be downloaded directly from the website. An organization might also use an optical disc to update individual computers or, if there are a lot of computers, stream the service pack update over the network.

Service packs are large groups of patches and updates. But they are static, meaning after one is released, it remains the same. So, additional updates are always necessary. By default this is taken care of by Windows Update. To modify the Windows Update settings, choose Start > All Programs > Windows Update. Then click the Change Settings link. Click the drop-down menu under Important Updates to select the correct setting. In this scenario it was “Check for updates but let me choose whether to download and install them.” This is a good solution for an individual computer, giving the user a good amount of control over what is installed. However, it probably wouldn’t be the best solution in an organization, and it is more likely that updates would be streamed across the network with a centralized solution such as SCCM.

Keep in mind that some computers will need to be updated beyond the service pack, *and* beyond what is automatically downloaded from Windows Update. Patches for specific problems are known as hotfixes. It is important to know how to acquire these hotfixes (also known as update rollups). They are usually found at the Microsoft Support website and are listed by Knowledge Base (KB) number. For example, one hotfix that repairs a memory leak in Windows 7 SP1 can be found at the following link: <http://support.microsoft.com/kb/2911106>.

It is article number 2911106 in the Microsoft Knowledge Base. It actually fixes a lot of documented issues, and can be an important fix for various Windows operating systems in addition to Windows 7 SP1. Over time, these hotfixes are gathered together in automatically downloaded Windows Update groups (if it is deemed necessary), and ultimately are added to newer service packs.

Video Solution: Watch the video solution “3-1: Discerning and Updating the Service Pack Level” on the accompanying disc for in-depth details of each step, plus content on Linux, OS X, Android, and iOS.

Case Study 3-2 Solution

Virtualization security is vital. VMs should be secured the same way that a regular operating system is secured. However, the VM itself (and the virtual hosting software) can be further secured by disabling virtual hardware, both within the virtual machine settings and within the virtual machine BIOS.

This solution utilizes a Windows 7 hosting computer and assumes that you have already downloaded and installed Microsoft Virtual PC 2007, created a virtual machine, and installed an OS. Basic steps follow below. Be sure to watch the accompanying video solution as well.

- Step 1.** Check the Microsoft Virtual PC 2007 software SP level from Control Panel > Programs > Programs and Features. If necessary, upgrade to the latest SP from the following link:
www.microsoft.com/download/en/details.aspx?displaylang=en&id=24439
- Step 2.** Set security options in the Virtual PC console from File > Options > Security.
- Step 3.** Disable unnecessary hardware within the Virtual PC console for the VM in question. For example, the sound card, COM ports, LPT ports, and floppy disks.
- Step 4.** Start the virtual machine and secure the virtual BIOS. Modify the BIOS boot order, disable unnecessary devices, and configure an administrative password.
- Step 5.** Start the virtual machine and check the SP level of the virtual OS.
- Step 6.** Disable unnecessary hardware in the Device Manager of the VM.
- Step 7.** Remove any network sharing connections between the VM and the physical host.

Step 8. (Optional) Exit the VM and secure the folder on the host OS that contains the VM files.

Video Solution: Watch the video solution “3-2: Securing a Virtual Machine” on the accompanying disc for in-depth details of each step.

Case Study 3-3 Solution

Stopping services is an extremely important skill for a security administrator (not to mention for the Security+ exam). As an IT person, you should feel at home in the command-line. Running commands, scripting, and testing network connections are all part of a day’s work in the computer world. From a security standpoint, some things that cannot be accomplished in the GUI *can* be performed in the command-line.

To stop a service such as the Windows Firewall in Windows, use the following syntax:

```
net stop mpssvc
```

or

```
sc stop mpssvc
```

To stop a service in Linux (for example, stopping the udevmonitor service in Ubuntu), use the following syntax:

```
sudo stop udevmonitor
```

Be prepared to enter the administrator password because you have invoked the `sudo` option.

Video Solution: Watch the video solution “3-3: Working with Services in Windows and Linux” on the accompanying disc. This goes into a bit more depth, showing a few more commands, and deals with processes as well.

Simulation: Complete the simulation “3-3: Stopping Services in the Command-Line.”



This chapter covers the following subjects:

- **Securing the Browser:** What is a computer without a web browser? Some might answer “worthless.” Well, a compromised browser is worse than no browser at all. The web browser must be secured to have a productive and enjoyable web experience. In this section, we concentrate on Internet Explorer and Firefox, and show various ways to secure them.
- **Securing Other Applications:** Organizations use many applications, and they each have their own group of security vulnerabilities. In this section, we spend a little time on common applications such as Microsoft Office and demonstrate how to make those applications safe.
- **Secure Programming:** Programmers use many techniques when validating and verifying the security of their code. This section covers a few basic concepts of programming security such as system testing, secure code review, and fuzzing.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 3.5, 4.1, and 4.3.

Application Security

Browser security should be at the top of any security administrator's list. It's another example of inherently insecure software "out of the box." Browsers are becoming more secure as time goes on, but malware and especially adware are presenting more of a challenge—as mentioned in Chapter 1, "Introduction to Security," the scales are always tipping back and forth.

Most browsers have plenty of built-in options that you can enable to make them more secure, and third-party programs can help in this endeavor as well. This chapter focuses mostly on Internet Explorer and Firefox, but the concepts we cover can be applied to most other browsers. However, users don't just work with web browsers. They use office applications frequently as well, so these should be secured, too. Also, other applications, such as the command-line, though a great tool, can also be a target. Back office applications such as the ones that supply database information and e-mail are also vulnerable and should be hardened accordingly. And finally, any applications that are being developed within your domain should be reviewed carefully for bugs.

Be sure to secure any application used or developed on your network. It takes only one vulnerable application to compromise the security of your network.

Let's start with discussing how to secure web browsers.

Foundation Topics

Securing the Browser

There is a great debate as to which web browser to use. The two front runners in the business world are Internet Explorer and Firefox, though Chrome has gained a lot of popularity over recent years. Personally, it doesn't matter too much to me, because as a security guy, I am going to spend a decent amount of time securing either one. However, each does have advantages, and one might work better than the other depending on the environment. So if you are also in charge of implementing a browser solution, be sure to plan for performance *and*

security right from the start. As to planning for and configuring security, I do make some standard recommendations to customers, students, and readers. Let's discuss a few of those now.

The first recommendation is to *not* use the very latest version of a browser. (Same advice I always give for any application, it seems.) Let the people at the top of the marketing pyramid, the innovators, mess around with the “latest and greatest;” let those people find out about the issues, backdoors, and whatever other problems a new application might have; at worst, let their computer crash! For the average user, and especially for a fast-paced organization, the browser needs to be rock-solid; these organizations will not tolerate any downtime. I always allow for some time to pass before fully embracing and recommending software. (My lead time for new software is between 6 and 12 months depending on what it is.) The reason I bring this up is because most companies share the same view and implement this line of thinking as a company policy. They don't want to be caught in a situation where they spent a lot of time and money installing something that is not compatible with their systems.

The next recommendation is to consider what type of computer, or computers, will be running the browser. Generally, Linux computers run Firefox or another browser besides Internet Explorer (IE); however, you can run a type of IE on Linux, but WINE must be installed first. IE is common in the Windows market, but Firefox and Chrome work well on Windows computers, too. Some applications such as Microsoft Office are, by default, linked to IE, so it is wise to consider other applications that are in use when deciding on a browser. Another important point is whether you will be centrally managing multiple client computers' browsers. IE can be centrally managed through the use of Group Policy objects (GPOs) on a domain; I'll show a quick demonstration of this later in the chapter.

You might also want to consider how the browser companies fix vulnerabilities. If a vulnerability is found in Firefox, it generally becomes common knowledge quickly, which could lead to rapid exploits of the vulnerability before the folks at Mozilla have a chance to fix it. However, an advantage of Firefox is that vulnerabilities appear to be fixed faster than IE vulnerabilities the majority of the time. On the flip side, Microsoft will find out about vulnerabilities but will *attempt* to keep them secret, which pretty much eliminates any possible exploits born from company-presented information. But...Microsoft might take longer to fix the vulnerability. It should be noted that some sites do not allow connections by any browser except IE. This is a “security feature” of those websites and should be investigated before implementing other browsers in your organization. If your company makes connections to those types of sites, no other browser will be appropriate. Conversely, some sites do not fare well when using IE, and are accessed more efficiently with another browser. As far as security in general, IE received a poor reputation during

older versions. However, Microsoft has worked on this in recent years, resulting in a much more secure application. Firefox has been known all along for its security, but it would seem that the two are evenly matched at this point. If you were to research the total number of discovered vulnerabilities for each browser, it would probably be close to the same number.

When it comes to functionality, both browsers work very well, but one browser might work better for the specific purposes of an individual. By combining the functionality a user requires in a browser, along with the security needed, you should come up with the right choice. Anyway, I think that's enough yappin' about the two for now—we'll cover some specific security techniques for each in just a little bit.

General Browser Security Procedures

First, some general procedures should be implemented regardless of the browser your organization uses. These concepts can be applied to desktop browsers as well as mobile browsers.

- Implement policies.
- Train your users.
- Use a proxy and content filter.
- Secure against malicious code.

Each of these is discussed in more detail in the following sections.

Implement Policies

The policy could be hand-written, configured at the browser, implemented within the computer operating system, or better yet, configured on a server centrally. Policies can be configured to manage add-ons, and disallow access to websites known to be malicious, have Flash content, or use a lot of bandwidth. As an example, Figure 4-1 displays Internet Explorer Security Features within the Local Group Policy of a Windows 7 computer. You can access it by opening the computer's Local Computer Policy (in the figure it was added as a snap-in to an MMC) and navigating to

User Configuration > Administrative Templates > Windows Components > Internet Explorer > Security Features

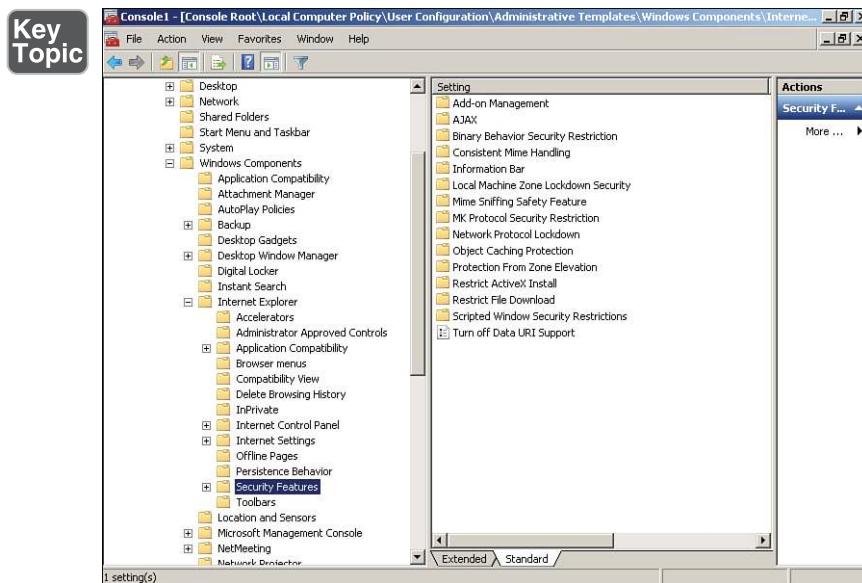


Figure 4-1 Internet Explorer Security Features in the Local Computer Policy

Of course, literally hundreds of settings can be changed for Internet Explorer. You can also modify Internet Explorer Maintenance Security by navigating to

User Configuration > Windows Settings > Internet Explorer Maintenance > Security

This is shown in Figure 4-2. The Security Zones and Content Ratings object was double-clicked to show the dialog box of the same name, which allows you to customize the Internet security zones of the browser. Some versions of Windows will not enable you to access the Local Computer Policy; however, most security features can be configured directly within the browser in the case that you don't have access to those features in the OS.

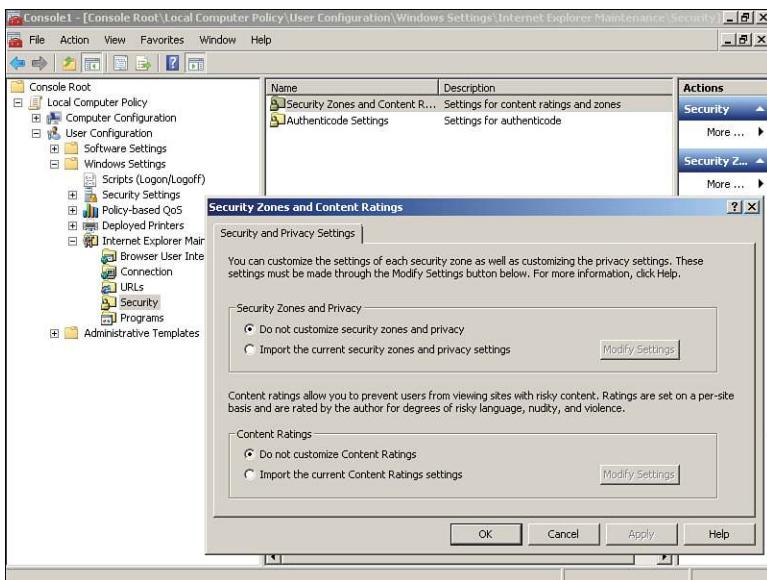


Figure 4-2 Internet Explorer Maintenance Security in the Local Computer Policy

Now, you wouldn't want to configure these policy settings on many more than a few computers individually. If you have multiple computers that need their IE security policies updated, consider using a template (described in Chapter 3, "OS Hardening and Virtualization"), or if you have a domain controller, consider making the changes from that central location. From there, much more in-depth security can be configured and deployed to the IE browsers within multiple computers. An example of the IE policies, as managed from a domain controller, is shown in Figure 4-3. For this, I set up a Windows Server 2008 as a domain controller (controlling the domain dpro3.com), created an organizational unit (OU) named Marketing, and then created a Group Policy object named Marketing-Policy that I added to the MMC. From that policy the Internet Explorer settings, which can affect all computers within the Marketing OU, can be accessed by navigating to

Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer.

From here we can configure trusted and non-trusted sites, zones, and advanced security features in one shot for all the computers in the OU. A real time-saver!

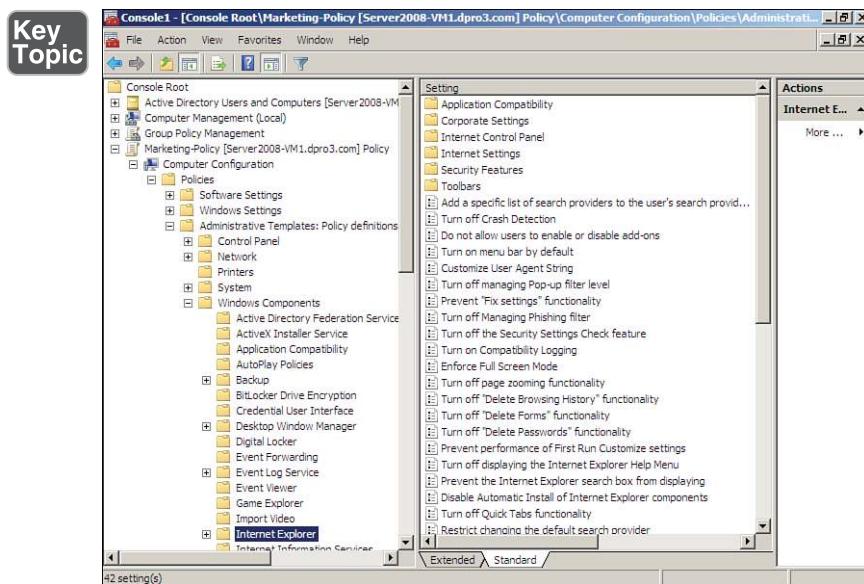


Figure 4-3 Internet Explorer Policies in the Marketing-Policy GPO

NOTE You can also perform these and other similar tasks mentioned in this chapter within newer Windows Server products such as Windows Server 2012 R2 using the Group Policy Management Console (GPMC).

Train Your Users

User training is important to determine which websites to access, how to use search engines, and what to do if pop-ups appear on the screen. The more users you can reach with your wisdom, the better! Onsite training classes, webinars, and downloadable screencasts all work great. Or if your organization doesn't have those kinds of resources, consider writing a web article to this effect—make it engaging and interesting, yet educational.

For example, explain to users the value of pressing Alt+F4 to close pop-up windows instead of clicking No or an X. Pop-ups could be coded in such a way that No actually means Yes, and the close-out X actually means “take me to more annoying websites!” Alt+F4 is a hard-coded shortcut key that closes applications.

Another example is to show users how to determine if their communications are secure on the web. Just typing HTTPS in the address bar isn't enough. A browser might show a green background in the address bar if the website uses a proper

encryption certificate. Some browsers use a padlock in the locked position to show it is secure. One website that shows these security notifications in action is `https://www.paypal.com`, but most (if not all) banking sites incorporate security certificates that tell the browser to show the security notifications as well. To find out the specific security employed by the website to protect the session, click the padlock icon and select More Information or Connection, or something to that effect (depending on the browser). This will show the encryption type and certificate being used. We'll talk more about these concepts in Chapter 13, "Encryption and Hashing Concepts," and Chapter 14, "PKI and Encryption Protocols."

Use a Proxy and Content Filter

HTTP proxies (known as proxy servers) act as a go-between for the clients on the network and the Internet. Simply stated, they cache website information for the clients, reducing the amount of requests that need to be forwarded to the actual corresponding web server on the Internet. This is done to save time, make more efficient use of bandwidth, and help to secure the client connections. By using a content filter in combination with this, specific websites can be filtered out, especially ones that can potentially be malicious, or ones that can be a waste of man-hours, such as P2P websites/servers. I know—I'm such a buzzkill. But these filtering devices are common in today's networks; we talk more about them in Chapter 7, "Network Perimeter Security." For now, it is important to know how to connect to them with a browser. We use Internet Explorer as an example. Remember that the proxy server is a mediator between the client and the Internet. So the client's web browser must be configured to connect to them. You can either have the browser automatically detect a proxy server or (and this is more common) configure it statically. Here's how:

- Step 1.** Open Internet Explorer. (I'm using IE 11, but other versions of IE will be similar in navigation, and in the look of the screenshots shown in the figures.)
- Step 2.** On the menu bar go to Tools. If the menu bar is not visible, press `Alt+T` on the keyboard to bring up the menu.
- Step 3.** Select Internet Options. This should display the Internet Options dialog box.
- Step 4.** Click the Connections tab.
- Step 5.** Click the LAN Settings button. This displays the Local Area Network (LAN) Settings window, as shown in Figure 4-4.

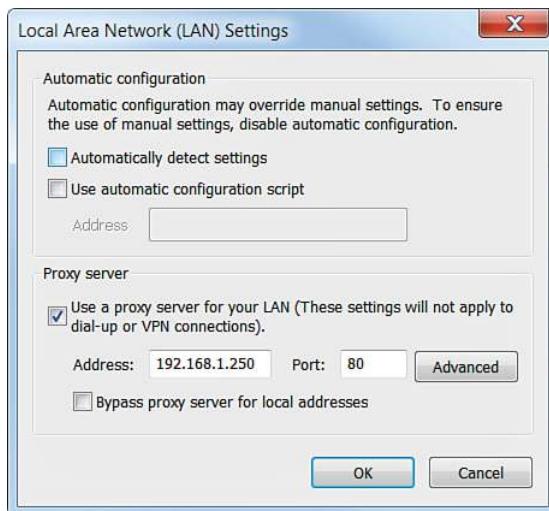


Figure 4-4 Configuring the Proxy Server Connection in Internet Explorer

- Step 6.** Check the Use a Proxy Server for Your LAN checkbox. This enables the fields in the Proxy Server area.
- Step 7.** In the Address field, type in the IP address or name of the proxy server, for example 192.168.1.250.
- Step 8.** Select a port; by default 80 is selected because it corresponds with HTTP and most web requests. However, your proxy might use a different port. Consult your network documentation for details.
- Step 9.** If your proxy server also acts as a go-between for other services such as FTP or secure web transactions, configure these by clicking the Advanced button.
- Step 10.** Click OK for the Local Area Network (LAN) Settings dialog box.
- Step 11.** Click OK for the Internet Options dialog box. The client should now be configured to use a proxy server for all its HTTP transactions. To remove the proxy server at any time, simply deselect the Use a Proxy Server for Your LAN checkbox.

NOTE This setting can also be configured within an organizational unit's Group Policy object on the domain controller. This way, it can be configured one time but affect all the computers within the particular OU.

Of course, any fancy networking configuration such as this can be used for evil purposes as well. The malicious individual can utilize various malware to write their own proxy configuration to the client operating system, thereby redirecting the unsuspecting user to potentially malevolent websites. So as a security administrator you should know how to enable a legitimate proxy connection used by your organization, but also know how to disable an illegitimate proxy connection used by attackers.

Secure Against Malicious Code

Depending on your company's policies and procedures, you might need to configure a higher level of security concerning ActiveX controls, Java, JavaScript, Flash media, phishing, and much more. We show a few of these configurations in the subsequent sections.

Securing Internet Explorer

There are many ways to make Internet Explorer more secure. Be warned, though, that the more a browser is secured, the less functional it becomes. Generally, the best solution is to find a happy medium between functionality and security.

The first thing that you should do is to update the browser. Internet Explorer can be updated directly through the Windows Update feature; however, watch for completely new versions as well (which can also be downloaded from Microsoft's website). Whenever updating, always check the list of updates before installing them.

Next, install pop-up blocking and other ad-blocking solutions. Many antivirus suites have pop-up blocking tools. There is also the Google Toolbar and other tools like it. And of course, newer versions of web browsers will block some pop-ups on their own.

Now we move on to configuring security within the browser itself. By adjusting Internet Explorer settings, you can add a layer of defense that helps to prevent spyware and other malicious attacks.

First we configure security zones. This and many other security configurations can be completed in the Internet Options dialog box, which can be accessed by going to Tools on the menu bar and selecting Internet Options. Then click the Security tab to show the Internet Explorer security zones. Remember, just because they are called security zones doesn't necessarily make them secure. Adjust the security level for the zone named Internet. Many organizations set this to High, as shown in Figure 4-5.

Key Topic

Figure 4-5 Internet Options Dialog Box—Security Zones

You can set the security level in the same manner for the Local Intranet zone, Trusted Sites zone, and Restricted Sites zone. In addition, you can set custom levels by clicking the Custom Level button. Here you can disable ActiveX controls and plug-ins, turn the scripting of Java applets on and off, and much more. The Security tab is also where you can add trusted sites to the computer. For example, if you have a high security level, and IE always asks whether a particular website is okay to visit, and it's a site you visit every day and know to be legitimate, you can add it to the trusted sites by clicking the Trusted Sites zone, clicking the Sites button, and adding the URL of the site in question. Conversely, you can restrict sites by clicking the Restricted Sites zone and again clicking the Sites button.

Cookies can also pose a security threat. The next tab in the Internet Options window is the Privacy tab. This is where you can select how cookies will be handled.

Cookies are text files placed on the client computer that store information about it, which could include your computer's browsing habits and possibly user credentials. The latter are sometimes referred to as *persistent* cookies, used so that a person doesn't have to log in to a website every time. By adjusting the slider, you can either accept all cookies, deny all cookies, or select one of several options in between. Figure 4-6 displays this slider set to High, which blocks cookies that save information that can be used to contact the user and cookies that do not have a privacy policy.

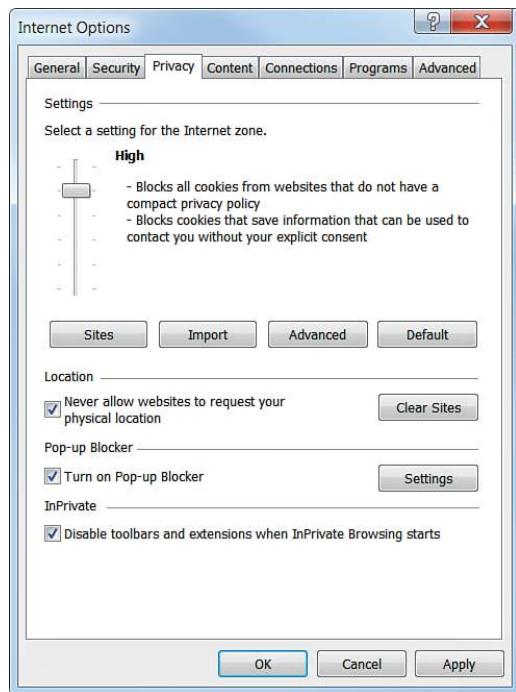
Key Topic

Figure 4-6 Internet Options Dialog Box—Privacy Tab

NOTE You will see that the Never Allow Websites to Request Your Physical Location checkbox is also checked. This is another smart security precaution.

You can also override any automatic cookie handling that might occur by clicking the Advanced button (this displays the Advanced Privacy Settings dialog box), checking the box, and selecting Prompt (for example). This way, a user will be prompted when a website attempts to create a cookie. With this setting in place, IE displays a window similar to Figure 4-7. In this example, my website www.davidlprowse.com was accessed. My site automatically tried to create a cookie due to the bulletin board system code. IE sees this, stops it before it occurs, and verifies with the user whether to accept it. This particular cookie is harmless, so in this case I would accept it. There is a learning curve for users when it comes to knowing which cookies to accept. I guarantee that once or twice they will block a cookie that subsequently blocks functionality of the website. In some cases, an organization deals with too many websites that have too many cookies, so this particular security configuration is not an option.



Figure 4-7 IE Cookie Privacy Alert

Tracking cookies are used by spyware to collect information about a web user's activities. Cookies can also be the target for various attacks; namely, session cookies are used when an attacker attempts to hijack a session. There are several types of session hijacking. One common type is cross-site scripting (also known as XSS), which is when the attacker manipulates a client computer into executing code considered trusted as if it came from the server the client was connected to. In this way, the hacker can acquire the client computer's session cookie (allowing them to steal sensitive information) or exploit the computer in other ways. We cover more about XSS later in this chapter, and more about session hijacking in Chapter 6, "Networking Protocols and Threats."

Another concept similar to cookies is **locally shared objects (LSOs)**, also called Flash cookies. These are data that Adobe Flash-based websites store on users' computers, especially for Flash games. The privacy concern is that LSOs are used by a variety of websites to collect information about users' browsing habits. However, LSOs can be disabled via the Local Settings Manager (in most of today's operating systems) or, for older operating systems, via the Online Settings Manager at Adobe's website. LSOs can also be deleted entirely with third-party software, or by accessing the user's profile folder in Windows. For example, in Windows 7, the path would be similar to the following:

```
C:\Users\[Your Profile]\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\[variable folder name]
```

Pop-ups are the bane of any web surfer. There is a pop-up blocker in the Privacy tab of Internet Explorer; this is on by default but is worth checking if a user is getting a lot of pop-ups.

The Content tab allows for parental controls and a content advisor, both of which can help secure the browser. This tab is also where you can find encryption certificates. You can find more information on certificates in Chapter 14.

The Connections tab enables a user to make secure connections through a VPN and also connect to the Internet via a proxy server as mentioned earlier. You can find more information on VPNs in Chapter 9, “Physical Security and Authentication Models.”

The Advanced tab has more than a dozen security settings that you can find by scrolling toward the bottom of the Settings box. For example, a hotel that offers Internet access as a service for guests might check mark the Empty Temporary Internet Files folder option. This way, the histories of users are erased when they close the browser. On a related note, salespeople, field technicians, and other remote users should be trained to delete temporary files and cookies when they are using computers on the road. From here, you can also configure whether to check if TLS/SSL certificates have been revoked. You can also check if the proper version of TLS or SSL is used. At the time of this book’s publishing, it is wise to have SSL 3.0 selected and SSL 2.0 deselected. Some organizations also disable third-party browser extensions from this tab in the Browsing section.

You can enable and disable add-on programs in the Programs tab by clicking the Manage Add-ons button. (This can also be accessed directly within the Tools menu.) IE always asks before installing add-ons, but over time a company might decide that certain add-ons (that were already installed) could be vulnerabilities. For example, in Figure 4-8, the Shockwave Flash Object ActiveX control is selected on a computer running IE 11. There are scenarios where this control could cause IE to close or perhaps cause the system to crash; it can be turned off by clicking Disable toward the bottom of the window (older versions of IE show a radio button for this). Many add-ons are ActiveX controls, and ActiveX could also be turned off altogether as mentioned previously. Depending on the add-on and the situation, other ways to fix the problem include updating Flash and upgrading IE.

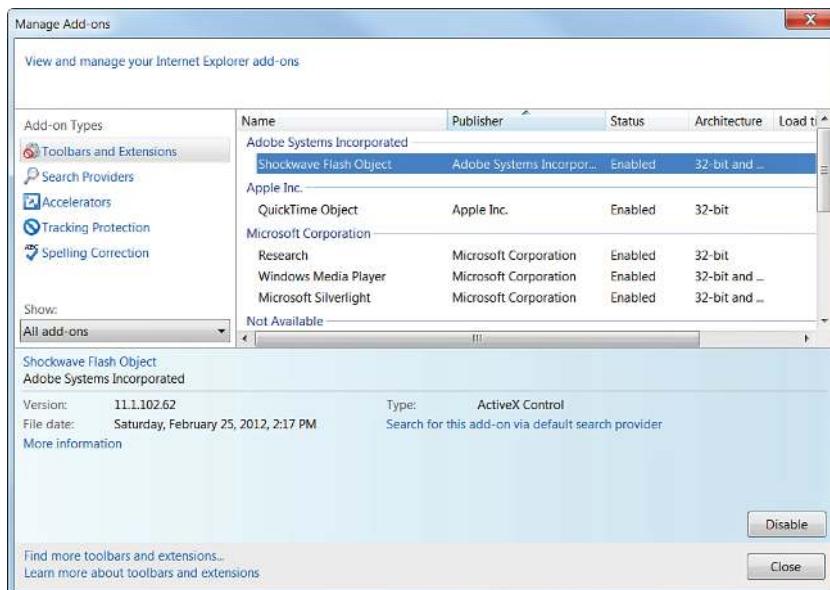


Figure 4-8 Managing Add-ons

ActiveX controls are small program building blocks used to allow a web browser to execute a program. They are similar to Java applets; however, Java applets can run on any platform, whereas ActiveX can run only on Internet Explorer (and Windows operating systems). You can see how a downloadable, executable ActiveX control or Java applet from a suspect website could possibly contain viruses, spyware, or worse. These are known as *malicious add-ons*—Flash scripts especially can be a security threat. Generally, you can disable undesirable scripts on either the Advanced tab or the Custom level of the Security tab. If a particular script technology cannot be disabled within the browser, consider using a content filtering solution.

Of course, this section has only scraped the surface, but it gives you an idea of some of the ways to secure Internet Explorer. Remember to implement Group Policies from a server (domain controller) to adjust the security settings of IE for many computers across the network. It saves time and is therefore more efficient.

In Chapter 3 we mentioned that removing applications that aren't used is important. But removing web browsers can be difficult, if not downright impossible, and should be avoided. Web browsers become one with the operating system, especially so in the case of IE and Windows.

If a computer has multiple browsers, and your organization decides to use Internet Explorer as the *default* browser, you can make this so by going to the Programs tab and selecting the Make Default button. But even if a computer uses Firefox in lieu of IE, it isn't practical to attempt the removal of IE. The same goes for the converse.

Securing Firefox

If an organization decides to use Firefox instead of IE, Firefox can be set as the default by opening the browser, navigating to the Tools menu, clicking Options, clicking Advanced, and on the General tab clicking the Make Firefox the Default Browser button. (FYI, version 27 is shown in the figures.) You can also check mark the Always Check to See If Firefox Is the Default Browser on Startup checkbox, as shown in Figure 4-9, just in case another browser has become the default for some strange reason. Other browsers on the computer might not be up to date, and therefore could be vulnerable. By setting one browser as the default over the other, you can avoid problems associated with users clicking links within applications such as e-mail, possibly opening the wrong browser automatically.

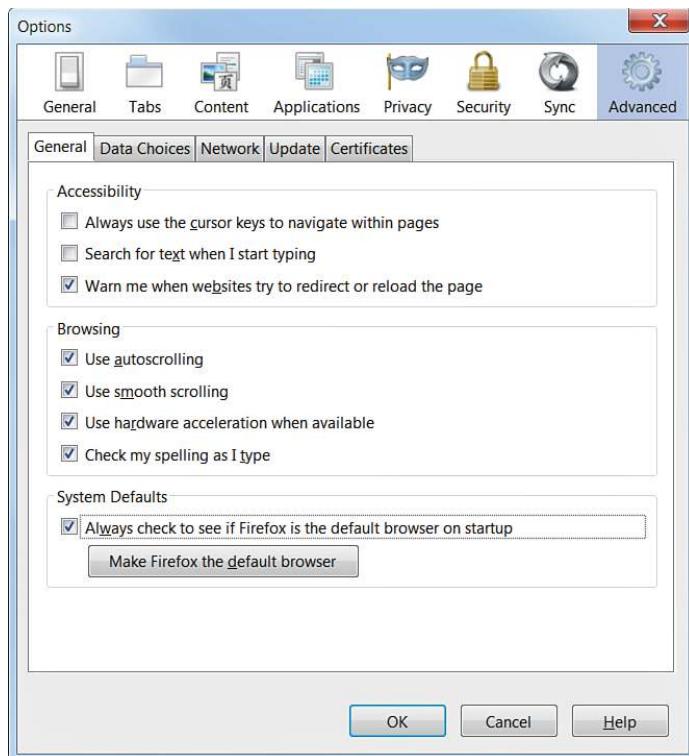


Figure 4-9 Firefox General Tab of the Advanced Options

One excellent way to protect the user session is to check mark the Warn Me When Websites Try to Redirect or Reload the Page option. Redirects can often have negative results; this puts the user in more control when visiting unknown websites.

This Options dialog box is where all the important security configurations appear. Many of the security features we mentioned in the Internet Explorer section can be enabled in Firefox as well, but the navigation to them will be slightly different. Firefox does not offer security zones in the way that IE does, nor does it offer features that enable the management of ActiveX controls.

Cookies can be configured by clicking the Privacy option at the top of the Options dialog box, as shown in Figure 4-10, and selecting Use Custom Settings for History from the drop-down menu. Exceptions can be configured as to which sites' cookies will be allowed. You can also view the list of cookies currently stored on the computer. Allowed cookies are also known as whitelists. By default, third-party cookies are “always” accepted. But, your organization might have a policy stating that third-party cookies are never allowed. Or perhaps it has a policy indicating that Firefox’s history needs to be cleared when the browser closes. These types of policies can help to secure the system from unwanted cookies.

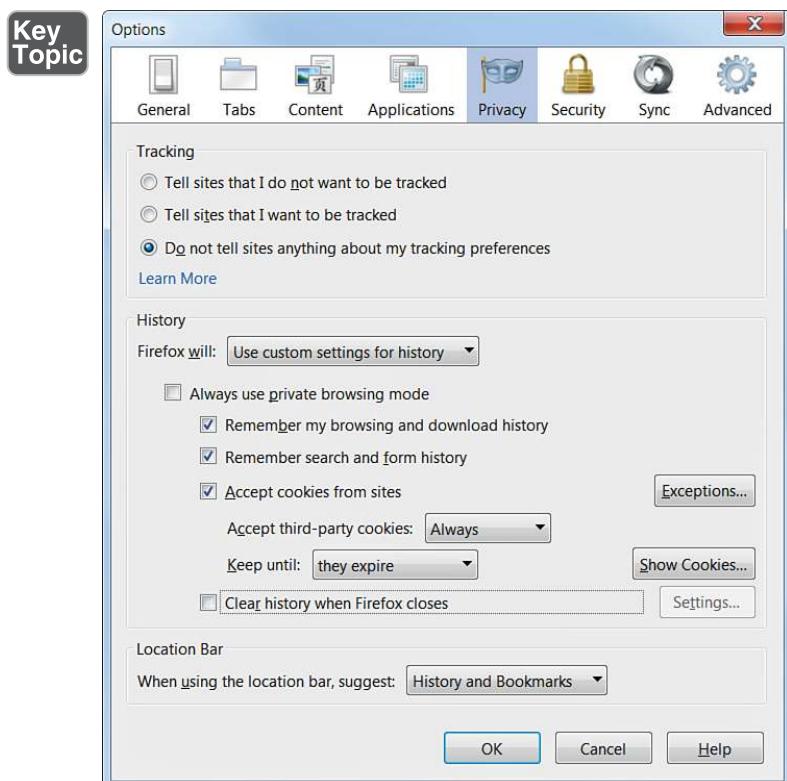


Figure 4-10 Firefox Privacy Options

The Security option houses configurations such as add-on warnings, password remembrance, and other warning messages, as shown in Figure 4-11. Some organizations make it a policy to disable the Remember Passwords for Sites checkbox. If you do save passwords, it would be wise to enter a master password. This way, when saved passwords are necessary, Firefox will ask for only the master password, and you don't have to type or remember all the others. A password quality meter tells you how strong the password is. Personally, I don't recommend allowing any web browser to store passwords. Period. But, your organization's policies may differ in this respect.

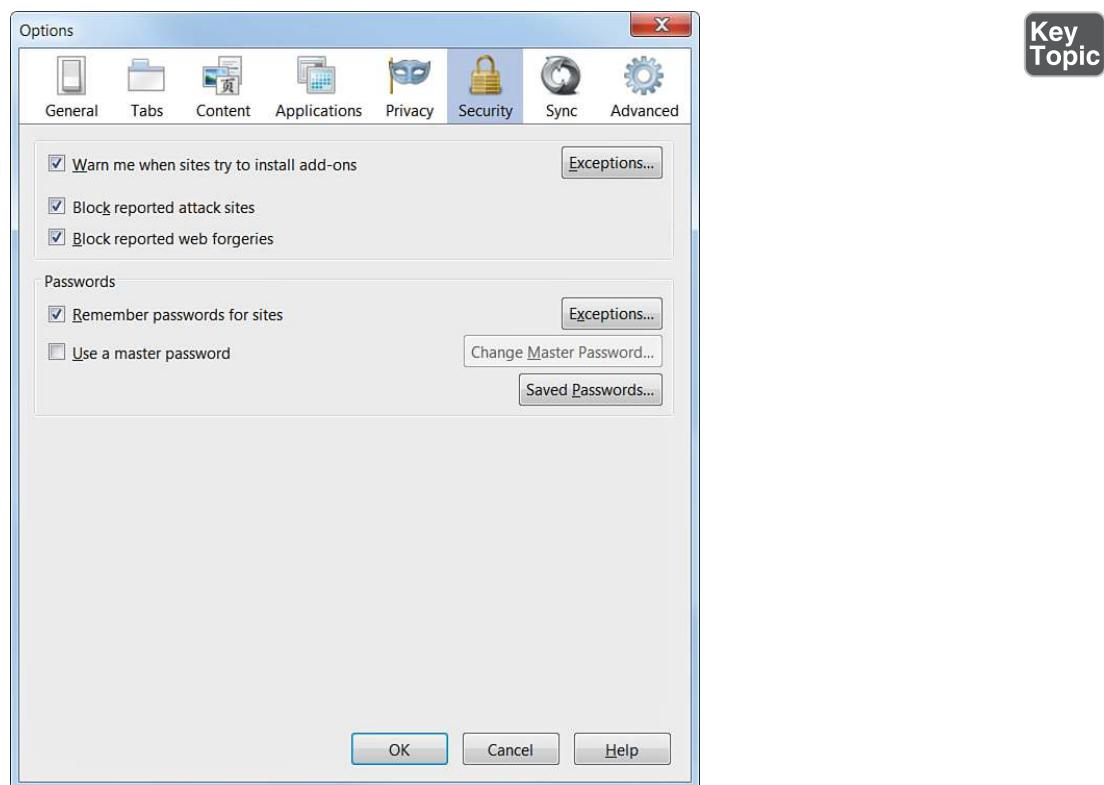


Figure 4-11 Firefox Security Options

The Advanced option has several tabs where various portions of Firefox can be configured. These include the Certificates tab, which allows you to view any certificates that the browser received in the past from websites that were visited, and import new certificates if necessary. Also, the Network tab offers the capability to connect to the Internet via a proxy server. This can be done by following these steps:

- Step 1.** Click the Settings button. This displays the Connection Settings dialog box.
- Step 2.** Proxies can be auto-detected, but to continue setting up one manually, click the Manual Proxy Configuration radio button.
- Step 3.** Type in the IP address or name of the proxy server, followed by the inbound port it uses.

The resulting configuration would look something similar to Figure 4-12. This figure shows a configured HTTP proxy. You can also enable automatic proxy configurations if your proxy server allows for that. A specific URL would be needed that points to the appropriate server and configuration script.

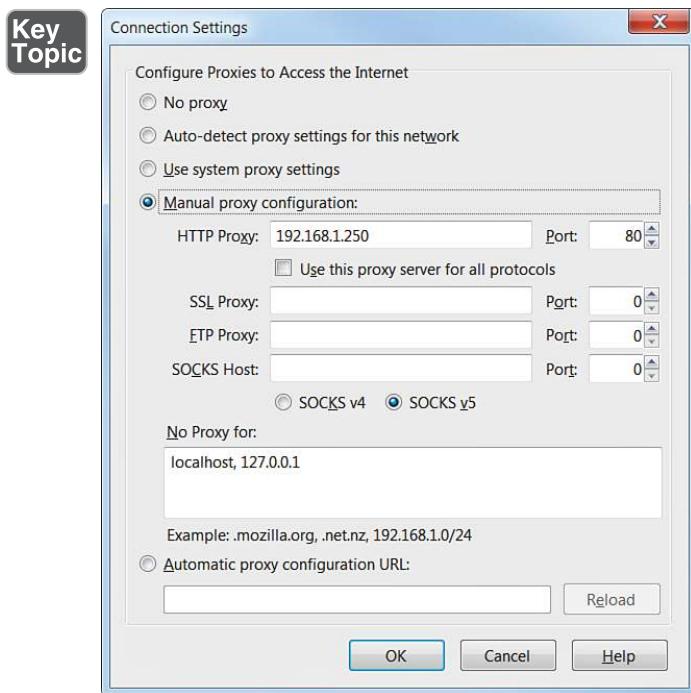


Figure 4-12 Firefox Proxy Connection

Another way to secure Firefox is to use third-party pop-up blocking software such as Adblock Plus. This is an extension to Firefox, or add-on, so the use of add-ons needs to be enabled. However, programs like this one will automatically update as new types of advertisement pop-ups are released.

Firefox has an entire site dedicated to browser add-ons at the following link:
<https://addons.mozilla.org/en-US/firefox/>

One example of a smart add-on is NoScript. You can install this security suite add-on to protect against possible malicious JavaScript, Flash, and XSS code. This helps to ward off hijacking, click-jacking, and cross-site scripting (XSS) attempts. Check out the site to find more smart add-ons that help to make Firefox more secure and efficient. There are add-ons to get a handhold on the amount of Google ads you encounter, anti-phishing tools, and lots more.

Securing Other Browsers

The Chrome browser has made a huge leap in popularity over the past several years. Chrome is an interesting browser—whereas some settings are independent of any other software on the computer, others piggyback IE in Windows. Let's explain that in a little more detail.

First of all, to find any security settings in Chrome, you have to access the Settings section (often found by clicking a button in the upper-right corner of the application). Then click Show Advanced Settings at the bottom of the screen. That expands the Settings to show a host of privacy settings, such as the ability to change the content settings (turn off JavaScript, block third-party cookies, and so on), disallow tracking when browsing the web, or send usage statistics to Google. Most organizations want to max out the security settings when using Chrome, because they want to limit threats and reduce the amount of information that is gathered by third parties. All of these settings so far are independent of IE. But in the Network section, there is the option to configure a proxy connection—this does piggyback IE. In this case, what is configured in IE is also configured in Chrome (by default). There are other similar examples as well. The key here is to realize that even if Chrome is updated, there could still be vulnerabilities due to IE not being updated. This applies even if IE is not regularly used. So if you use Chrome on a Windows computer, make sure you secure it, but also make sure that IE is updated and secured as well.

There is also Apple's Safari browser, which comes in a distant fourth in browser market share. However, if you are a Mac user, Safari is most likely the browser you use. So it is quite important for all of the audio/video editors, graphics design people, photographers, publishers of all sorts, and so on. In days gone by it was said that Mac computers didn't get malware. That of course was a generalization. *Any system can be affected by malware.* It's just that it didn't happen that often to Mac computers, and it did happen very often to Windows-based computers. But now, it seems that all operating systems are under siege. (Microsoft and Android are the front-runners, but no system is safe.) OS X can be the victim of viruses, ransomware, and lots of other malware. So it makes sense that Safari has a security section, which can be accessed by going to Safari > Preferences and clicking the Security option. By default, plug-ins are allowed, and JavaScript is enabled. Disabling these two items is one way to help secure the browser. In fact, it is recommended that

Java (for example, the JRE client) be removed from the system altogether. Cookie security can be increased from the Privacy option, and proxy configurations can be made from the Advanced option.

NOTE Always be ready to check the proxy configuration in case some kind of malware installed a proxy without the user's knowledge. This can ultimately be used to redirect the user to unwanted and potentially harmful websites.

When Mac users browse the web, a smart policy is to limit the users to downloading apps from the App Store only. And of course, patching the system and running AV software are also suggested.

There are also browsers such as Opera, and other up-and-coming browsers. But these can all benefit from the same basic methods that were detailed in the IE and Firefox sections.

When it comes to mobile browsers, Apple's Safari is king with an installed base of over half of the mobile devices in existence (as of the writing of this book). It can be secured in much the same manner as its desktop counterpart. The Android browser, a firm second in the marketplace, can take advantage of most of the techniques mentioned earlier in the chapter. One option that is slightly different is the ability to enable or disable the Flash *player*. But the bulk of the security settings are located from within the browser by going to Menu > Settings > Privacy and Security. From there you can enable/disable cookies, enable/disable location access, and change how website passwords are stored (if at all). There are other mobile browsers too—Opera Mini, Chrome, BlackBerry, IE for mobile devices, and so on. But the basic principles in this chapter hold true for all of them.

NOTE Another way to keep the browser secure, as well as the entire system, is to avoid jailbreaking or rooting the device. If the device has been misconfigured in this way, it is easier for attackers to assault the web browser and, ultimately, subjugate the system.

Keep in mind that the technology world is changing quickly, especially when it comes to the Internet, browsing, web browsers, and attacks. Be sure to periodically review your security policies for web browsing and keep up to date with the latest browser functionality, updates, security settings, and malicious attacks.

One last comment on browsers: sometimes a higher level of security can cause a browser to fail to connect to some websites. If a user cannot connect to a site, consider checking the various security settings such as trusted sites, cookies, and so on. If necessary, reduce the security level temporarily so that the user can access the site.

Securing Other Applications

Typical users shouldn't have access to any applications other than the ones they specifically need. For instance, would you want a typical user to have full control over the Command Prompt or PowerShell in Windows? Doubtful—and protective measures should be put into place to make sure the typical user does not have access.

One way to do this is to use **User Account Control (UAC)** on qualifying Windows operating systems. UAC is a security component of Windows Vista and newer, and Windows Server 2008 and newer. It keeps every user (besides the actual Administrator account) in standard user mode instead of as an administrator with full administrative rights—even if they are a member of the administrators group. It is meant to prevent unauthorized access and avoid user error in the form of accidental changes. A user attempting to execute commands in the Command Prompt will be blocked and will be asked for credentials before continuing. This applies to other applications within Windows.

Another way to deny access to applications is to create a policy. For example, on a Windows Server, you can do this in two ways. The first way is to disallow access to specific applications; this policy is called Don't Run Specified Windows Applications (a form of application blacklisting). However, the list could be longer than Florida, so another possibility would be to configure the Run Only Specified Windows Applications policy (a form of application whitelisting), as shown in Figure 4-13. This and the previously mentioned policy are adjacent to each other and can be found at the following path in Windows Server:

Policy (in this case we use the Marketing-Policy again) > User Configuration > Policies > Administrative Templates > System

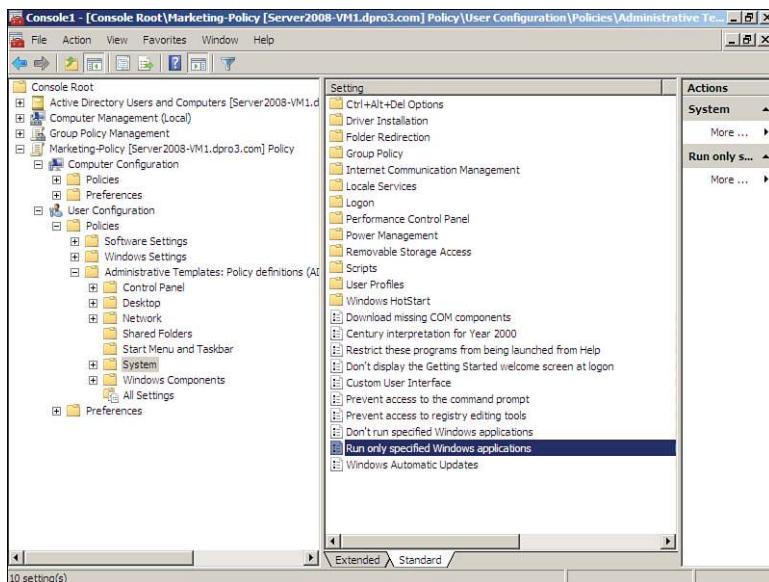


Figure 4-13 Run Only Specified Windows Applications Policy

When double-clicked, the policy opens and you can enable it and specify one or more applications that are allowed. All other applications will be denied to the user (if the user is logged on to the domain and is a member of the Marketing OU to which the policy is applied). Maybe you as the systems administrator decide that the marketing people should be using only Microsoft PowerPoint—a rather narrow view, but let's use that just for the sake of argument. All you need to do is click the Enabled radio button, click the Show button, and in the Show Contents window click the Add button to add the application—in this case, PowerPoint, which is Powerpnt.exe. An example of this is shown in Figure 4-14.

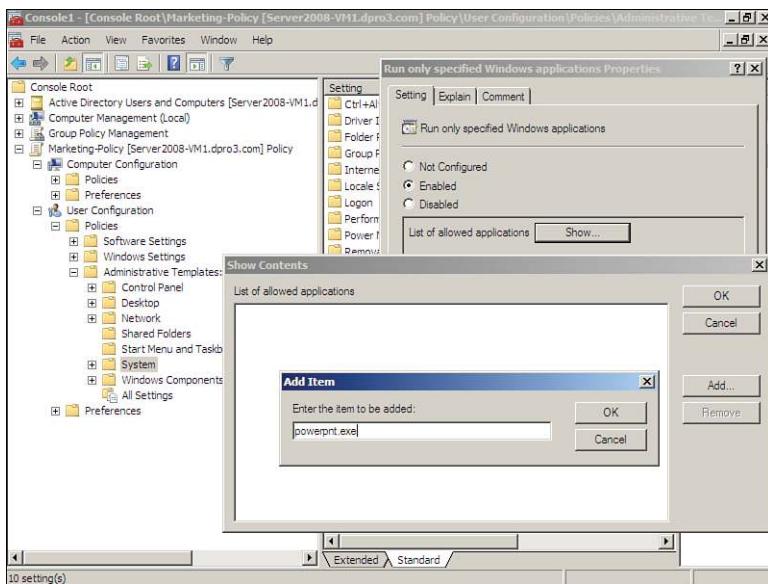


Figure 4-14 Adding a Single Allowed Application

This is in-depth stuff, and the CompTIA Security+ exam *probably* won't test you on exact procedures for this, but you should be aware that there are various ways to disallow access to just about anything you can think of. Of course, the more practice you can get on various servers, including Windows Server, the better. For those applications that users are allowed to work with, they should be secured accordingly.

In general, applications should be updated, patched, or have the appropriate service packs installed. This is collectively known as *application patch management*, and is an overall part of the configuration management of an organization's software environment. Table 4-1 shows some common applications and some simple safeguards that can be implemented for them.

Table 4-1 Common Applications and Safeguards

Application Name	Safeguards
Outlook	<p>Install the latest Office service pack. (This applies to all Office suite applications.)</p> <p>Keep Office up to date with Windows Update. (This also applies to all Office suite applications.)</p> <p>Consider an upgrade to a newer version of Office, if the currently used one is no longer supported.</p> <p>Increase the junk e-mail security level or use a whitelist.</p> <p>Read messages in plain text instead of HTML.</p> <p>Enable attachment blocking.</p> <p>Use a version that enables Object Model Guard functionality, or download it for older versions.</p> <p>Password protect any .PST files.</p> <p>Consider encrypting the authentication scheme, and possibly other traffic, including message traffic between Outlook clients and Exchange servers. Secure Password Authentication (SPA) can be used to secure the login, and S/MIME and PGP can be used to secure actual e-mail transmissions. Or, in the case of web-based e-mail, use SSL or TLS for encryption.</p>
Word	<p>Consider using passwords for opening or modifying documents.</p> <p>Use read-only or comments only (tracking changes) settings.</p> <p>Consider using a digital certificate to seal the document.</p>
Excel	<p>Use password protection on worksheets.</p> <p>Set macro security levels.</p> <p>Consider Excel encryption.</p>

Mobile apps should be secured as well. You might want to disable GPS to protect a mobile app, or the mobile device in general. You should also consider strong passwords for e-mail accounts and accounts to “app stores” and similar shopping portals. Watch for security updates for the mobile apps your organization uses.

We also need to give some thought to back office applications that run on servers. Database software, e-mail server software, and other back office “server” software needs to be hardened and secured as well. High-level server application examples from Microsoft include SQL Server and Exchange Server—and let’s not forget FTP servers and web servers. These applications have their own set of configuration requirements and might be insecure out-of-the-box. For instance, a database server, FTP server, or other similar server will often have its own separate administrator

account with a blank password by default. It is common knowledge what the names of these administrative user accounts are, and if they haven't been secured, hacking the system becomes mere child's play. Be sure to rename accounts (and disable unnecessary accounts) and configure strong passwords, just the way you would in an operating system. One other thing to watch for in general is consolidation. Some organizations, in an attempt to save money, will merge several back office systems onto one computer. While this is good for the budget, and uses a small amount of resources, it opens the floodgates for attack. The more services a server has running, the more open doorways that exist to that system—and, the more possible ways that the server can fail. The most important services should be compartmentalized physically or virtually in order to reduce the size of the attack surface, and lower the total amount of threats to an individual system.

Organizations use many applications specific to their type of business. Stay on top of the various vendors that supply your organization with updates and new versions of software. Always test what effects one new piece of software will have on the rest of your installed software before implementation.

So far in this chapter we have discussed browser software, server-based applications, and other apps such as Microsoft Office. But that just scratches the surface. Whatever the application you use, attempt to secure it by planning how it will be utilized and deployed, updating it, and configuring it. Access the manufacturer's website for more information on how to secure the specific applications you use. Just remember that users (and other administrators) still need to work with the program. Don't make it so secure that a user gets locked out!

Secure Programming

We mentioned several times that many applications are inherently insecure out-of-the-box. But this problem can be limited with the implementation of secure programming or **secure coding concepts**. Secure coding concepts can be defined as the best practices used during software development in an effort to increase the security of the application being built—they *harden* the code of the application. In this section we cover several types of secure coding concepts used by programmers, some of the vulnerabilities programmers should watch out for, and how to defend against them.

Systems Development Life Cycle

To properly develop a secure application, the developer has to scrutinize it at every turn, and from every angle, throughout the life of the project. Over time, this idea manifested itself into the concept known as the **systems development life cycle (SDLC)**—an organized process of planning, developing, testing, deploying, and

maintaining systems and applications, and the various methodologies used to do so. The SDLC can be broken down into several phases, including

1. **Planning and analysis**—Goals are determined, needs are assessed, and high-level planning is accomplished.
2. **Systems design**—The design of the system or application is defined and diagrammed in detail.
3. **Implementation**—The code for the project is written.
4. **Testing**—The system or application is checked thoroughly in a testing environment.
5. **Deployment**—The system or application is put into production and is now available to end-users.
6. **Maintenance**—Software is monitored and updated throughout the rest of its life cycle.

This is a basic example of the phases in an SDLC. It could be more or less complicated depending on the project and the organization involved.

From a larger perspective a programmer/systems developer should keep the CIA concept in mind:

- **Maintaining confidentiality:** Only allowing users access to data to which they have permission
- **Preserving integrity:** Ensuring data is not tampered with or altered
- **Protecting availability:** Ensuring systems and data are accessible to authorized users when necessary

The CIA concepts are important when doing a **secure code review**, which can be defined as an in-depth code inspection procedure. It is often included by organizations as part of the testing phase of the SDLC but is usually conducted before other tests such as fuzzing or penetration tests, which we discuss more later in this chapter.

In general, quality assurance policies and procedures should be implemented while developing and testing code. This will vary from one organization to the next, but generally includes procedures that have been developed by a team, a set of checks and balances, and a large amount of documentation. By checking the documentation within a project, a developer can save a lot of time, while keeping the project more secure.

One secure and structured approach that organizations take is called threat modeling. **Threat modeling** enables you to prioritize threats to an application, based

on their potential impact. The modeling process includes identifying assets to the system or application, uncovering vulnerabilities, identifying threats, documenting threats, and rating those threats according to their potential impact. The more risk, the higher the rating. Threat modeling is often incorporated into the SDLC during the design, testing, and deployment phases.

Some other security principles that should be incorporated into the SDLC include

- **Principle of least privilege:** Applications should be coded and run in such a way as to maintain the principle of least privilege. Users should only have access to what they need. Processes should run with only the bare minimum access needed to complete their functions. However, this can be coupled with separation of privilege, where access to objects depends on more than one condition (for example, authentication plus an encrypted key).
- **Principle of defense in depth:** The more security controls the better. The layering of defense in secure coding may take the form of validation, auditing, special authentication techniques, and so on.
- **Applications should never trust user input:** Input should be validated carefully.
- **Minimize the attack surface area:** Every additional feature that a programmer adds to an application increases the size of the attack surface and increases risk. Unnecessary functions should be removed, and necessary functions should require authorization.
- **Establish secure defaults:** Out-of-the-box offerings should be as secure as possible. If possible, user password complexity and password aging default policies should be configured by the programmer, not the user. Permissions should default to no access and should be granted only as they are needed.
- **Fail securely:** At times, applications will fail. How they fail determines their security. Failure exceptions might show the programming language that was used to build the application, or worse, lead to access holes. Error handling/exception handling code should be checked thoroughly so that a malicious user can't find out any additional information about the system. These error-handling methods are sometimes referred to technically as pseudocodes. For example, to handle a program exception, a properly written pseudocode will basically state (in spoken English): "If a program module crashes, then restart the program module."
- **Fix security issues correctly:** Once found, security vulnerabilities should be thoroughly tested, documented, and understood. Patches should be developed to fix the problem, but not cause other issues or application regression.

For the Security+ exam, the most important of the SDLC phases are maintenance and testing. In the maintenance phase, which doesn't end until the software is removed from all computers, an application needs to be updated accordingly, corrected when it fails, and constantly monitored. We discuss more about monitoring in Chapter 12, "Monitoring and Auditing." In the testing phase, a programmer (or team of programmers and other employees) checks for bugs and errors in a variety of ways. It's imperative that you know some of the vulnerabilities and attacks to a system or application, and how to fix them and protect against them. The best way to prevent these attacks is to test and review code.

Programming Testing Methods

Let's discuss the testing methods and techniques that can be implemented to seek out programming vulnerabilities and help prevent attacks from happening.

Programmers have various ways to test their code, including system testing, input validation, and fuzzing. By using a combination of these testing techniques during the testing phase of the SDLC, there is a much higher probability of a secure application as the end result.

System testing is generally broken down into two categories: black-box and white-box. **Black-box testing** utilizes people who do not know the system. These people (or programs if automated) test the functionality of the system. Specific knowledge of the system code, and programming knowledge in general, is not required. The tester does not know about the system's internal structure and is often given limited information about what the application or system is supposed to do. In black-box testing, one of the most common goals is to crash the program. If a user is able to crash the program by entering improper input, the programmer has probably neglected to thoroughly check the error-handling code and/or input validation.

On the other side of the spectrum, **white-box testing** (also known as transparent testing) is a way of testing the internal workings of the application or system. Testers must have programming knowledge and are given detailed information about the design of the system. They are given login details, production documentation, and source code. System testers might use a combination of fuzzing (covered shortly), data flow testing, and other techniques such as penetration testing and sandboxes. A *penetration test* is a method of evaluating a system's security by simulating one or more attacks on that system. We speak more about penetration testing in Chapter 11, "Vulnerability and Risk Assessment." A **sandbox** is a term applied to when a web script (or other code) runs in its own environment for the express purpose of not interfering with other processes, often for testing. Sandboxing technology is frequently used to test unverified applications for malware, malignant code, and possible errors such as buffer overflows.

A third category that has become more common of late is *gray-box testing*, where the tester has internal knowledge of the system from which to create tests but conducts the tests the way a black-box tester would—at the user level.

Input validation is very important for website design and application development. **Input validation**, or data validation, is a process that ensures the correct usage of data—it checks the data that is inputted by users into web forms and other similar web elements. If data is not validated correctly, it can lead to various security vulnerabilities and the possibility of data corruption. You can validate data in many ways, from coded data checks and consistency checks to spelling and grammar checks, and so on. Whatever data is being dealt with, it should be checked to make sure it is being entered correctly and won't create or take advantage of a security flaw. If validated properly, bad data and malformed data will be rejected. Input validation should be done both on the client side and, more importantly, on the server side. Let's look at an example next.

If an organization has a web page with a PHP-based contact form, the data entered by the visitor should be checked for errors, or maliciously typed input. The following is a piece of PHP code contained within a common contact form:

```
else if (!preg_match('/^ [A-Za-z0-9.-]+$/ ', $domain))  
{  
    // character not valid in domain part  
    $isValid = false;  
}
```

This is a part of a larger piece of code that is checking the entire e-mail address a user enters into a form field. This particular snippet of code checks to make sure the user is not trying to enter a backslash in the domain name portion of the e-mail address. This is not allowed in e-mail addresses and could be detrimental if used maliciously. Note in the first line within the brackets it says `A-Za-z0-9.-`, which is telling the system what characters are allowed. Uppercase and lowercase letters, numbers, periods, and dashes are allowed, but other characters such as backslashes, dollar signs, and so on are not allowed. Those other characters would be interpreted by the form's supporting PHP files as illegitimate data and would not be passed on through the system. The user would receive an error, which is a part of client-side validation. But, the more a PHP form is programmed to check for errors, the more it is possible to have additional security holes. Therefore, server-side validation is even more important. Any data that is passed on by the PHP form should be checked at the server as well. In fact, an attacker might not even be using the form in question, and might be attacking the URL of the web page in some other manner. This can be checked at the server within the database software, or through other means. (The same goes for pages that utilize JavaScript.)

This is just one basic example, but as mentioned previously, input validation is the key to preventing attacks such as SQL injection and XSS. All form fields should be tested for good input validation code, both on the client side and the server side. By combining the two, and checking every access attempt, you develop complete mediation of requests.

Fuzz testing (or fuzzing) is another smart concept. This is where random data is inputted into a computer program in an attempt to find vulnerabilities. This is often done without knowledge of the source code of the program. The program to be tested is run, has data inputted to it, and is monitored for exceptions such as crashes. This can be done with applications and operating systems. It is commonly used to check file parsers within applications such as Microsoft Word, and network parsers that are used by protocols such as DHCP. Fuzz testing can uncover full system failures, memory leaks, and error-handling issues. Fuzzing is usually automated (a program that checks a program) and can be as simple as sending a random set of bits to be inputted to the software. However, designing the inputs that cause the software to fail can be a tricky business, and often a myriad of variations of code needs to be tried to find vulnerabilities. Once the fuzz test is complete, the results are analyzed, the code is reviewed and made stronger, and vulnerabilities that were found are removed. The stronger the fuzz test, the better the chances that the program will not be susceptible to exploits.

As a final word on this, once code is properly tested and approved, it should be reused whenever possible. This helps to avoid “re-creating the wheel” and avoids common mistakes that a programmer might make that others might have already fixed.

Programming Vulnerabilities and Attacks

Let's discuss some program code vulnerabilities and the attacks that exploit them. This section gives specific ways to mitigate these risks during application development, hopefully preventing these threats and attacks from becoming realities.

NOTE This is a rather short section, and covers a topic that we could fill several books with. It is not a seminar on how to program, but rather a concise description of programmed attack methods, and some defenses against them. The Security+ objectives do not go into great detail concerning these methods, but CompTIA does expect you to have a broad and basic understanding.

Backdoors

To begin, applications should be analyzed for backdoors. As mentioned in Chapter 2, “Computer Systems Security,” backdoors are used in computer programs to bypass normal authentication and other security mechanisms in place. These can be avoided by updating the operating system and applications and firmware on devices, and especially by carefully checking the code of the program. If the system is not updated, a malicious person could take all kinds of actions via the backdoor. For example, a software developer who works for a company could install code through a backdoor that reactivates the user account after it was disabled (for whatever reason—termination, end of consulting period, and so on). This is done through the use of a logic bomb (in addition to the backdoor) and could be deadly once the software developer has access again. To reiterate, make sure the OS is updated, and also consider job rotation, where programmers check each other’s work.

Buffer Overflows

Next, program code should protect against buffer overflows. A **buffer overflow** is when a process stores data outside the memory that the developer intended. This could cause erratic behavior in the application, especially if the memory already had other data in it. Stacks and heaps are data structures that can be affected by buffer overflows. The stack is a key data structure necessary for the exchange of data between procedures. The heap contains data items whose size can be altered during execution. Value types are stored in a stack, whereas reference types are stored in a heap. An ethical coder will try to keep these running efficiently. An unethical coder wanting to create a program vulnerability could, for example, omit input validation, which could allow a buffer overflow to affect heaps and stacks, which in turn could adversely affect the application or the operating system in question.

Let’s say a programmer allows for 16 bytes in a string variable. This won’t be a problem normally. However, if the programmer failed to verify that *no more than* 16 bytes could be copied over to the variable, that would create a vulnerability that an attacker could exploit with a buffer overflow attack. The buffer overflow can also be initiated by certain inputs. For example, corrupting the stack with no-operation (nop, NOP, or NOOP) machine instructions, which when used in large numbers can start a NOP slide, can ultimately lead to the execution of unwanted arbitrary code, or lead to a denial-of-service (DoS) on the affected computer.

All this can be prevented by patching the system or application in question, making sure that the OS uses data execution prevention, and utilizing bounds checking, which is a programmatic method of detecting whether a particular variable is within design bounds before it is allowed to be used. It can also be prevented by using correct code, checking code carefully, and using the right programming language for

the job in question (the right tool for the right job, yes?). Without getting too much into the programming side of things, special values called “canaries” are used to protect against buffer overflows.

On a semi-related note, **integer overflows** are when arithmetic operations attempt to create a numeric value that is too big for the available memory space. This creates a *wrap* and can cause resets and undefined behavior in programming languages such as C and C++. The security ramifications is that the integer overflow can violate the program’s default behavior and possibly lead to a buffer overflow. This can be prevented or avoided by making overflows trigger an exception condition, or by using a model for automatically eliminating integer overflow, such as the CERT As-if Infinitely Ranged (AIR) integer model. More can be learned about this model at the following link:

<http://www.cert.org/secure-coding/tools/integral-security.cfm>

Arbitrary Code Execution/Remote Code Execution

Arbitrary code execution is when an attacker obtains control of a target computer through some sort of vulnerability, thus gaining the power to execute commands on that remote computer at will. Programs that are designed to exploit software bugs or other vulnerabilities are often called arbitrary code execution exploits. These types of exploits inject “shellcode” to allow the attacker to run arbitrary commands on the remote computer. This type of attack is also known as **remote code execution (RCE)** and can potentially allow the attacker to take full control of the remote computer and turn it into a zombie.

RCE commands can be sent to the target computer using the URL of a browser, or by using the Netcat service, among other methods. To defend against this, applications should be updated, or if the application is being developed by your organization, it should be checked with fuzz testing and strong input validation (client side and server side) as part of the testing stage of the SDLC. If you have PHP running on a web server, it can be set to disable remote execution of configurations. A web server (or other server) can also be configured to block access from specific hosts.

NOTE RCE is also very common with web browsers. All browsers have been affected at some point, though some instances are more publicized than others. To see proof of this, access the Internet and search for the Common Vulnerabilities and Exposures (CVE) list for each type of web browser.

XSS and XSRF

Two web application vulnerabilities to watch out for include **cross-site scripting (XSS)** and **cross-site request forgery (XSRF)**.

XSS holes are vulnerabilities that can be exploited with a type of code injection. Code injection is the exploitation of a computer programming bug or flaw by inserting and processing invalid information—it is used to change how the program executes data. In the case of an XSS attack, an attacker inserts malicious scripts into a web page in the hopes of gaining elevated privileges and access to session cookies and other information stored by a user's web browser. This code (often JavaScript) is usually injected from a separate “attack site.” It can also manifest itself as an embedded JavaScript image tag, header manipulation (as in manipulated HTTP response headers), or other HTML embedded image object within e-mails (that are web-based). The XSS attack can be defeated by programmers through the use of output encoding (JavaScript escaping, CSS escaping, and URL encoding), by preventing the use of HTML tags, and by input validation: for example, checking forms and confirming that input from users does not contain hypertext. On the user side, the possibility of this attack’s success can be reduced by increasing cookie security and by disabling scripts in the ways mentioned in the first section of this chapter, “Securing the Browser.” If XSS attacks by e-mail are a concern, the user could opt to set his e-mail client to text only.

The XSS attack exploits the trust a user’s browser has in a website. The converse of this, the XSRF attack, exploits the trust that a website has in a user’s browser. In this attack (also known as a one-click attack), the user’s browser is compromised and transmits unauthorized commands to the website. The chances of this attack can be reduced by requiring tokens on web pages that contain forms, special authentication techniques (possibly encrypted), scanning .XML files (which could contain the code required for unauthorized access), and submitting cookies twice instead of once, while verifying that both cookie submissions match.

More Code Injection Examples

Other examples of code injection include SQL injection, XML injection, and LDAP injection. Let’s discuss these briefly now.

Databases are just as vulnerable as web servers. The most common kind of database is the relational database, which is administered by a relational database management system (RDBMS). These systems are usually written in the Structured Query Language (SQL). An example of a SQL database is Microsoft’s SQL Server (pronounced “sequel”); it can act as the back end for a program written in Visual Basic or Visual C++. Another example is MySQL, a free, open-source relational database often used in conjunction with websites that employ PHP pages. The main concern

with SQL is the SQL injection attack, which occurs in databases, ASP.NET applications, and blogging software (such as WordPress) that use MySQL as a back end. In these attacks user input in web forms is not filtered correctly and is executed improperly, with the end result of gaining access to resources or changing data. For example, the login form for a web page that uses a SQL back end (such as a WordPress login page) can be insecure, especially if the front-end application is not updated. An attacker will attempt to access the database (from a form or in a variety of other ways), query the database, find out a user, and then inject code to the password portion of the SQL code—perhaps something as simple as `x = x`. This will allow any password for the user account to be used. If the login script was written properly (and validated properly), it should deflect this injected code. But if not, or if the application being used is not updated, it could be susceptible. It can be defended against by constraining user input, filtering user input, using input validating forms, and using special parameters with stored procedures.

There are, however, other databases that don't use SQL (or use code in addition to SQL). Known as NoSQL databases, they offer a different mechanism for retrieving data than their relational database counterparts. These are commonly found in virtual systems provided by cloud-based services. While they are usually resistant to SQL injection, there are NoSQL injection attacks as well. Because of the type of programming used in NoSQL, the potential impact of a NoSQL injection attack can be greater than that of a SQL injection attack. An example of a NoSQL injection attack is the JavaScript Object Notation (JSON) injection attack. But, NoSQL databases are also vulnerable to brute-force attacks (cracking of passwords) and connection pollution (a combination of XSS and code injection techniques). Methods to protect against NoSQL injection are similar to the methods mentioned for SQL injection. However, because NoSQL databases are often used within cloud services, a security administrator for a company might not have much control over the level of security that is implemented. In these cases, careful scrutiny of the service-level agreement (SLA) between the company and the cloud provider is imperative.

LDAP injection is similar to SQL injection, again using a web form input box to gain access, or by exploiting weak LDAP lookup configurations. The Lightweight Directory Access Protocol is a protocol used to maintain a directory of information such as user accounts, or other types of objects. The best way to protect against this (and all code injection techniques for that matter) is to incorporate strong input validation.

XML injection attacks can compromise the logic of XML (Extensible Markup Language) applications—for example, XML structures that contain the code for users. It can be used to create new users and possibly obtain administrative access. This can be tested for by attempting to insert XML metacharacters such as single and double quotes. It can be prevented by filtering *in* allowed characters (for example, A–Z only). This is an example of “default deny” where only what you explicitly filter in is permitted; everything else is forbidden.

One thing to remember is that when attackers utilize code injecting techniques, they are adding their own code to existing code, or are inserting their own code into a form. A variant of this is command injection, which doesn't utilize new code; instead, an attacker executes system-level commands on a vulnerable application or OS. The attacker might enter the command (and other syntax) into an HTML form or other web-based form to gain access to a web server's password files.

NOTE Though not completely related, another type of injection attack is DLL injection. This is when code is run within the address space of another process by forcing it to load a dynamic link library (DLL). Ultimately, this can influence the behavior of a program that was not originally intended. It can be uncovered through penetration testing, which we will discuss more in Chapter 11.

Once again, the best way to defend against code injection/command injection techniques in general is by implementing input validation during the development, testing, and maintenance phases of the SDLC.

Directory Traversal

Directory traversal, or the .. (dot dot slash) attack, is a method of accessing unauthorized parent (or worse, root) directories. It is often used on web servers that have PHP files and are Linux or UNIX-based, but it can also be perpetrated on Microsoft operating systems (in which case it would be ..\ or the “dot dot backslash” attack). It is designed to get access to files such as ones that contain passwords. This can be prevented by updating the OS, or by checking the code of files for vulnerabilities, otherwise known as fuzzing. For example, a PHP file on a Linux-based web server might have a vulnerable `if` or `include` statement, which when attacked properly could give the attacker access to higher directories and the `passwd` file.

Zero Day Attack

A **zero day attack** is an attack executed on a vulnerability in software, before that vulnerability is known to the creator of the software. It's not a specific attack, but rather a group of attacks including viruses, Trojans, buffer overflow attacks, and so on. These attacks can cause damage even after the creator knows of the vulnerability, because it may take time to release a patch to prevent the attacks and fix damage caused by them. It can be discovered by thorough analysis and fuzz testing.

Zero day attacks can be prevented by using newer operating systems that have protection mechanisms and by updating those operating systems. It can also be

prevented by using multiple layers of firewalls and by using whitelisting, which only allows known good applications to run. Collectively, these preventive methods are referred to as zero day protection.

Table 4-2 summarizes the programming vulnerabilities/attacks we have covered in this section.



Table 4-2 Summary of Programming Vulnerabilities and Attacks

Vulnerability	Description
Backdoor	Placed by programmers, knowingly or inadvertently, to bypass normal authentication, and other security mechanisms in place
Buffer overflow	When a process stores data outside the memory that the developer intended
Remote code execution (RCE)	When an attacker obtains control of a target computer through some sort of vulnerability, gaining the power to execute commands on that remote computer
Cross-site scripting (XSS)	Exploits the trust a user's browser has in a website through code injection, often in web forms
Cross-site request forgery (XSRF)	Exploits the trust that a website has in a user's browser, which becomes compromised and transmits unauthorized commands to the website
Code injection	When user input in database web forms is not filtered correctly and is executed improperly. SQL injection is a very common example.
Directory traversal	A method of accessing unauthorized parent (or worse, root) directories
Zero day	A group of attacks executed on vulnerabilities in software before those vulnerabilities are known to the creator

The CompTIA Security+ exam objectives don't expect you to be a programmer, but they do expect you to have a basic knowledge of programming languages and methodologies so that you can help to secure applications effectively. I recommend a basic knowledge of programming languages used to build applications, such as Visual Basic, C++, C#, Java, and Python, as well as web-based programming languages such as HTML, ASP, and PHP, plus knowledge of database programming languages such as SQL. This foundation knowledge will help you not only on the exam, but also as a security administrator when you have to act as a liaison to the programming team, or if you are actually involved in testing an application.

Chapter Summary

Without applications, a computer doesn't do much for the user. Unfortunately, applications are often the most vulnerable part of a system. The fact that there are so many of them and that they come from so many sources can make it difficult to implement effective application security. This chapter gave a foundation of methods you can use to protect your programs.

The key with most organizations is to *limit* the number of applications that are used. The fewer applications, the easier they are to secure and, most likely, the more productive users will be. We mentioned the whitelisting and blacklisting of applications in this chapter and in Chapter 3, and those methods can be very effective. However, there are some applications that users cannot do without. One example is the web browser. Internet Explorer is beyond prolific when it comes to desktop computers. Firefox, Chrome, and Safari are also very widely used. For mobile devices, Safari and the Android browser are the most common. One general rule for browsers is to watch out for the latest version. You should be on top of security updates for the current version you are using, but always test a new version of a browser very carefully before implementing it.

In general, browser security precautions include implementing policies, training your users, using proxy and content filters, and securing against malicious code. Beyond that, IE and Firefox have their own specific methods of security. For instance, each has its own methods for managing cookies, working with trusted sites, using add-ons, turning off ActiveX and JavaScript, and watching for properly encrypted sessions. Use these and other methods mentioned in the chapter to thoroughly secure the browsers on your client computers.

Other applications can be secured by implementing User Account Control (UAC), whitelisting applications through policy, using strong password protection, and encrypting data and traffic.

As a security administrator, you usually work with applications that have already been developed for you. But sometimes, you might dabble in some development yourself. If this is the case, you should adhere to the principles of secure programming discussed in this chapter. The systems development life cycle (SDLC) gives you a methodical process of planning, developing, testing, deploying, and maintaining your systems and applications, while maintaining the confidentiality, preserving the integrity, and protecting the availability of your data. Principles you should invoke include least privilege, defense in depth, minimizing the attack surface, and failing securely.

To really make the most of the SDLC, you should test thoroughly, or at least verify that your programmers have done so. Black-box and white-box testing, sandboxing, fuzzing, and input validation checks are excellent methods for testing code

and preventing programming vulnerabilities and attacks such as the use of backdoors, buffer overflows, remote code execution, code injection, directory traversal, and zero day attacks.

Learn as much as you can about web browsers, and other commonly used applications such as the Microsoft Office suite, so that you can be better prepared to protect them. Build your knowledge about programming techniques, including high-level languages such as Visual Basic and C++, and web-based languages including HTML and PHP. By combining the knowledge of a systems administrator and a programmer, you will have the best chance of securing your systems and applications.

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 4-3 lists a reference of these key topics and the page number on which each is found.

Table 4-3 Key Topics for Chapter 4

Key Topic Element	Description	Page Number
Figure 4-1	Internet Explorer Security Features in the Local Computer Policy	130
Figure 4-3	Internet Explorer policies in the Marketing-Policy GPO	132
Figure 4-4	Configuring the proxy server connection in Internet Explorer	134
Figure 4-5	Internet Options dialog box—Security zones	136
Figure 4-6	Internet Options dialog box—Privacy tab	137
Figure 4-10	Firefox Privacy options	142
Figure 4-11	Firefox Security options	143
Figure 4-12	Firefox proxy connection	144
Table 4-2	Summary of programming vulnerabilities and attacks	162

Define Key Terms

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

cookies, locally shared object (LSO), User Account Control (UAC), secure coding concepts, systems development life cycle (SDLC), secure code review, threat modeling, black-box testing, white-box testing, sandbox, input validation, fuzz testing, buffer overflow, integer overflow, remote code execution (RCE), cross-site scripting (XSS), cross-site request forgery (XSRF), directory traversal, zero day attack

Review Questions

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

1. Which of the following is one way of preventing spyware from being downloaded?
 - A. Use firewall exceptions.
 - B. Adjust Internet Explorer security settings.
 - C. Adjust the Internet Explorer home page.
 - D. Remove the spyware from Add/Remove Programs.
2. What key combination should be used to close a pop-up window?
 - A. Windows+R
 - B. Ctrl+Shift+Esc
 - C. Ctrl+Alt+Del
 - D. Alt+F4
3. Which protocol can be used to secure the e-mail login from an Outlook client using POP3 and SMTP?
 - A. SMTP
 - B. SPA
 - C. SAP
 - D. Exchange

4. What are two ways to secure Internet Explorer? (Select the two best answers.)
 - A. Set the Internet zone's security level to High.
 - B. Disable the pop-up blocker.
 - C. Disable ActiveX controls.
 - D. Add malicious sites to the Trusted Sites zone.
5. Heaps and stacks can be affected by which of the following attacks?
 - A. Buffer overflows
 - B. Rootkits
 - C. SQL injection
 - D. Cross-site scripting
6. As part of your user awareness training, you recommend that users remove which of the following when they finish accessing the Internet?
 - A. Instant messaging
 - B. Cookies
 - C. Group policies
 - D. Temporary files
7. Which statement best applies to the term Java applet?
 - A. It decreases the usability of web-enabled systems.
 - B. It is a programming language.
 - C. A web browser must have the capability to run Java applets.
 - D. It uses digital signatures for authentication.
8. Which of the following concepts can ease administration but can be the victim of a malicious attack?
 - A. Zombies
 - B. Backdoors
 - C. Buffer overflow
 - D. Group Policy

- 9.** In an attempt to collect information about a user's activities, which of the following will be used by spyware?
- A.** Tracking cookie
 - B.** Session cookie
 - C.** Shopping cart
 - D.** Persistent cookie
- 10.** What is it known as when a web script runs in its own environment and does not interfere with other processes?
- A.** Quarantine
 - B.** Honeynet
 - C.** Sandbox
 - D.** VPN
- 11.** How can you train a user to easily determine whether a web page has a valid security certificate? (Select the best answer.)
- A.** Have the user contact the webmaster.
 - B.** Have the user check for HTTPS://.
 - C.** Have the user click the padlock in the browser and verify the certificate.
 - D.** Have the user call the ISP.
- 12.** To code applications in a secure manner, what is the best practice to use?
- A.** Cross-site scripting
 - B.** Flash version 3
 - C.** Input validation
 - D.** HTML version 5
- 13.** An organization hires you to test an application that you have limited knowledge of. You are given a login to the application but do not have access to source code. What type of test are you running?
- A.** White-box
 - B.** Gray-box
 - C.** Black-box
 - D.** SDLC

- 14.** You check the application log of your web server and see that someone attempted unsuccessfully to enter the text `test; etc/passwd` into an HTML form field. Which attack was attempted?
 - A.** SQL injection
 - B.** Code injection
 - C.** Command injection
 - D.** Buffer overflow
- 15.** An attacker takes advantage of a vulnerability in programming that allows the attacker to copy more than 16 bytes to a standard 16-byte variable. Which attack is being initiated?
 - A.** Directory traversal
 - B.** Command injection
 - C.** XSS
 - D.** Buffer overflow
- 16.** What's the best way to prevent SQL injection attacks on web applications?
 - A.** Input validation
 - B.** Host-based firewall
 - C.** Add HTTPS pages
 - D.** Update the web server
- 17.** Which of the following attacks uses a JavaScript image tag in an e-mail?
 - A.** SQL injection
 - B.** Cross-site scripting
 - C.** Cross-site request forgery
 - D.** Directory traversal
- 18.** Which of the following should occur first when developing software?
 - A.** Fuzzing
 - B.** Penetration testing
 - C.** Secure code review
 - D.** Patch management

- 19.** You are the security administrator for a multimedia development company. Users are constantly searching the Internet for media, information, graphics, and so on. You receive complaints from several users about unwanted windows appearing on their displays. What should you do?
- A.** Install antivirus software
 - B.** Install pop-up blockers
 - C.** Install screensavers
 - D.** Install a host-based firewall
- 20.** You have analyzed what you expect to be malicious code. The results show that JavaScript is being utilized to send random data to a separate service on the same computer. What attack has occurred?
- A.** DoS
 - B.** SQL injection
 - C.** LDAP injection
 - D.** Buffer overflow
- 21.** Which of the following best describes a protective countermeasure for SQL injection?
- A.** Validating user input within web-based applications
 - B.** Installing an IDS to monitor the network
 - C.** Eliminating XSS vulnerabilities
 - D.** Implementing a firewall server between the Internet and the database server
- 22.** You have implemented a security technique where an automated system generates random input data to test an application. What have you put into practice?
- A.** XSRF
 - B.** Fuzzing
 - C.** Hardening
 - D.** Input validation

- 23.** Many third-party programs have security settings disabled by default. What should you as the security administrator do before deploying new software?
 - A.** Network penetration testing
 - B.** Input validation
 - C.** Application whitelisting
 - D.** Application hardening
- 24.** Which of the following will allow the triggering of a security alert because of a tracking cookie?
 - A.** Anti-spyware application
 - B.** Anti-spam software
 - C.** Network-based firewall
 - D.** Host-based firewall
- 25.** Your organization's servers and applications are being audited. One of the IT auditors tests an application as an authenticated user. Which of the following testing methods is being used?
 - A.** White-box
 - B.** Penetration testing
 - C.** Black-box
 - D.** Gray-box
- 26.** Which of the following encompasses application patch management?
 - A.** Policy management
 - B.** Fuzzing
 - C.** Configuration management
 - D.** Virtualization

Answers and Explanations

- 1. B.** Adjust the Internet Explorer security settings so that security is at a higher level, and add trusted and restricted websites.
- 2. D.** Alt+F4 is the key combination that is used to close an active window. Sometimes it is okay to click the X, but malware creators are getting smarter all the time; the X could be a ruse.

3. **B.** SPA (Secure Password Authentication) is a Microsoft protocol used to authenticate e-mail clients. S/MIME and PGP can be used to secure the actual e-mail transmissions.
4. **A.** and **C.** By increasing the Internet zone security level to High, you employ the maximum safeguards for that zone. ActiveX controls can be used for malicious purposes; disabling them makes it so that they do not show up in the browser. Disabling a pop-up blocker and adding malicious sites to the Trusted Sites zone would make Internet Explorer less secure.
5. **A.** Heaps and stacks are data structures that can be affected by buffer overflows. Value types are stored in a stack, whereas reference types are stored in a heap. An ethical coder will try to keep these running efficiently. An unethical coder will attempt to use a buffer overflow to affect heaps and stacks, which in turn could affect the application in question or the operating system. The buffer overflow might be initiated by certain inputs and can be prevented by bounds checking.
6. **B.** The best answer is cookies, which can be used for authentication and session tracking and can be read as plain text. They can be used by spyware and can track people without their permission. It is also wise to delete temporary Internet files as opposed to temporary files.
7. **C.** To run Java applets, a web browser must have that option enabled. Java increases the usability of web-enabled systems, and Java is a programming language. It does not use digital signatures for authentication.
8. **B.** Backdoors were originally created to ease administration. However, hackers quickly found that they could use these backdoors for a malicious attack.
9. **A.** A tracking cookie will be used, or misused, by spyware in an attempt to access a user's activities. Tracking cookies are also known as browser cookies or HTTP cookies, or simply cookies. Shopping carts take advantage of cookies to keep the shopping cart reliable.
10. **C.** When a web script runs in its own environment for the express purpose of not interfering with other processes, it is known as running in a sandbox. Often, the sandbox will be used to create sample scripts before they are actually implemented. Quarantining is a method used to isolate viruses. A honeynet is a collection of servers used to attract hackers and isolate them in an area where they can do no damage. VPN is short for virtual private network, which enables the connection of two hosts from remote networks.
11. **C.** In Internet Explorer, the user should click the padlock in the browser; this will show the certificate information. Often, the address bar will have different colors as the background; for example, blue or green means that the certificate

is valid, whereas red or pink indicates a problem. In Firefox, click the name of the website listed in the address bar just before where it says HTTPS to find out the validity of the certificate. Contacting the webmaster and calling the ISP are time-consuming, not easily done, and not something that an end user should do. Although HTTPS:// can tell a person that the browser is now using Hypertext Transfer Protocol Secure, it does not necessarily determine whether the certificate is valid.

12. **C.** Input validation is the best practice to use when coding applications. This is important when creating web applications or web pages that require information to be inputted by the user.
13. **B.** A gray-box test is when you are given limited information about the system you are testing. Black-box testers are not given logins, source code, or anything else, though they may know the functionality of the system. White-box testers are given logins, source code, documentation, and more. SDLC stands for systems development life cycle, of which these types of tests are just a part.
14. **C.** In this case a command was entered, and the attacker was attempting to gain access to the password file within the /etc directory. If the attacker tried to inject code, he would not use commands, but rather PHP, ASP, or another language. SQL injections are usually run on databases, not web servers' HTML forms. Buffer overflows have to do with memory and how applications utilize it.
15. **D.** A buffer overflow can be initiated when a string variable is not programmed correctly—for example, if the variable allows for more than the standard amount of bytes. Directory traversal is when an attacker uses commands and code to access unauthorized parent directories. Command injection is when commands and command syntax are entered into an application or OS. XSS or cross-site scripting is when code is injected into a website form to obtain information and unauthorized access.
16. **A.** Input validation is the best way to prevent SQL injection attacks on web servers and database servers (or combinations of the two). Host-based firewalls aid in preventing network attacks but not necessarily coded attacks of this type. HTTPS pages initiate a secure transfer of data, but they don't necessarily lock out attackers that plan on using SQL injection. Updating the web server is a good idea, but will have little if any effect on the forms that are written by the web programmer.
17. **B.** Cross-site scripting (XSS) can be initiated on web forms or through e-mail. It often uses JavaScript to accomplish its means. SQL injection is when code (SQL based) is inserted into forms or databases. Cross-site request forgery (XSRF) is when a user's browser sends unauthorized commands to a website,

- without the user's consent. Directory traversal is when an attacker attempts to gain access to higher directories in an OS.
18. C. Of the listed answers, secure code review should happen first in the SDLC. It should be followed by fuzzing and penetration testing, in that order. Patch management is a recurring theme until the software meets the end of its life cycle.
19. B. The windows that are being displayed are most likely pop-ups. Standard pop-up blockers will prevent most of these. Antivirus software of itself does not have pop-up blocking technology but might be combined in a suite of anti-malware software that does have pop-up blocking capability. Screensavers won't affect the users' web sessions. Host-based firewalls are a good idea and will prevent attacks, but since a firewall will allow the connections that users make to websites, it cannot stop pop-ups.
20. D. Buffer overflows can be initiated by sending random data to other services on a computer. While JavaScript is commonly used in XSS attacks, it can also be used to create a buffer overflow. DoS stands for denial-of-service, which is when a computer sends many packets to a server or other important system in the hope of making that system fail. SQL and LDAP injection do not use JavaScript.
21. A. Input validation is extremely important when it comes to secure programming. To prevent SQL injection attacks, be sure that the developers have thoroughly tested the web page by validating user input. An IDS can help to detect network attacks, but is not going to help prevent SQL injection. Eliminating XSS vulnerabilities might just happen to help with all types of code injection, but you can't be sure. You should validate inputs specifically for each attack. A firewall may stop some network-based attacks, but not coded attacks.
22. B. Fuzzing (or fuzz testing) is when a person, or more commonly an automated system, enters random data into a form or application in an effort to test it. XSRF (cross-site request forgery, also abbreviated as CSRF) is an exploit of a website where unauthorized commands are issued from a trusted user. Hardening is the act of securing an operating system or application. Input validation is when forms and other web pages are checked to make sure that they will filter inputted data properly, and is used in conjunction with fuzzing.
23. D. You should employ application hardening. This means updating the application, configuring strong passwords, applying policies if necessary, and in general, configuring the settings of the application securely. Network penetration testing is when a group of tools is used to see if a host has open ports or other vulnerabilities. Input validation is when the code of a form is checked

to make sure it filters user input correctly. Application whitelisting is when only specific applications are allowed to be run, usually enforced by computer policy.

24. A. Anti-spyware can be used to trigger security alerts in case a user's web browser accesses a web page that includes a tracking cookie. Anti-spam software can possibly trigger alerts when an e-mail appears to be spam (or simply move it to a junk folder automatically). Firewalls can be configured to send alerts to security administrators, but usually they concern an IP address that attempted to gain access to the network.
25. D. This would be an example of gray-box testing. The IT auditor is not an employee of the company (which is often a requirement for white-box testing) but rather an outside consultant. Being an outside consultant, the IT auditor should not be given confidential details of the system to be tested. However, the auditor was given a real login, so the auditor cannot be employing black-box testing. Penetration testing might be occurring in this scenario as well—this is when an auditor, or other security expert, tests servers' network connections for vulnerabilities. But the scenario only states that the auditor is testing an application.
26. C. Configuration management encompasses application patch management and other ways of hardening an OS or application. Policy management is considered separate because it can be used to harden or *soften* a system; plus, it is best done at a server—affecting many systems at once. Fuzzing (or fuzz testing) is the act of providing random data to a computer program, testing it in an automated fashion. Virtualization is the term used to refer to any virtual computing platform.

Case Studies for Chapter 4

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

Case Study 4-1: Securing Web Browsers

Scenario: Your organization uses Internet Explorer version 10 as its main web browser. Your job as the security administrator is to secure Internet Explorer in as many ways as possible.

Take a look at the configuration settings for your version of IE. Write down some of the ways that IE can be secured.

(Optional) Take a look at any other browsers you might have running (Firefox, Chrome, Safari, Opera, etc.) and define the types of security they have as well.

Case Study 4-2: Whitelisting and Blacklisting Applications in a Windows Server Policy

Scenario: You have been employed as a consultant to set up a couple of policies in Windows Server. The first of these is to configure which applications can, and can't, be executed by employees.

Explain in your own words how you would accomplish your goal in Windows Server. If you have access to a Windows Server (for testing purposes), attempt to do this configuration within the operating system. If you don't, consider downloading an evaluation copy of Windows Server and loading it into a virtual machine.

Case Study Solutions

Case Study 4-1 Solution

Internet Explorer can be secured in many ways. The first thing you might do is to update to the newest version (if your organization's policy permits) and make sure that version is fully patched. Test the new version thoroughly before deployment. Otherwise, the following is a short list of some of the best ways to secure the browser:

1. Turn on automatic website checking with the phishing filter or SmartScreen filter.
2. Increase the security of the browser's "zones" such as the Internet zone.
3. Increase security for cookies.
4. Empty temporary Internet files on exit.
5. Set up whitelisting and blacklisting by configuring trusted and restricted websites.
6. (Optional) Set up a proxy connection.

Video Solution: Watch the video solution "4-1: Securing Web Browsers" on the accompanying disc.

Simulation: Complete the simulation “4-1: Securing Web Browsers.”

Case Study 4-2 Solution

Whitelisting means that you give users access to specific applications *only*—for example, Microsoft Word (winword.exe) or Internet Explorer (iexplore.exe). Blacklisting means that you deny users access to specific applications. Both of these are possible within the same Group Policy object (GPO) in Windows Server. To create this GPO and modify it correctly, it is assumed that you have promoted the Windows Server to a domain controller, and that you have created an organizational unit (OU) to work with. It also assumes that you have an MMC to use as your workspace. The video solution (4-2) shows how to create the OU. The following shows the basic steps involved with configuring the GPO:

NOTE The following solution is based on Windows Server 2008. However, Windows Server 2012 will be similar.

Step 1. Create a new policy based off the OU and add it to the MMC:

- A. Go to File > Add/Remove Snap-in. This displays the Add/Remove Snap-ins dialog box.
- B. Scroll down to Group Policy Management Editor, highlight it, and click Add. This displays the Select Group Policy Object window.
- C. In the Select Group Policy Object dialog box, click Browse.
- D. Double-click the name of the OU folder (for example, accounting.dpro3.com). Yours might differ in OU name and domain name.
- E. On the upper-right side of the window, click the middle icon, which is called Create New Group Policy Object.
- F. Click the New button. Name the policy (for purposes of this example, use acct-policy) and press Enter. Then click OK. This creates a standard policy within the Accounting OU.
- G. Click Finish in the Select Group Policy Object window and click OK in the Add or Remove Snapins window. This should add the new policy to the MMC.

Step 2. Configure the policy:

- A. Expand the acct-policy.
- B. Navigate to User Configuration > Policies > Administrative Templates > System.
- C. Double-click Don't Run Specified Windows Applications.
- D. Click the Enabled radio button.
- E. Click Show.
- F. Click Add and add an application (for example, winword.exe, the executable for Microsoft Word). Then click OK. Be sure to reset this at the end of the lab if it will affect any computers or users.
- G. Click OK for the policy's Properties window. This brings you back to the MMC. The policy will now be enabled.
- H. Double-click the Run Only Specified Windows Applications policy.
- I. Enable the policy; then click Show.
- J. Add an application by clicking the Add button, typing the name of an application (for example, excel.exe, the executable for Microsoft Excel), and clicking OK.
- K. Click OK for the policy's Properties window. This brings you back to the MMC. The policy will now be enabled.

Step 3. Save your MMC.**Step 4.** Test whether or not your new policy works by logging in to a client computer with one of the user accounts that is part of the OU.

Video Solution: Watch the video solution “4-2: Whitelisting and Blacklisting Applications with a Windows Server Policy” on the accompanying disc.



This chapter covers the following subjects:

- **Network Design:** This section discusses network design elements such as hubs, switches, and routers, and how to protect those devices from attack. It also talks about network address translation, private versus public IP addresses, and the private IP ranges. You then learn about network zones and interconnections—for example, intranets and extranets, demilitarized zones, LANs, and WANs. Finally, you learn how to defend against attacks on your virtual local area networks, IP subnets, and telephony devices.
- **Cloud Security and Server Defense:** As time moves forward, more and more organizations transfer some or all of their server and network resources to the cloud. This creates many potential hazards and vulnerabilities that must be addressed by the security administrator and by the cloud provider. Top among these concerns are the servers, where all data is stored and accessed. Servers of all types should be hardened and protected from a variety of attacks in an effort to keep the integrity of data from being compromised. However, data must also be available. And so, the security administrator must strike a balance of security and availability. In this section we'll discuss cloud-based threats as well as server vulnerabilities, and how to combat them effectively.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 1.1, 1.2, 1.3, and 4.4.

Network Design Elements

Up until now we have focused on the individual computer system. Let's expand our security perimeter to now include networks. Network design is extremely important in a secure computing environment. The elements that you include in your design can help to defend against many different types of network attacks. Being able to identify these network threats is the next step in securing your network. If you apply the strategies and defense mechanisms included in this chapter, you should be able to stave off most network-based assaults. The security of the servers and network infrastructure of an organization is the job of the security administrator, but with the inclusion of the cloud the areas of responsibility might vary. This depends on how much of the cloud is provided by a third party, and how much of the cloud is held privately within the organization's domain. Whether dealing with cloud providers, onsite cloud-based resources, locally owned servers and networks, or a mixture of all of them, the security administrator has a lot of duties and must understand not only security but how computer networking really functions. To save time and be more efficient, this chapter and the following three chapters assume that you have a working knowledge of networks and that you have the CompTIA Network+ certification or commensurate experience. Hereafter, this book will work within that mindset and will refer directly to the security side of things as it progresses. So put on your networking hat and let's begin with network design.

Foundation Topics

Network Design

Proper network design is critical for the security of your network, servers, and client computers. You need to protect your network devices so that they and the clients that they connect together will be less subject to attack. Implementing network address translation and properly employing standard private IP ranges can further protect all the computers in a standard network. A thorough knowledge of network zones—for example, local area networks and demilitarized zones—is also important when designing a secure network. Finally, by utilizing subnetworks, virtual local area networks (VLANs), network access control, and secure telephony devices, you can put the final touches on your network design.

We start with a quick review of the OSI model, which most of the topics in Chapters 5 through Chapter 8 (and beyond) relate to. This is not a full discourse on the OSI model, which is considered to be a prerequisite concept for the Security+ exam, but should help to stimulate your brain and help get you thinking from an “OSI” point of view.

The OSI Model

The Open Systems Interconnection (OSI) reference model was created and ratified by the International Organization for Standardization (ISO), and is represented in the United States by the American National Standards Institute (ANSI). This model was created to do the following:

- Explain network communications between hosts on the LAN or WAN.
- Present a categorization system for communication protocol suites (such as TCP/IP).
- Show how different protocol suites can communicate with each other.

Remember, network communications existed before the OSI model was created. This model is an abstract way of categorizing the communications that already exist. The model was devised to help engineers understand what is happening with communication protocols behind the scenes. It is broken down into seven layers, as shown in Table 5-1. They are listed numerically, which would be considered from the bottom up.

Table 5-1 OSI Model Layers

Layer #	Name	Usage	Unit of Measurement
Layer 1	Physical layer	Physical and electrical medium for data transfer.	bits
Layer 2	Data link layer	Establishes, maintains, and decides how data transfer is accomplished over the physical layer.	Frames
Layer 3	Network layer	Dedicated to routing and switching information between different hosts, networks, and internetworks.	Packets
Layer 4	Transport layer	Manages and ensures error-free transmission of messages between hosts through logical addressing and port assignment (connection-oriented). Also manages streaming connections, where n number of errors are permitted (connectionless).	Segments (TCP) Datagrams (UDP)

Layer #	Name	Usage	Unit of Measurement
Layer 5	Session layer	Governs the establishment, termination, and synchronization of sessions within the OS over the network and between hosts.	Messages
Layer 6	Presentation layer	Translates the data format from sender to receiver and provides mechanisms for code conversion, data compression, and file encryption.	Messages
Layer 7	Application layer	Where message creation begins. End-user protocols such as FTP, HTTP, and SMTP work on this layer.	Messages

NOTE The “units of measurement” in the table are also referred to as protocol data units, or PDUs.

We could fill a book on the OSI model, but again, this is a prerequisite for the Security+ exam, so it will not be covered in depth here. However, at the very least you should know the layers, their order, and their basic descriptions. In Chapter 6, “Networking Protocols and Threats,” we will apply different protocols to their respective OSI layers.

If you feel you need to brush up on the OSI model more, then consider computer networking books (for example, Network+ textbooks), online articles, and networking training classes.

NOTE For more information on the OSI model, consider one of the many CompTIA Network+ books available, or see the following links:

<http://www.cisco.com/cpress/cc/td/cpress/fund/ith/ith01gb.htm#xtocid166844>
<http://support.microsoft.com/kb/103884>

Network Devices

Let's begin with the network devices common on today's networks. Central connecting devices such as hubs and switches need to be secured and monitored; it makes sense because these devices connect all the computers on your local area network. Attacks aimed at these devices could bring down the entire LAN. And of course, routers are extremely important when interconnecting LANs and subnets. Because many routers have visible IP addresses on the Internet, you should expand your line of thinking to include the act of securing these devices from attackers that might come from outside and *inside* your network. It is more common that attackers will be situated outside your network, but you never know!

Hub

A hub is a central connecting device used in a physical star topology. It is used in Ethernet networks only. A hub is actually a simple device, connecting multiple computers together and amplifying and passing on the electrical signal. Internally, the hub just has one trunk circuit to which all the ports connect. The hub sends the data signal out to all ports. Because of this, it can be easily compromised. A mischievous person could connect a laptop to any port on the hub, or any Ethernet jack that connects to the hub, and access all network traffic with the aid of a protocol analyzer.

NOTE Protocol analyzers are also known as network sniffers, or packet sniffers. For more information on protocol analyzers, see Chapter 11, “Vulnerability and Risk Assessment.”

A hub resides on the Physical layer of the OSI model; therefore, when attempting to secure a hub, you have to think in physical, tangible terms. For example, the hub should be located in a secure area—server room, locked wiring closet, and so on. Further security precautions should be made to monitor traffic, which is covered in Chapter 12, “Monitoring and Auditing.” However, the best way to secure a hub is to remove it! Basic hubs are deprecated devices and should be replaced with a switch or other more current device. Most companies today rely on the switch instead of the hub for the bulk of their computer connections.

Switch

Ethernet switching was developed in 1996 and quickly took hold as the preferred method of networking, taking the place of deprecated devices such as hubs and

bridges. This is due to the switch's improvement in the areas of data transfer and security. Like a hub, a switch is a central connecting device to which all computers on the network connect. Again, like a hub, a switch regenerates the signal. That's where the similarity ends, however. Unlike a hub, a switch (by default) sends the signal to the correct individual computer, instead of sending it out to every port. It does this by mapping computers' MAC addresses to their corresponding physical port. This can effectively make every port an individual entity, thus securing the network, and exponentially increasing data throughput. Switches employ a matrix of copper wiring instead of the standard trunk circuit, and intelligence to pass information to the correct port. Although there are layer 1 through layer 4 switches, the type generally covered on the Security+ exam is the layer 2 switch. This switch sends information to each computer via MAC addresses.

Although the switch is by far the superior solution compared to a hub, some security implications are still involved with it. These include but are not limited to the following:

- **MAC flooding:** Switches have memory set aside to store the MAC address to the port translation table, known as the Content Addressable Memory table, or **CAM table**. A MAC flood can send numerous packets to the switch, each of which has a different source MAC address, in an attempt to use up the memory on the switch. If this is successful, the switch changes state to what is known as **fail-open mode**. At this point, the switch broadcasts data on all ports the way a hub does. This means two things: First, that network bandwidth will be dramatically reduced, and second, that a mischievous person could now use a protocol analyzer, running in promiscuous mode, to capture data from any other computer on the network. Yikes!

Key Topic

Some switches are equipped with the capability to shut down a particular port if it receives a certain amount of packets with different source MAC addresses. For example, Cisco switches use port security. This restricts a port by limiting and identifying MAC addresses of the computers permitted to access that port. A Cisco switch defines three categories of secure MAC addresses as part of a policy on the switch. Other providers have like policies that can be implemented. Other ways to secure against MAC flooding and constrain connectivity include using 802.1X-compliant devices, dynamic VLANs, and network intrusion detection systems (NIDSs), and consistently monitoring the network. We speak more to these concepts later in this chapter and in future chapters.

- **Physical tampering:** Some switches have a dedicated management port. If this is accessible, a person could perpetuate a variety of attacks on the network. Even if a single port of the switch is accessible, a person could attempt the aforementioned MAC flooding attack and move on from there. In addition, if

a person were to get physical access to the switch, that person could attempt *looping*, which is when both ends of a network cable are connected to the same switch. Some switches come with the ability to enable loop protection within the firmware, but you would rather prevent the problem from physically happening in the first place. So remember that the switch needs to be physically secured, most likely in a server room with some type of access control system. It sounds so simple, but it is commonly overlooked by many companies. Also, disable any unused ports on the switch, if the switch has that capability.

Router

A router connects two or more networks to form an internetwork. Routers are used in LANs, in WANs, and on the Internet. This device routes data from one location to another, usually by way of the IP address and IP network numbers. Routers function on the Network layer of the OSI model.

NOTE For a short primer about the OSI model and its layers, see the following link:
<http://www.davidlprowse.com/articles/?p=905>

Routers come in several forms: SOHO routers, those four-port devices used in homes and small offices to connect to the Internet; servers, which can be configured for routing if they have multiple network adapters and the proper software; and, most commonly, black-box devices such as Cisco routers. Routers are intelligent and even have their own operating system; for example, Cisco routers use IOS (Inter-network Operating System). Often, a DMZ will be set up within a router, especially SOHO router devices; we speak more about the DMZ later in this chapter.

Routers can be the victim of denial-of-service attacks, malware intrusions, and other attacks (covered in more depth later in this chapter) and can spread these attacks and malware to other sections of the network. Routers can be protected from these attacks in the following ways:

- **Secure router configuration:** Most routers are inherently insecure out-of-the-box. This means that they might have a blank default password, easily guessable username, known IP addresses, default routing tables, and so on. The first line of defense is to configure the username and password so that it is hard to guess and hard to crack. This means very complex passwords. Go through all possible default configurations and lock them down before putting the router on a live network.

- **Firewalls:** Firewalls protect against and filter out unwanted traffic. A firewall can be an individual device or can be added to a router. For example, most SOHO routers have a firewall built in, and Cisco Integrated Services Routers (ISR) include the Cisco IOS Firewall. Regular routers, and routers with firewall functionality, have the ability to block certain kinds of traffic. For example, if the ICMP protocol has been blocked, then you would not be able to ping the router. You can find more information on firewalls in Chapter 7, “Network Perimeter Security.”
- **Intrusion prevention systems (IPSs):** An IPS will not only detect but also prevent directed attacks, botnet attacks, malware, and other forms of attacks. An IPS can be installed as a network-based solution or on a particular computer and some routers. More information on network-based IPS (and IDS) solutions can be found in Chapter 7.
- **Secure VPN connectivity:** Instead of connecting directly to a router, virtual private networks enable for secure connections utilizing IPsec and SSL. Secure VPN connectivity can be implemented with SOHO routers (for smaller organizations), VPN concentrators (for larger organizations), advanced routers like ones offered by Cisco, or with a Windows Server. You can find more information about VPNs in Chapter 9, “Physical Security and Authentication Models.”
- **Content filtering:** Content filtering blocks or restricts access to certain websites. This provides protection from malicious websites. Content filtering can be installed as a server, as an appliance (for example, a web security gateway), or on some routers. You can find more information about content filters in Chapter 7.
- **Access control lists (ACLs):** Access control lists enable or deny traffic. These can be implemented on a router and within firewalls; in some cases the two will be the same physical device. For example, an ACL can be configured to deny any connections by computers that have IP addresses outside the network number. You can find more information about ACLs in Chapter 10, “Access Control Methods and Models.”

Network Address Translation, and Private Versus Public IP

Network address translation (NAT) is the process of changing an IP address while it is in transit across a router. This is usually implemented so that one larger address space (private) can be remapped to another address space, or single IP address (public). In this case it is known as network masquerading, or IP masquerading, and was originally implemented to alleviate the problem of IPv4 address exhaustion. Today, NAT provides a level of protection in IPv4 networks by hiding

a person's private internal IPv4 address—known as the *firewall effect*. Basic routers only allow for basic NAT, which is IPv4 address-translation-only. But more advanced routers allow for PAT, or **port address translation**, which translates both IPv4 addresses and port numbers. Commonly, a NAT implementation on a firewall hides an entire private network of IPv4 addresses (for example, the 192.168.1.0 network) behind a single publicly displayed IPv4 address. Many SOHO routers, servers, and more advanced routers offer this technology to protect a company's computers on the LAN. Generally, when an individual computer attempts to communicate through the router, **static NAT** is employed, meaning that the single private IPv4 address will translate to a single public IPv4 address. This is also called **one-to-one mapping**.

It is also important to know the difference between private and public addresses. A private address is one not displayed directly to the Internet and is normally behind a firewall (or NAT-enabled device). Typically these are addresses that a SOHO router or DHCP server would assign automatically to clients. A list of reserved private IPv4 ranges is shown in Table 5-2. Public addresses are addresses displayed directly to the Internet; they are addresses that anyone can possibly connect to around the world. Most addresses besides the private ones listed in Table 5-2 are considered public addresses. Figure 5-1 shows an example of a router/firewall implementing NAT. The router's public address is 207.172.15.50, and its private address is 10.0.0.1. Computers to the left of the router are on the LAN, and all their IP addresses are private, protected by NAT, which occurs at the router. Servers on the Internet (within the cloud) have public IPv4 addresses (for example, 208.96.234.193) so that they can be accessed by anyone on the Internet.

Key Topic**Table 5-2** Private IPv4 Ranges (as Assigned by the IANA)

IP Class	Assigned Range
Class A	10.0.0.0–10.255.255.255
Class B	172.16.0.0–172.31.255.255
Class C	192.168.0.0–192.168.255.255

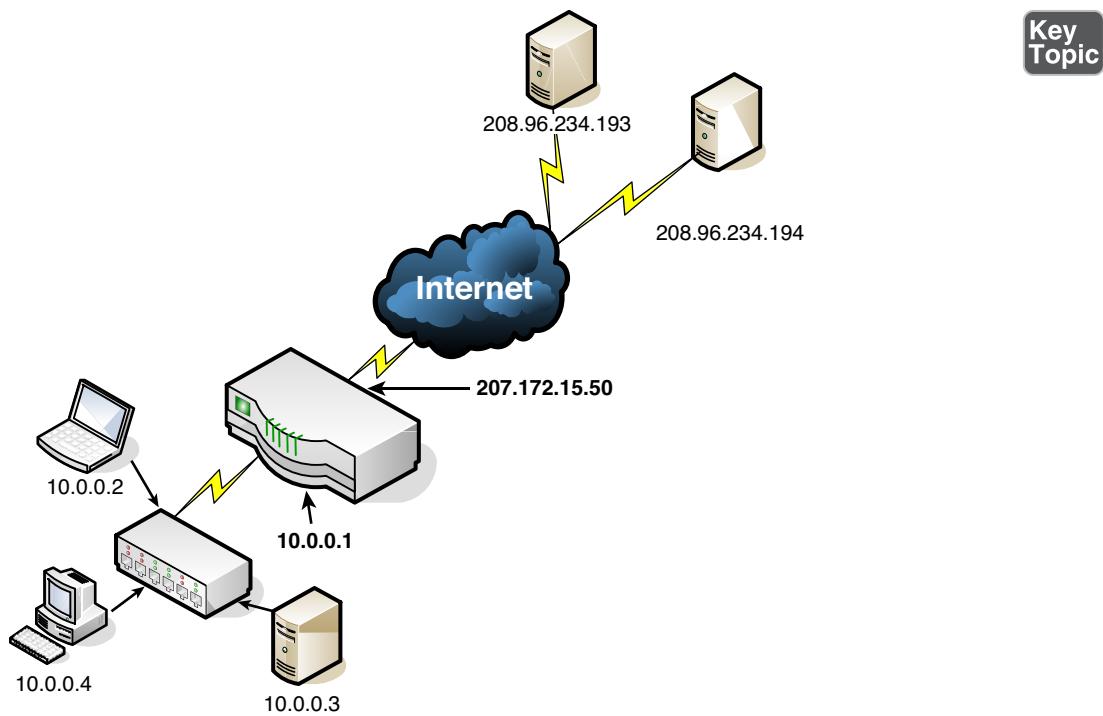


Figure 5-1 Example of Public and Private IPv4 Addresses

You should also know the categories of IPv6 addresses. Table 5-3 provides a review of these types. Keep in mind that the standard “private” range for IPv6 is FE80::/10, which spans addresses that start with FE80, FE90, FEA0, and FEB0. This is the default reserved range of IPv6 addresses that computers on a LAN (and behind a firewall) will be assigned from.

Table 5-3 Types of IPv6 Addresses

IPv6 Type	Address Range	Purpose
Unicast	Global unicast starts at 2000 Link-local ::1 and FE80::/10	Address assigned to one interface of one host.
Anycast	Structured like unicast addresses	Address assigned to a group of interfaces on multiple nodes. Packets are delivered to the “first” interface only.
Multicast	FF00::/8	Address assigned to a group of interfaces on multiple nodes. Packets are delivered to all interfaces.

There are risks involved with IPv6 auto-configured addresses. Once a computer is physically connected to a network, it can easily obtain an IPv6 address without any user interaction and begin communicating with other hosts on the network, perhaps in an insecure manner. To avoid this, consider using 802.1X authentication, which stops IPv6 traffic until the host is authenticated to the network. You can read more on 802.1X in Chapter 9. Also, consider using encrypted tunnels, and network adapters that are certified for secure wired and/or wireless transmissions.

A last word about IP security—Both IPv4 and IPv6 have security issues, and both have various ways that they can be secured. Don't be fooled; both types of IP networks need to be designed with security in mind. For example, IPv6 has IPsec support built in, but that might not be the best method of security for your organization. IPv4 also can make use of IPsec, and in that aspect can be just as secure as IPv6, but the support isn't built in, so you might choose to implement alternative security methods for IPv4. Many networks use both protocols, and though one is working in a secure manner, that doesn't mean the other protocol is protected. Remember to design both types of IP networks to address all security concerns, and test them thoroughly on multiple platforms.

Network Zones and Interconnections

When designing your network, think about all the pieces of the network and all the connections your network might make to other networks. Are you in charge of a single local area network? Or are you responsible for more than one local area network that perhaps form a wide area network? What kind of, and how many Internet connections do you have? Will you have servers that need to be accessed by users on the Internet? Is the cloud or virtualization involved? And will you need to share information with company employees that work from home or with other organizations, while securing that information from the average user on the Internet? The more interconnections and network zones that you have, the more security risk you are taking on. Keep this in mind as you read through the section.

LAN Versus WAN

A local area network, or LAN, is a group of networked computers contained in a small space such as a small office, a school, or one or two close-knit buildings. Generally, the computers in the LAN are all assigned private IP addresses and are behind a firewall. Although computers on a LAN do not have to connect to the Internet, they usually do, but do so via a router that acts as an IP proxy and employs NAT. (NAT is far more common on IPv4 networks, but not unheard of on IPv6 networks.) It is important to secure computers on the LAN by placing them behind

the router, assigning private IP addresses if necessary, and verifying that anti-malware programs are installed.

A wide area network, or WAN, is one or more LANs connected together. The big difference between a LAN and a WAN is that a WAN covers a larger geographic area. This implies that the services of a telecommunications or data communications provider are necessary. The security implications of a WAN are great; the more connections your network has, the more likely attacks will become. All connections should be monitored and firewalled if possible. Consider that there might be connections to other states or countries...and, to the biggest WAN of them all—the Internet.

Internet

The Internet is the worldwide interconnection of individual computers and computer networks. Because it is a public arena, anyone on the Internet can possibly be a target, or an attacker. All types of sessions on the Internet should be protected at all times. For example, voice calls should be done within a protected VoIP system; data sessions should be protected by being run within a virtual private network; and so on. Individual computers should be protected by firewalls and anti-malware programs. Networks should be protected by firewalls as well. But what about systems that need to access the LAN and also need to be accessed by clients on the Internet? Well, one option is to create an area that is not quite the LAN, and not quite the Internet; this is a demilitarized zone, or DMZ.

Demilitarized Zone (DMZ)

When talking about computer security, a **demilitarized zone (DMZ)** is a special area of the network (sometimes loosely referred to as a subnetwork) that houses servers that host information accessed by clients or other networks on the Internet. Some of these servers might include web, FTP, mail, and database computers. It's important that each server is configured with the proper default gateway IP address so that users on the Internet can access it. These servers might also be accessible to clients on the LAN in addition to serving the Internet. There are several ways to set up a DMZ; a common way is the **3-leg perimeter** DMZ, as shown in Figure 5-2. Notice the third “leg” that branches off the firewall to the right. This leads to a special switch that has WWW and FTP servers connected to it. Also note that the DMZ is on a different IP network than the LAN, although both the LAN and DMZ are private IP network numbers.

Key Topic

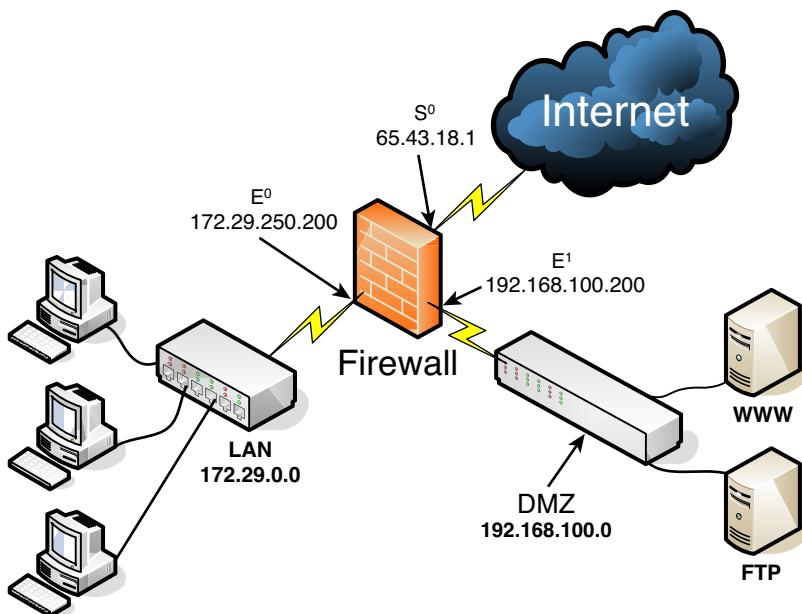


Figure 5-2 3-Leg Perimeter DMZ

The firewall can (and usually will) be configured in a secure fashion on the DMZ connection (192.168.100.200) and an even more secure fashion on the LAN connection (172.29.250.200). The DMZ connection in Figure 5-2 needs to have only inbound ports 80 (WWW) and 21 (FTP) open; all other ports can be closed, thus filtering inbound traffic. The LAN connection can be completely shielded on the inbound side. Although DMZs can be created logically, they are most often found as physical implementations. There are several other implementations of a DMZ. For example, a DMZ can be set up with two firewalls that surround it, also known as a **back-to-back perimeter** network configuration; in this case the DMZ would be located between the LAN and the Internet. A DMZ might also be set up within a router, especially in small organizations that use basic SOHO router devices. It all depends on the network architecture and security concerns of the organization.

Intranets and Extranets

Intranets and extranets are implemented so that a company (or companies) can share its data using all the features and benefits of the Internet, while keeping that data secure within the organization, select organizations, and specific users. In the case of an intranet, only one company is involved; it could be as simple as an internal company website, or a more advanced architecture of servers, operational systems, and networks that deploy tools, applications, and of course data. In the case of an

extranet, multiple companies can be involved, or an organization can opt to share its data and resources with users that are not part of the organization(s). This sharing is done via the Internet, but again, is secured so that only particular people and organizations can connect.

Whether you have an intranet or an extranet, security is a major concern. Proper authentication schemes should be implemented to ensure that only the appropriate users can access data and resources. Only certain types of information should be stored on an intranet or extranet. Confidential, secret, and top secret information should not be hosted within an intranet or extranet. Finally, the deployment of a firewall(s) should be thoroughly planned out in advance. An example of a company that hosts an intranet and an extranet is shown in Figure 5-3. Note that data computers from Company A can access the intranet because they work for the company. Also note that Company B can access the extranet, but not the intranet. In this example, the company (Company A) has created two DMZs, one for its intranet and one for its extranet. Of course, it is possible to set this up using only one DMZ, but the access control lists on the firewall and other devices would have to be planned and monitored more carefully. If possible, separating the data into two distinct physical locations will have several benefits, namely, being more secure; although, it will cost more money to do so. This all depends on the acceptable risk level of the organization and its budget!

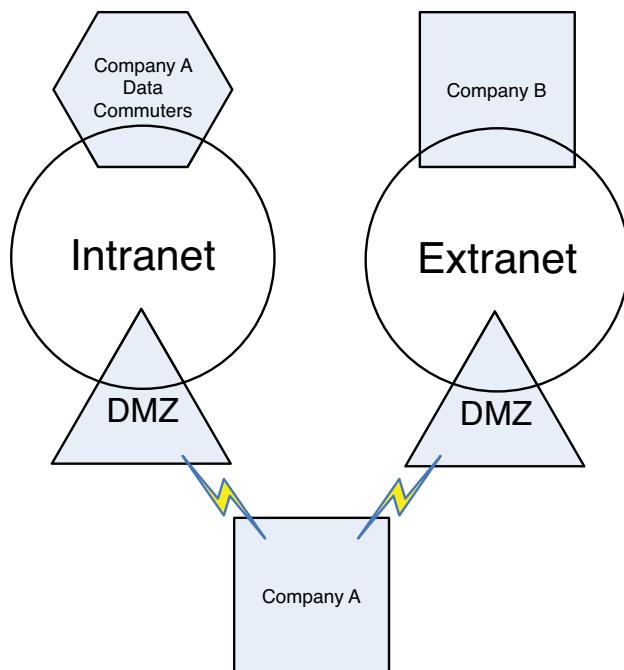


Figure 5-3 Example of an Intranet and Extranet

Network Access Control (NAC)

In this chapter, we have mentioned several types of networking technologies and design elements. But whichever you choose to use, it needs to be controlled in a secure fashion. **Network access control (NAC)** does this by setting the rules by which connections to a network are governed. Computers attempting to connect to a network are denied access unless they comply with rules pertaining to levels of antivirus protection, system updates, and so on...effectively weeding out those who would perpetuate malicious attacks. The client computer continues to be denied until it has been properly updated, which in some cases can be taken care of by the NAC solution automatically. This often requires some kind of preinstalled software (an agent) on the client computer, or the computer is scanned by the NAC solution remotely.

Some companies (such as Cisco) offer hardware-based NAC solutions, whereas other organizations offer software-based NAC solutions such as FreeNAC (<http://freenac.net/>) or PacketFence (www.packetfence.org), which are both open source.

The IEEE 802.1X standard, known as port-based network access control, or PNAC, is a basic form of NAC that enables the establishment of authenticated point-to-point connections, but NAC has grown to include software; 802.1X is now considered a subset of NAC. See the section “Authentication Models and Components” in Chapter 9 for more information about IEEE 802.1X.

Subnetting

Subnetting is the act of creating subnetworks logically through the manipulation of IP addresses. These subnetworks are distinct portions of a single IP network.

Subnetting is implemented for a few reasons:

- It increases security by compartmentalizing the network.
- It is a more efficient use of IP address space.
- It reduces broadcast traffic and collisions.

To illustrate the first bullet point, examine Figure 5-4. This shows a simple diagram of two subnets within the 192.168.50.0 IPv4 network using the subnet mask 255.255.255.240; this would also be known as 192.168.50.0/28 in CIDR notation (covered shortly). You can see that the subnets are divided; this implies that traffic is isolated—it cannot travel from one subnet to another without a route set up specifically for that purpose. So, computers within Subnet ID 2 can communicate with each other by default, and computers within Subnet ID 8 can communicate with each other, but computers on Subnet 2 *cannot* communicate with computers on Subnet 8, and vice versa.

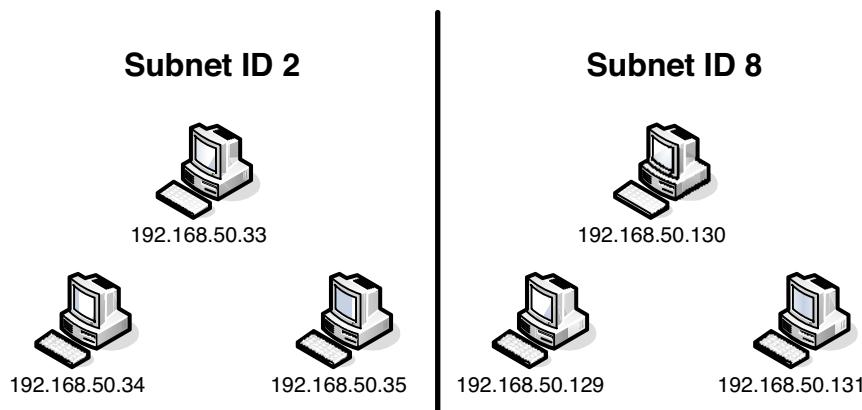


Figure 5-4 Example of a Subnetted Network

As a security precaution, using subnet 0 (zero) is discouraged, and instead a network administrator should start with subnet 1, which in the preceding example would be 192.168.50.16. This avoids any possible confusion regarding the actual network number (192.168.50.0) and its subnets. If a network administrator were to use the first subnet and then inadvertently use a default subnet mask (such as 255.255.255.0), this would create a security vulnerability—the hosts on that subnet would have access to more of the network than they normally should. This kind of mistake is common when using the first subnet and is the main reason it is discouraged.

Another common example of an organization subnetting its network is to take what would normally be a Class A network (with the 255.0.0.0 subnet mask) and make it classless by changing the subnet mask to, for example, 255.255.255.224. This is also referred to as *classless interdomain routing*, or CIDR. For instance, we could use 10.7.7.0 as the network number. Normally, it would simply be referred to as the 10 network if it was Class A. But the subnet mask 255.255.255.224 makes it *function* as a subnetted Class C network, which effectively makes it classless. In CIDR notation this would be written out as 10.7.7.0/27, because there are 27 masked bits in the subnet mask. The subnet mask's "224" is the key. When we calculate this, we find that we can have 30 usable hosts per subnet on the 10.7.7.0 network. The first range of hosts would be 10.7.7.1–10.7.7.30, the second range would be 10.7.7.33–10.7.7.62, and so on. A host with the IP address 10.7.7.38 would not be able to communicate (by default) with a host using the IP address 10.7.7.15 because they are on two separate subnets.

NOTE You can check the preceding statements by searching for and using a free online *subnetting calculator*. I highly recommend you practice this!

When compartmentalizing the network through subnetting, an organization's departments can be assigned to individual subnets, and varying degrees of security policies can be associated with each subnet. Incidents and attacks are normally isolated to the subnet that they occur on. Any router that makes the logical connections for subnets should have its firmware updated regularly, and traffic should be occasionally monitored to verify that it is isolated.

Virtual Local Area Network (VLAN)

A VLAN is implemented to segment the network, reduce collisions, organize the network, boost performance, and, hopefully, increase security. A device such as a switch can control the VLAN. Like subnetting, a VLAN compartmentalizes the network and can isolate traffic. But unlike subnetting, a VLAN can be set up in a physical manner; an example of this would be the port-based VLAN, as shown in Figure 5-5. In this example, each group of computers such as Classroom 1 has its own VLAN; however, computers in the VLAN can be located anywhere on the *physical* network. For example, Staff computers could be located in several physical areas in the building, but regardless of where they are located, they are associated with the Staff VLAN because of the physical port they connect to. Due to this, it is important to place physical network jacks in secure locations for VLANs that have access to confidential data.

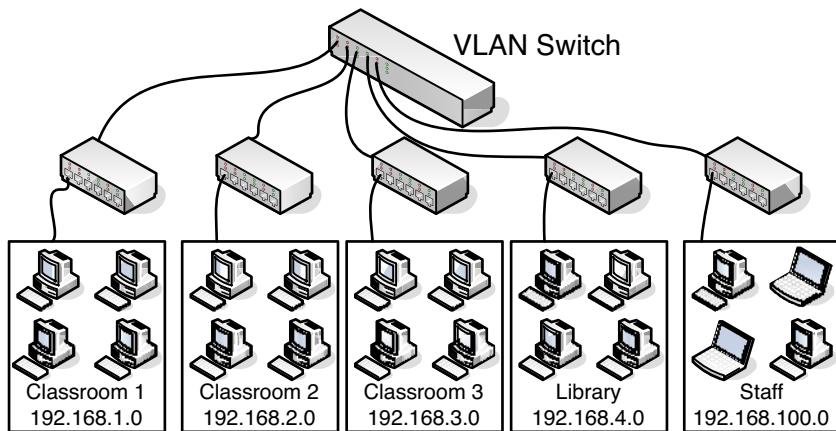


Figure 5-5 Example of a VLAN

There are also logical types of VLANs, such as the protocol-based VLAN and the MAC address-based VLAN, that have a whole separate set of security precautions, but those precautions go beyond the scope of the CompTIA Security+ exam.

The most common standard associated with VLANs is IEEE 802.1Q, which modifies Ethernet frames by “tagging” them with the appropriate VLAN information, based on which VLAN the Ethernet frame should be directed to.

VLANs restrict access to network resources, but this can be bypassed through the use of **VLAN hopping**. VLAN hopping can be divided into two categories, as shown in Table 5-4.

Table 5-4 Types of VLAN Hopping

Key Topic

VLAN Hopping	Method	How It Works	How to Defend
Switch spoofing	Switch spoofing	The attacking computer must be capable of speaking the tagging and trunking protocols used by the VLAN trunking switch to imitate the switch. If successful, traffic for one or more VLANs is then accessible to the attacking computer.	Put unplugged ports on the switch into an unused VLAN. Configure the switch ports in charge of passing tagged frames to be trunks and to explicitly forward specific tags. Avoid using default VLAN names such as VLAN or VLAN1.
Double tagging	Double tagging	In a double-tagging attack, an attacking host attaches two VLAN tags to the frames it transmits. The first, proper header is stripped off by the first switch the frame encounters, and the frame is then forwarded. The second, false header is then visible to the second switch that the frame encounters.	Upgrade firmware or software. Pick an unused VLAN as the default VLAN (also known as a native VLAN) for all trunks, and do not use it for any other intent. Consider redesigning the VLAN if multiple 802.1Q switches are used.

MAC flooding attacks can also be perpetuated on a VLAN, but because the flood of packets will be constrained to an individual VLAN, VLAN hopping will not be possible as a result of a MAC flood.

VLANs can also be the victims of ARP attacks, brute-force attacks, spanning-tree attacks, and other attacks, all of which we discuss in later chapters.

NOTE So far, the virtual LANs we have discussed use physical switches to make the connectivity between computers. However, in a completely virtualized environment—one where all of the operating systems are virtual—it is possible to use a virtual switch to connect the systems together. In this case, everything is virtual, from the servers to the network infrastructure. It is often used in testing environments, and gives new meaning to the term “virtual LAN.”

Telephony Devices

Telephony aims at providing voice communication for your users and requires various equipment to accomplish this goal. Older devices such as modems can be the victim of an attack, but nowadays computers are also heavily involved in telephony; this is known as computer telephony integration, or CTI. What does this mean for you, the security administrator? Well, for one thing, special telephones and servers require particular security, for a whole new level of attacks and ways of targeting this equipment. The telephone, regardless of what type, is still one of the primary communication methods and therefore needs to be up and running all the time.

Modems

In networking environments such as a network operations center (NOC) or server room, modems are still used by network administrators to connect to servers and networking equipment via dial-up lines. Often, this is a redundant, worst-case scenario implementation—sometimes, it is the default way for admins to access and configure their networking equipment. In some cases, this is done without any authentication, and to make matters worse, sometimes admins use Telnet to configure their equipment. Of course, this is insecure, to say the least. A modem can be the victim of **war-dialing**, which is the act of scanning telephone numbers by dialing them one at a time. Computers usually pick up on the first ring, and the war-dialing system makes a note of that and adds that number to the list. Besides the obvious social annoyance this could create, a hacker would then use the list to attempt to access computer networks. Now think back to the system that has no authentication scheme in place!

So to protect modem connections, a network admin should 1) use the callback feature in the modem software and set it to call the person back at a preset phone number; 2) use some type of username/password authentication scheme and select only strong passwords because war-dialers will most likely try at password guessing; and 3) use dial-up modems sparingly, only in secure locations, and try to keep the modem's phone number secret. And by the way, a quick word on Telnet; it is not secure and should be substituted with SSH or another, more secure way of configuring a remote device.

For the typical user who still uses a modem on a client computer, set the modem to not answer incoming calls, and be sure not to use any remote control software on the system that houses the modem. Finally, consider upgrading to a faster and more secure Internet access solution!

PBX Equipment

A private branch exchange (PBX) makes all of an organization's internal phone connections and also provides connectivity to the public switched telephone network (PSTN). Originally, PBXs were simple devices, but as time progressed they incorporated many new features and along the way became more of a security concern. For example, a hacker might attempt to exploit a PBX to obtain free long distance service or to employ social engineering to obtain information from people at the organization that owns the PBX. To secure a standard PBX, make sure it is in a secure room (server room, locked wiring closet, and so on); usually it should be mounted to the wall but could be fixed to the floor as well. Also, change passwords regularly, and only allow authorized maintenance; log any authorized maintenance done as well. PBX computers often have a remote port (basically a built-in modem or other device) for monitoring and maintenance; ensure that this port is not exploited and that only authorized personnel know how to access it. Today's PBX devices might act as computer-telephony integration servers on the network, and/or might incorporate VoIP, which is also known as an IP-PBX.

VoIP

Voice over Internet Protocol (VoIP) is a broad term that deals with the transmission of voice data over IP networks such as the Internet. It is used by organizations and in homes. In an organization, IP phones can be the victim of attacks much like individual computers can. In addition, VoIP servers can be exploited the same way that other servers can; for example, by way of denial-of-service attacks. When securing VoIP servers, security administrators should implement many of the same precautions that they would make for more traditional servers, such as file servers and FTP servers. Some VoIP solutions, especially for home use, use the Session Initiation Protocol (SIP), which can be exploited by man-in-the-middle (MITM) attacks. To help reduce risk, VoIP systems should be updated regularly and use encryption and an authentication scheme.

Another concern with VoIP is *availability*. If there are multiple types of network traffic competing for bandwidth, you could use the Quality of Service (QoS) configuration to prioritize traffic on a router, and to ultimately increase the availability of IP telephony. We could talk about VoIP for days, but luckily for you, the exam requires that you have only a basic understanding of what VoIP is and how to protect it in a general sense. Most of the ways that you will mitigate risk on a VoIP system are the same as you would for other server systems, and these are covered later in this chapter as well as in Chapter 6.

Cloud Security and Server Defense

Until recently, the “cloud” was just a name for the Internet—anything beyond your network that you as a user couldn’t see. Technically speaking, the cloud was the area of the telephone company’s infrastructure—it was everything between one organization’s demarcation point, and the demarcation point of another organization. It included central offices, switching offices, telephone poles, circuit switching devices, packet assemblers/disassemblers (PADs) packet switching exchanges (PSEs), and so on. In fact, all these things, and much more, are still part of the “cloud,” in the technical sense. Back in the day, this term was used only by telecommunications professionals and network engineers.

Now, the “cloud” has taken on a whole new meaning. Almost everyone has heard of it and probably used it to some extent. It is used heavily in marketing, and the meaning is less technical and more service-oriented than it used to be. It takes the place of most intranets and extranets that had existed for decades before its emergence.

We talked about basic computer protection in Chapter 2, “Computer Systems Security,” the hardening of operating systems (including virtual operating systems) in Chapter 3, “OS Hardening and Virtualization,” and secure programming in Chapter 4, “Application Security.” In this section we’ll build on those knowledge sets and describe some server defense. I place servers in this section of the chapter because they are at the heart of networking. Servers control the sending and receiving of all kinds of data over the network, including FTP and websites, e-mail and text messaging, and data stored as single files and in database format. A great many of these servers are now in the cloud, with more moving there every day. And the cloud, however an organization connects to it, is all about networking. So the cloud, virtualization, and servers in general are all thoroughly intertwined.

Cloud Computing

Cloud computing can be defined as a way of offering on-demand services that extend the capabilities of a person’s computer or an organization’s network. These might be free services, such as browser-based e-mail from providers such as Yahoo! and Gmail, or they could be offered on a pay-per-use basis, such as services that offer data access, data storage, infrastructure, and online gaming. A network connection of some sort is required to make the connection to the “cloud” and gain access to these services in real time.

Some of the benefits to an organization using cloud-based services include lowered cost, less administration and maintenance, more reliability, increased scalability, and possible increased performance. A basic example of a cloud-based service would be browser-based e-mail. A small business with few employees definitely needs e-mail, but it can’t afford the costs of an e-mail server and perhaps does not want to have its

own hosted domain and the costs and work that go along with that. By connecting to a free web browser-based service, the small business can obtain near unlimited e-mail, contacts, and calendar solutions. But, there is no administrative control, and some security concerns, which we discuss in just a little bit.

Cloud computing services are generally broken down into three categories of services:

- **Software as a service (SaaS):** The most commonly used and recognized of the three categories, SaaS is when users access applications over the Internet that are provided by a third party. The applications need not be installed on the local computer. In many cases these applications are run within a web browser; in other cases the user connects with screen sharing programs or remote desktop programs. A common example of this is webmail.
- **Infrastructure as a service (IaaS):** A service that offers computer networking, storage, load balancing, routing, and VM hosting. More and more organizations are seeing the benefits of offloading some of their networking infrastructure to the cloud.
- **Platform as a service (PaaS):** A service that provides various software solutions to organizations, especially the ability to develop applications in a virtual environment without the cost or administration of a physical platform. PaaS is used for easy-to-configure operating systems and on-demand computing. Often, this utilizes IaaS as well for an underlying infrastructure to the platform.

Between 2005 and 2010, cloud services were slow to be adopted by organizations. One of the reasons for this is the inherent security issues that present themselves when an organization delegates its software, platforms, and especially infrastructure to a cloud-based service provider. After 2010, however, implementation of cloud services has grown dramatically, with most companies either already running cloud services or in the planning stages.

There are different types of clouds used by organizations: public, private hybrid, and community. Let's discuss each briefly.

- **Public cloud:** When a service provider offers applications and storage space to the general public over the Internet. A couple of examples of this include free, web-based e-mail services, and pay-as-you-go business-class services. The main benefits of this include low (or zero) cost and scalability. Providers of public cloud space include Google, Rackspace, and Amazon.
- **Private cloud:** Designed for a particular organization in mind. The security administrator has more control over the data and infrastructure. A limited number of people have access to the cloud, and they are usually located behind a firewall of some sort in order to gain access to the private cloud. Resources

might be provided by a third party, or could come from the security administrator's server room or data center.

- **Hybrid cloud:** A mixture of public and private clouds. Dedicated servers located within the organization and cloud servers from a third party are used together to form the collective network. In these hybrid scenarios, confidential data is usually kept in-house.
- **Community cloud:** Another mix of public and private, but one where multiple organizations can share the public portion. Community clouds appeal to organizations that usually have a common form of computing and storing of data.

The type of cloud an organization uses will be dictated by its budget, the level of security it requires, and the amount of manpower (or lack thereof) it has to administer its resources. While a private cloud can be very appealing, it is often beyond the ability of an organization, forcing that organization to seek the public or community-based cloud. However, it doesn't matter what type of cloud is used. Resources still have to be secured by someone, and you'll have a hand in that security one way or the other.

Cloud Security

Cloud security hinges on the level of control a security administrator retains and the types of security controls the admin implements. When an organization makes a decision to use cloud computing, probably the most important security control concern to administrators is the loss of physical control of the organization's data. A more in-depth list of cloud computing security concerns includes lack of privacy, lack of accountability, improper authentication, lack of administrative control, data sensitivity and integrity problems, data segregation issues, location of data and data recovery problems, malicious insider attack, bug exploitation, lack of investigative support when there is a problem, and finally, questionable long-term viability. In general, everything that you worry about for your local network and computers! Let's also mention that cloud service providers can be abused as well—attackers often attempt to use providers' infrastructure to launch powerful attacks.

Solutions to these security issues include the following:

- **Complex passwords:** Strong passwords are beyond important; they are critical, as I will mention many times in this text. As of the writing of this book (2014), accepted password schemes include the following:
 - **For general security:** 10 characters minimum, including at least one capital letter, one number, and one special character
 - **For confidential data:** 15 characters minimum, including a minimum two each of capital letters, numbers, and special characters

When it comes to the cloud, a security administrator might just opt to use the second option for every type of cloud. The reasoning is that public clouds can be insecure (you just don't know), and private clouds will most likely house the most confidential data. To enforce the type of passwords you want your users to choose, a strong server-based policy is recommended.

- **Powerful authentication methods:** Passwords are all well and good, but how the person is authenticated will prove to be just as important. Multifactor authentication can offer a certain amount of defense in depth. In this scenario, if one form of authentication is compromised, the other works as a backup. For example, in addition to a password, a person might be asked for biometric confirmation such as a thumbprint or voice authorization, for an additional PIN, or to swipe a smart card. Multifactor authentication may or may not be physically possible, depending on the cloud environment being used, but if at all possible, it should be considered.
- **Strong cloud data access policies:** We're talking the who, what, and when. When it comes to public clouds especially, you should specifically define which users have access, exactly which resources they have access to, and when they are allowed to access those resources. Configure policies from servers that govern the users; for example, use Group Policy objects on a Windows Server domain controller.
- **Encryption:** Encryption of individual data files, whole disk encryption, digitally signed virtual machine files...the list goes on. Perhaps the most important is a robust public key infrastructure (PKI), which we discuss further in Chapter 14, "PKI and Encryption Protocols." That is because many users will access data through a web browser.
- **Standardization of programming:** The way applications are planned, designed, programmed, and run on the cloud should all be standardized from one platform to the next, and from one programmer to the next. Most important is standardized testing in the form of input validation, fuzzing, and white-, gray-, or black-box testing.
- **Protection of *all* the data!:** This includes storage area networks (SANs), general cloud storage, and the handling of big data (for example, astronomical data). When data is stored in multiple locations, it is easy for some to slip through the cracks. Detailed documentation of what is stored where (and how it is secured) should be kept and updated periodically. As a top-notch security admin, you don't want your data to be tampered with. So, implementing some cloud-based security controls can be very helpful. For example, consider the following: deterrent controls (prevent the tampering of data), preventive controls (increase the security strength of a system that houses data), corrective controls (reduce the effects of data tampering that has occurred), and detective controls (detect attacks in real time, and have a defense plan that can be immediately carried out).

NOTE We'll discuss security controls in more depth in Chapter 11.

What else are we trying to protect here? We're concerned with protecting the identity and privacy of our users (especially executives because they are high-profile targets). We need to secure the privacy of credit card numbers and other super-confidential information. We want to secure physical servers that are part of our server room or data center, because they might be part of our private cloud. We desire protection of our applications with testing and acceptance procedures. (Keep in mind that these things all need to be done within contractual obligations with any third-party cloud providers.) And finally, we're interested in promoting the availability of our data. After all of our security controls and methods have been implemented, we might find that we have locked out more people than first intended. So our design plan should contain details that will allow for available data, but in a secure manner.

Customers considering using cloud computing services should ask for transparency—or detailed information about the provider's security. The provider must be in compliance with the organization's security policies; otherwise, the data and software in the cloud becomes far less secure than the data and software within the customer's own network.

Other “Cloud”-based Concerns

There are other technologies to watch out for that are loosely connected with what we call cloud technologies. One example is social media. Social media environments can include websites as well as special applications that are loaded directly on to the computer (mobile or desktop), among other ways to connect, both legitimate and illegitimate. People share the darndest things on social media websites, which can easily compromise the security of employees and data. The point? There are several ways to access social media platforms, and it can be difficult for a security administrator to find every website, application, service, and port that is used by social media. In cases such as these, an admin might consider more whitelisting of applications, so that users are better locked down.

Another thing to watch for is P2P networks. File sharing, gaming, media streaming, and all the world is apparently available to a user—if the user knows where to look. However, P2P often comes with a price: malware and potential system infiltration. By the latter I mean that computers can become unwilling participants in the sharing of data on a P2P network. This is one example in which the cloud invades client

computers, often without the user's consent. Access to file sharing, P2P, and torrents also needs a permanent "padlock."

Then there's the darknet. Where Batman stores his data... No, a darknet is another type of P2P (often referred to as an F2F, meaning friends to friends) that creates connections between trusted peers (unlike most other P2Ps), but uses nonstandard ports and protocols. This makes it a bit more difficult to detect. Darknets are often the safe haven of illegal activities because they are designed specifically to resist surveillance. Computers that are part of an admin's network, and more often, virtual machines in the admin's cloud, can be part of these darknets, and can easily go undetected by the admin. In some cases, an employee of the organization (or an employee of the cloud provider) might have configured some cloud-based resources to join a darknet. This can have devastating legal consequences if illegal activities are traced to your organization. Thorough checks of cloud-based resources can help to prevent this. Also, screening of employees, careful inspection of service-level agreements with cloud providers, and the use of third-party IT auditors can avoid the possibility of darknet connectivity, P2P links, and improper use of social media.

Server Defense

Now we come down to it. Servers are the cornerstone of data. They store it, transfer it, archive it, and allow or disallow access to it. They need super-fast network connections that are monitored and baselined regularly. They require an admin to configure policies, check logs, and perform audits frequently. They exist in networks both large and small, within public and private clouds, and are often present in virtual fashion. What it all comes down to is that servers contain the data and the services that everyone relies on. So they are effectively the most important things to secure on your network.

Let's break down five types of servers that are of great importance (in no particular order), and talk about some of the threats and vulnerabilities to those servers, and ways to protect them.

File Servers

File server computers store, transfer, migrate, synchronize, and archive files. Really any computer can act as a file server of sorts, but examples of actual server software include Microsoft Server, OS X Server, and the various types of Linux server versions (for example, Ubuntu Server 12.04 or Red Hat Server), not to mention Unix. File servers are vulnerable to the same types of attacks and malware that typical desktop computers are. To secure file servers (and the rest of the servers on this list), employ hardening, updating, anti-malware applications, software-based firewalls,

hardware-based intrusion detection systems (HIDSs), and encryption, and be sure to monitor the server regularly.

Network Controllers

A network controller is a server that acts as a central repository of user accounts and computer accounts on the network. All users log in to this server. An example of this would be a Windows Server 2012 system that has been promoted to a domain controller (runs Active Directory). In addition to the attacks mentioned for file servers, a domain controller can be the victim of LDAP injection. It also has Kerberos vulnerabilities, which can ultimately result in privilege escalation or spoofing. As mentioned in Chapter 4, LDAP injection can be prevented with proper input validation. But in the specific case of a Windows domain controller, really the only way to keep it protected (aside from the preventive measures mentioned for file servers) is to install specific security update hot patches for the OS, even if the latest service pack has been installed. This also applies to Kerberos vulnerabilities.

NOTE An example of a Microsoft Security Bulletin addressing vulnerabilities in Kerberos can be found at the following link. You can see that even with the latest service pack, a server can still be vulnerable.

<http://technet.microsoft.com/en-us/security/bulletin/ms11-013>

E-mail Servers

E-mail servers are part of the message server family. When we make reference to a message server, we mean any server that deals with e-mail, faxing, texting, chatting, and so on. But for this section we'll concentrate strictly on the e-mail server. The most common of these is Microsoft Exchange. An Exchange Server might run POP3, SMTP, and IMAP, and allow for Outlook Web App (OWA) connections via a web browser. That's a lot of protocols and ports running. So it's not surprising to hear some Exchange admins confess that running an e-mail server can be difficult at times, particularly because it is vulnerable to XSS attacks, overflows, DoS attacks, SMTP memory exploits, directory traversal attacks, and of course spam. Bottom line, it has to be patched... a lot. An admin needs to keep on top of the latest attacks, and possibly be prepared to shut down or quarantine an e-mail server at a moment's notice. New attacks and exploits are constantly surfacing because e-mail servers are a common and big target with a large attack surface. For spam, a hardware-based spam filter is most effective (such as one from Barracuda), but software-based filters can also help. Thinking a little outside of the box, an admin could consider moving away from Microsoft (which is the victim of the most attacks) and toward

a Linux solution such as the Java-based SMTP server built into Apache, or with a third-party tool such as Zimbra (or one of many others). These solutions are not foolproof, and still need to be updated, but it is a well-known fact that historically Linux has not been attacked as often as Microsoft (in general), though the difference between the two in the number of attacks experienced has shrunk considerably since the turn of the millennium.

Web Servers

The web server could be the most commonly attacked server of them all. Examples of web servers include Microsoft's Internet Information Services (IIS), Apache HTTP Server (Linux), lighttpd (FreeBSD), Oracle iPlanet Web Server (Oracle), and iPlanet's predecessor Sun Java System Web Server (Sun Microsystems). Web servers in general can be the victim of DoS attacks, overflows, XSS and XSRF, remote code execution, and various attacks that make use of backdoors. For example, in IIS, if basic authentication is enabled, a backdoor could be created, and attackers could ultimately bypass access restrictions. An IIS admin must keep up to date with the latest vulnerabilities by reading Microsoft Security Bulletins, such as this one which addresses possible information disclosure:

<https://technet.microsoft.com/en-us/security/bulletin/ms12-073>

NOTE For more information about vulnerabilities to IIS (and other Microsoft software), visit the Security TechCenter at the following link:

<http://technet.microsoft.com/en-US/security/bb291012>

In general, a security administrator should keep up to date with **Common Vulnerabilities and Exposures (CVE)** as maintained by Mitre (<http://cve.mitre.org/>). The latest CVE listings for applications and operating systems can be found at several websites such as CVE Details.

Aside from the usual programmatic solutions to vulnerabilities such as XSS (discussed in Chapter 4), and standard updating and hot patching, a security admin might consider adding and configuring a hardware-based firewall from Cisco, Juniper, Check Point, or other similar company. And of course, HTTPS (be it SSL or, better yet, TLS) can be beneficial if the scenario calls for it. Once a server is secured, you can prove the relative security of the system to users by using an automated vulnerability scanning program (such as Netcraft) that leaves a little image on the web pages that states whether or not the site is secure and when it was scanned or audited.

Apache can be the casualty of many attacks as well, including privilege escalation, code injection, and exploits to the proxy portion of the software. PHP forms and the PHP engine could act as gateways to the Apache web server. Patches to known CVEs should be applied ASAP.

NOTE A list of CVEs to Apache HTTP Server (and the corresponding updates) can be found at the following link:
http://httpd.apache.org/security/vulnerabilities_22.html

When it comes to Apache web servers, security admins have to watch out for the web server attack called Darkleech. This takes the form of a malicious Apache module (specifically an injected HTML iframe tag within a PHP file). If loaded on a compromised Apache web server, it can initiate all kinds of attacks and deliver various payloads of malware and ransomware. Or, it could redirect a user to another site that contains an exploit kit such as the Blackhole exploit kit mentioned in Chapter 2. Though Darkleech is not limited to Apache, the bulk of Darkleech infected sites have been Apache-based.

NOTE So much for Microsoft being less targeted than Linux. As time moves forward, it seems that no platform is safe. A word to the wise—don't rely on any particular technology because of a reputation, and be sure to update and patch every technology you use.

As far as combating Darkleech, a webmaster can attempt to query the system for PHP files stored in folders with suspiciously long hexadecimal names. If convenient for the organization, all iframes can be filtered out. And of course, the Apache server should be updated as soon as possible, and if necessary, taken offline while it is repaired. In many cases, this type of web server attack is very hard to detect, and sometimes the only recourse is to rebuild the server (or virtual server image) that hosts the Apache server.

NOTE Another tool that some attackers use is archive.org. This website takes snapshots of many websites over time and stores them. They are accessible to anyone, and can give attackers an idea of older (and possibly less secure) pages and scripts that used to run on a web server. It could be that these files and scripts are still located on the web server even though they are no longer used. This is a vulnerability that security admins should be aware of. Strongly consider removing older unused files and scripts from web servers.

FTP Server

An FTP server can be used to provide basic file access publicly or privately. Examples of FTP servers include the FTP server built into IIS, the Apache FtpServer, and other third-party offerings such as FileZilla Server and Pure-FTPd.

The standard, default FTP server is pretty insecure. It uses well-known ports (20 and 21), doesn't use encryption by default, and has basic username/password authentication. As a result, FTP servers are often the victims of many types of attacks. Examples include bounce attacks—when a person attempts to hijack the FTP service to scan other computers; buffer overflow attempts—when an attacker tries to send an extremely long username (or password or filename) to trigger the overflow; and attacks on the anonymous account (if utilized).

If the files to be stored on the FTP server are at all confidential, the security administrator should consider additional security. This can be done by incorporating FTP software that utilizes secure file transfer protocols such as FTPS or SFTP. Additional security can be provided by using FTP software that uses dynamic assignment of data ports, instead of using port 21 every time. We'll discuss more about ports and secure protocols in Chapter 6. Encryption can prevent most attackers from reading the data files, even if they are able to get access to them. And of course, if not a public FTP, the anonymous account should be disabled.

But there are other, more sinister attacks lurking, ones that work in conjunction with the web server, which is often on the same computer, or part of the same software suite—for instance, the web shell. There are plenty of variants of the web shell, but we'll detail its basic function. The web shell is a program that is installed on a web server by an attacker, and is used to remotely access and reconfigure the server without the owner's consent.

Web shells are remote access Trojans (RATs), but are also referred to as backdoors, since they offer an alternative way of accessing the website for the attacker. The reason I place the web shell attack here in the FTP section is because it is usually the FTP server that contains the real vulnerability—weak passwords. Once an attacker

figures out an administrator password of the FTP server (often through brute-force attempts), the attacker can easily install the web shell, and effectively do anything desired to that web server (and/or the FTP server). It seems like a house of cards, and in a way it is.

How can we prevent this from happening? First, increase the password security and change the passwords of all administrator accounts. Second, eliminate any unnecessary accounts, especially any superfluous admin accounts and the dreaded anonymous account. Next, strongly consider separating the FTP server and web server to two different computers or virtual machines. Finally, set up automated scans for web shell scripts (usually PHP files, lo and behold), or have the web server provider do so. If the provider doesn't offer that kind of scanning, use a different provider. If a web shell attack is accomplished successfully on a server, the security admin must at the very least search for and delete the original RAT files, and at worst re-image the system and restore from backup. This latter option is often necessary if the attacker has had some time to compromise the server. Some organizations have policies that state servers must be re-imaged if they are compromised in any way, shape, or form. It's a way of starting anew with a clean slate, but it means a lot of configuring for the admin. But again, the overall concern here is the complexity of, and the frequency of changing, the password.

That's the short list of servers. But there are plenty of others you need to be cognizant of, including: DNS servers (which we cover in Chapter 6), application servers, virtualization servers, firewall/proxy servers, database servers, print servers, remote connectivity servers such as RRAS and VPN (which we will discuss more in Chapter 9), and computer telephony integration (CTI) servers. If you are in charge of securing a server, be sure to examine the CVEs and bulletins for that software, and be ready to hot-patch the system at a moment's notice. This means having an RDP, VNC, or other remote connection to that specific server ready to go on your desktop, so that you can access it quickly.

Chapter Summary

Designing a secure network is more than just setting up a Visio document and dragging a firewall onto the LAN. This might have been good security planning in 1998, but today we need a plan that includes many layers of protection, allowing for defense in depth. For instance, today's networks require specially secured devices such as switches, routers, and telephony equipment. And those networks might need demilitarized zones (DMZs), intrusion prevention systems (IPSSs), content filters, network access control (NAC), subnetting, virtual local area networks (VLANs), and of course...firewalls.

Keep in mind that some of these technologies might exist on, or be moved to, the cloud. This opens up Pandora’s box when it comes to security. The security administrator needs to be sure not only that resources are secured properly, but also that the cloud provider is reputable, and will take care of its end of the safety of the organization’s data and infrastructures.

An organization has a lot of choices when it comes to the cloud. Software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) are the three main types of cloud offerings. SaaS is probably the most common, and is used to run web-based applications remotely. IaaS offloads the network infrastructure of a company to the cloud and utilizes virtual machines to store entire operating systems. PaaS enables organizations to develop applications in a powerful virtual environment without using internal resources. Some organizations will opt to use more than one of these solutions.

Once the type of cloud solution is selected, an organization must select whether its resources will be kept publicly, privately, or a mixture of the two (hybrid or community-oriented). This will be based on the budget and manpower of the organization in question, but each option has its own set of security concerns.

Besides loss of administrative power, an organization going to the cloud might encounter data integrity issues, availability issues, and, worst of all, potential loss of confidentiality. That’s the entire CIA triad right there, so making use of the cloud should be approached warily. To reduce the chance of data breaches on the cloud, organizations make use of complex passwords, password and cloud data access policies, strong authentication methods, encryption, and protection of data and applications on several levels.

It’s the servers that are of greatest concern. They are attacked the most often, as it is they who contain the data. The common victims are the e-mail servers, web servers, and FTP servers, because they are so readily accessible, and because of the plethora of ways they can be compromised. Patching systems is an excellent method of protection—and keeping up to date with the latest Common Vulnerabilities and Exposures (CVE) is the best way to know exactly what needs to be patched.

As a final remark, a good security administrator has to remember that *any* platform is susceptible to attack, in one form or another. Every single server and networking device, either on the local network or on the cloud, should be secured accordingly.

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 5-5 lists a reference of these key topics and the page number on which each is found.

Table 5-5 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
Bulleted list	Description of MAC flooding and defense techniques	183
Table 5-2	Private IPv4 ranges (as assigned by the IANA)	186
Figure 5-1	Example of public and private IPv4 addresses	187
Figure 5-2	3-leg perimeter DMZ	190
Table 5-4	Types of VLAN hopping	195

Define Key Terms

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

MAC flooding, CAM table, failopen mode, network address translation, port address translation, static NAT, one-to-one mapping, demilitarized zone, 3-leg perimeter, back-to-back perimeter, network access control (NAC), VLAN hopping, war-dialing, cloud computing, software as a service (SaaS), infrastructure as a service (IaaS), platform as a service (PaaS), Common Vulnerabilities and Exposures (CVE)

Review Questions

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

- Which of the following would you set up in a multifunction SOHO router?
 - DMZ
 - DOS

- C. OSI
 - D. ARP
2. Which of the following is a private IPv4 address?
- A. 11.16.0.1
 - B. 127.0.0.1
 - C. 172.16.0.1
 - D. 208.0.0.1
3. Which of these hides an entire network of IP addresses?
- A. SPI
 - B. NAT
 - C. SSH
 - D. FTP
4. Which of the following statements best describes a static NAT?
- A. Static NAT uses a one-to-one mapping.
 - B. Static NAT uses a many-to-many mapping.
 - C. Static NAT uses a one-to-many mapping.
 - D. Static NAT uses a many-to-one mapping.
5. Which of the following should be placed between the LAN and the Internet?
- A. DMZ
 - B. HIDS
 - C. Domain controller
 - D. Extranet
6. You want to reduce network traffic on a particular network segment to limit the amount of user visibility. Which of the following is the best device to use in this scenario?
- A. Switch
 - B. Hub
 - C. Router
 - D. Firewall

7. You receive complaints about network connectivity being disrupted. You suspect that a user connected both ends of a network cable to two different ports on a switch. What can be done to prevent this?
 - A. Loop protection
 - B. DMZ
 - C. VLAN segregation
 - D. Port forwarding
8. You see a network address in the command-line that is composed of a long string of letters and numbers. What protocol is being used?
 - A. IPv4
 - B. ICMP
 - C. IPv3
 - D. IPv6
9. Which of the following cloud computing services offers easy to configure operating systems?
 - A. SaaS
 - B. IaaS
 - C. PaaS
 - D. VM
10. Which of the following might be included in Microsoft Security Bulletins?
 - A. PHP
 - B. CGI
 - C. CVE
 - D. TLS
11. Which of the following devices would most likely have a DMZ interface?
 - A. Switch
 - B. VoIP phone
 - C. Proxy server
 - D. Firewall

- 12.** Your network uses the subnet mask 255.255.255.224. Which of the following IPv4 addresses are able to communicate with each other? (Select the two best answers.)
- A.** 10.36.36.126
 - B.** 10.36.36.158
 - C.** 10.36.36.166
 - D.** 10.36.36.184
 - E.** 10.36.36.224
- 13.** You are implementing a testing environment for the development team. They use several virtual servers to test their applications. One of these applications requires that the servers communicate with each other. However, to keep this network safe and private, you do not want it to be routable to the firewall. What is the best method to accomplish this?
- A.** Use a virtual switch.
 - B.** Remove the virtual network from the routing table.
 - C.** Use a standalone switch.
 - D.** Create a VLAN without any default gateway.
- 14.** Your boss (the IT director) wants to move several internally developed software applications to an alternate environment, supported by a third-party, in an effort to reduce the footprint of the server room. Which of the following is the IT director proposing?
- A.** PaaS
 - B.** IaaS
 - C.** SaaS
 - D.** Community cloud
- 15.** A security analyst wants to ensure that all external traffic is able to access an organization's front-end servers but also wants to protect access to internal resources. Which network design element is the best option for the security analyst?
- A.** VLAN
 - B.** Virtualization
 - C.** DMZ
 - D.** Cloud computing

- 16.** In your organization's network you have VoIP phones and PCs connected to the same switch. Which of the following is the best way to logically separate these device types while still allowing traffic between them via an ACL?
- A.** Install a firewall and connect it to the switch.
 - B.** Create and define two subnets, configure each device to use a dedicated IP address, and then connect the whole network to a router.
 - C.** Install a firewall and connect it to a dedicated switch for each type of device.
 - D.** Create two VLANs on the switch connected to a router.
- 17.** You ping a hostname on the network and receive a response including the address 2001:4560:0:2001::6A. What type of address is listed within the response?
- A.** MAC address
 - B.** Loopback address
 - C.** IPv6 address
 - D.** IPv4 address
- 18.** Analyze the following network traffic logs depicting communications between Computer1 and Computer2 on opposite sides of a router. The information was captured by the computer with the IPv4 address 10.254.254.10.

```
Computer1  Computer2
[192.168.1.105] -----[INSIDE 192.168.1.1 router OUTSIDE 10.254.254.1]
-----[10.254.254.10] LOGS
7:58:36 SRC 10.254.254.1:3030, DST 10.254.254.10:80, SYN
7:58:38 SRC 10.254.254.10:80, DST 10.254.254.1:3030, SYN/ACK
7:58:40 SRC 10.254.254.1:3030, DST 10.254.254.10:80, ACK
```

Given the information, which of the following can you infer about the network communications?

- A.** The router implements NAT.
- B.** The router filters port 80 traffic.
- C.** 192.168.1.105 is a web server.
- D.** The web server listens on a nonstandard port.

- 19.** Your organization uses VoIP. Which of the following should be performed to increase the availability of IP telephony by prioritizing traffic?
- A. NAT
 - B. QoS
 - C. NAC
 - D. Subnetting
- 20.** You have been tasked with segmenting internal traffic between layer 2 devices on the LAN. Which of the following network design elements would most likely be used?
- A. VLAN
 - B. DMZ
 - C. NAT
 - D. Routing

Answers and Explanations

- 1.** A. A DMZ, or demilitarized zone, can be set up on a SOHO router (in the firewall portion) to create a sort of safe haven for servers. It is neither the LAN nor the Internet, but instead, a location in between the two.
- 2.** C. 172.16.0.1 is the only address listed that is private. The private assigned ranges can be seen in Table 5-2 earlier in the chapter. 11.16.0.1 is a public IPv4 address, as is 208.0.0.1. 127.0.0.1 is the IPv4 loopback address.
- 3.** B. NAT (network address translation) hides an entire network of IP addresses. SPI, or Stateful Packet Inspection, is the other type of firewall that today's SOHO routers incorporate.
- 4.** A. Static network address translation normally uses a one-to-one mapping when dealing with IP addresses.
- 5.** A. A demilitarized zone, or DMZ, can be placed between the LAN and the Internet; this is known as a back-to-back perimeter configuration. This allows external users on the Internet to access services but segments access to the internal network. In some cases, it will be part of a 3-leg firewall scheme. Host-based intrusion detection systems are placed on an individual computer, usually within the LAN. Domain controllers should be protected and are normally on the LAN as well. An extranet can include parts of the Internet and

parts of one or more LANs; normally it connects two companies utilizing the power of the Internet.

6. **A.** A switch can reduce network traffic on a particular network segment. It does this by keeping a table of information about computers on that segment. Instead of broadcasting information to all ports of the switch, the switch selectively chooses where the information goes.
7. **A.** Loop protection should be enabled on the switch to prevent the looping that can occur when a person connects both ends of a network cable to the same switch. A DMZ is a demilitarized zone that is used to keep servers in a midway zone between the Internet and the LAN. VLAN segregation (or VLAN separation) is a way of preventing ARP poisoning. Port forwarding refers to logical ports associated with protocols.
8. **D.** IPv6 uses a long string of numbers and letters in the IP address. These addresses are 128-bit in length. IPv4 addresses are shorter (32-bit) and are numeric only. ICMP is the Internet Control Message Protocol, which is used by ping and other commands. IPv3 was a test version prior to IPv4 and was similar in IP addressing structure.
9. **C.** Platform as a service (PaaS) is a cloud computing service that offers many software solutions, including easy-to-configure operating systems and on-demand computing. SaaS is software as a service, used to offer solutions such as webmail. IaaS is infrastructure as a service, used for networking and storage. VM stands for virtual machine, which is something that PaaS also offers.
10. **C.** Common Vulnerabilities and Exposures (CVE) can be included in Microsoft Security Bulletins and will be listed for other web server products such as Apache. PHP and CGI are pseudo-programming languages used within HTML for websites. Both can contain harmful scripts if used inappropriately. Transport Layer Security (TLS) is a protocol used by sites secured by HTTPS.
11. **D.** The firewall is the device most likely to have a separate DMZ interface. Switches connect computers on the LAN. VoIP phones are used by individuals to make and answer phone calls on a Voice over IP connection. A proxy server acts as a go-between for the clients on the LAN and the web servers that they connect to, and caches web content for faster access.
12. **C. and D.** The hosts using the IP addresses 10.36.36.166 and 10.36.36.184 would be able to communicate with each other because they are on the same subnet (known as subnet ID 5). All of the other answer choices' IP addresses are on different subnets, so they would not be able to communicate with each other (or with the IP addresses of the correct answers) by default. Table 5-6

provides the complete list of subnets and their ranges for this particular subnetted network. It is noteworthy that the answer 10.36.36.224 is not even usable because it is the first IP of one of the subnets. Remember that the general rule is: you can't use the first and last IP within each subnet. That is because they are reserved for the subnet ID and the broadcast addresses, respectively.

Table 5-6 List of Subnets for 10.36.36.0/27 (255.255.255.224 Subnet Mask)

Subnet ID	Mathematical IP Range	Usable IP Range
ID 0	10.36.36.0–10.36.36.31	10.36.36.1–10.36.36.30
ID 1	10.36.36.32–10.36.36.63	10.36.36.33–10.36.36.62
ID 2	10.36.36.64–10.36.36.95	10.36.36.65–10.36.36.94
ID 3	10.36.36.96–10.36.36.127	10.36.36.97–10.36.36.126
ID 4	10.36.36.128–10.36.36.159	10.36.36.129–10.36.36.158
ID 5	10.36.36.160–10.36.36.191	10.36.36.161–10.36.36.190
ID 6	10.36.36.192–10.36.36.223	10.36.36.193–10.36.36.222
ID 7	10.36.36.224–10.36.36.255	10.36.36.225–10.36.36.254

- 13. A.** The virtual switch is the best option. This virtual device will connect the virtual servers together without being routable to the firewall (by default). Removing the virtual network from the routing table is another possibility; but if you have not created a virtual switch yet, it should not be necessary. A physical standalone switch won't be able to connect the virtual servers together; a virtual switch (or individual virtual connections) is required. Creating a VLAN would also require a physical switch. In that scenario, you can have multiple virtual LANs each containing physical computers (not virtual computers), and each working off of the same physical switch. That answer would keep the VLAN from being routable to the firewall, but not virtual servers.
- 14. B.** The IT director is most likely proposing that you use infrastructure as a service (IaaS). A cloud-based service, IaaS is often used to house servers (within virtual machines) that store developed applications. It differs from PaaS in that it is the servers, and already developed applications, that are being moved from the server room to the cloud. However, PaaS might also be required if the applications require further development. The most basic cloud-based service, software as a service (SaaS), is when users work with applications (often web-based) that are provided from the cloud. A community cloud is when multiple organizations share certain aspects of a public cloud.

15. **C.** The demilitarized zone (DMZ) is the best option in this scenario. By creating a DMZ, and placing the front-end servers within it (on a separate branch of the firewall), you create a type of compartmentalization between the LAN (important internal resources) and the front-end servers. A VLAN is used to separate a LAN into multiple virtual units. Virtualization is a general term that usually refers to the virtualizing of operating systems. Cloud computing is another possible option in this scenario, because you could take the front-end servers and move them to the cloud. However, a certain level of control is lost when this is done, whereas with a DMZ, the security analyst still retains complete control.
16. **D.** The best option is to create two VLANs on the switch (one for the VoIP phones, and one for the PCs) and make sure that the switch is connected to the router. Configure access control lists (ACLs) as necessary on the router to allow or disallow connectivity and traffic between the two VLANs. Installing a firewall and configuring ACLs on that firewall is a possibility, but you would also have to use two separate dedicated switches if VLANs are not employed. This is a valid option, but requires additional equipment, whereas creating the two VLANs requires no additional equipment (as long as the switch has VLAN functionality). While subnetting is a possible option, it is more elaborate than required. The VLAN (in this case port-based) works very well in this scenario and is the best option.
17. **C.** The address in the response is a truncated IPv6 address. You can tell it is an IPv6 address because of the hexadecimal numbering, the separation with colons, and the groups of four digits. You can tell it is truncated because of the single zero and the double colon. A MAC address is also hexadecimal and can use colons to separate the groups of numbers (though hyphens often are used), but the numbers are grouped in twos. An example is 00-1C-C0-A1-54-15. The loopback address is a testing address for the local computer. In IPv6 it is simply ::1, whereas in IPv4 it is 127.0.0.1. Finally, IPv4 addresses in general are 32-bit dotted-decimal numbers such as 192.168.1.100.
18. **A.** The only one of the listed answers that you can infer from the log is that the router implements network address translation (NAT). You can tell this from the first line of the log, which shows the inside of the router using the 192.168.1.1 IP address and the outside using 10.254.254.1. NAT is occurring between the two at the router. This allows the IP 192.168.1.105 to communicate with 10.254.254.10 ultimately. However, the rest of the logs only show the first step of that communication between 10.254.254.10 and the router at 10.254.254.1.

What's really happening here? The router is showing that port 3030 is being used on 10.254.254.1. That is the port used by an online game known as

netPanzer. The client (10.254.254.10) is using port 80 to make a web-based connection to the game. You can see the three-way TCP handshake occurring with the SYN, SYN/ACK, and ACK packets. Ultimately, 10.254.254.10 is communicating with 192.168.1.105, but we only see the first stage of that communication to the router. As a security analyst you would most likely want to shut down the use of port 3030, so that employees can be more productive and you have less overall chance of a network breach.

As far as the incorrect answers, the router definitely is not filtering out port 80, as traffic is successfully being sent on that port. 192.168.1.105 is not a web server; it is most likely the netPanzer game server. Finally, even though port 80 is used by the client computer, there is likely no web server in this scenario.

19. **B.** Quality of Service (QoS) should be configured on the router to prioritize traffic, promoting IP telephony traffic to be more available. You'll get some detractors of QoS, especially for the SOHO side of networks, but if used on the right device and configured properly, it can make a difference. This might sound like more of a networking question, but it ties in directly to the CIA triad of security. Data confidentiality and integrity are important, but just as important is availability—the ability for users to access data when required. NAT is network address translation, which interprets internal and external IP networks to each other. NAC is network access control—for example, 802.1X. Subnetting is when a network is divided into multiple logical areas through IP addressing/planning and subnet mask configuring.
20. **A.** You would most likely use a virtual LAN (VLAN). This allows you to segment internal traffic within layer 2 of the OSI model, by using either a protocol-based scheme or a port-based scheme. The DMZ is used to create a safe haven for servers that are accessed by outside traffic. NAT is network address translation, which is a layer 3 option used on routers. Because we are dealing with a layer 2 scenario, routing in general is not necessary.

Case Studies for Chapter 5

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

Case Study 5-1: Creating a DMZ

Scenario: Your organization's network has all of its servers running directly within the LAN. The new IT director knows this is quite insecure, and so instructs you to develop a 3-leg firewall scheme.

Your task is to create a network diagram (either handwritten or with a program such as Microsoft Visio) that shows the LAN, Internet, firewall, and DMZ areas. Give examples of the IP addresses that might be used for all three connections to the firewall.

Case Study 5-2: Subnetting a Network

Scenario: The organization you work for has several departments. There is a lot of unnecessary traffic flowing between the Human Resources, Accounting, and Marketing departments. Each department has 10 to 15 computers running within it. Your task is to implement subnetting so that each of the three departments' computers are placed on separate subnets, thus reducing overall traffic, as well as securing the connections between the departments.

In this scenario you will use the 192.168.100.0 network. The current subnet mask is 255.255.255.0. You will need to modify this. Plan the network so that there are eight subnets in total. Specify which subnet ID each department uses, and what the usable ranges of IP addresses for those subnets are. Your answers may vary from the case study solution.

Case Study 5-3: Defending against the Web Shell

Scenario: One of your associate's websites was hacked into. The associate contacted you to see if you knew anything about a "Web Shell." The person had found that name within the syntax of one of the "new" files on his web server. Your task is to explain what is going on to your associate, and recommend a solution.

Question 1: What is the Web Shell?

Question 2: How did it get there?

Question 3: What should your recommendations be?

Case Study Solutions

Case Study 5-1 Solution

As shown in Figure 5-6, the 3-leg firewall scheme has a firewall in the center with three connections to the Internet, the LAN, and the DMZ. The LAN is using a

Class B private IP network. The DMZ is on a separate Class C IP network. And the Internet connection uses a public IP address so that the firewall can connect directly to other systems and networks on the Internet.

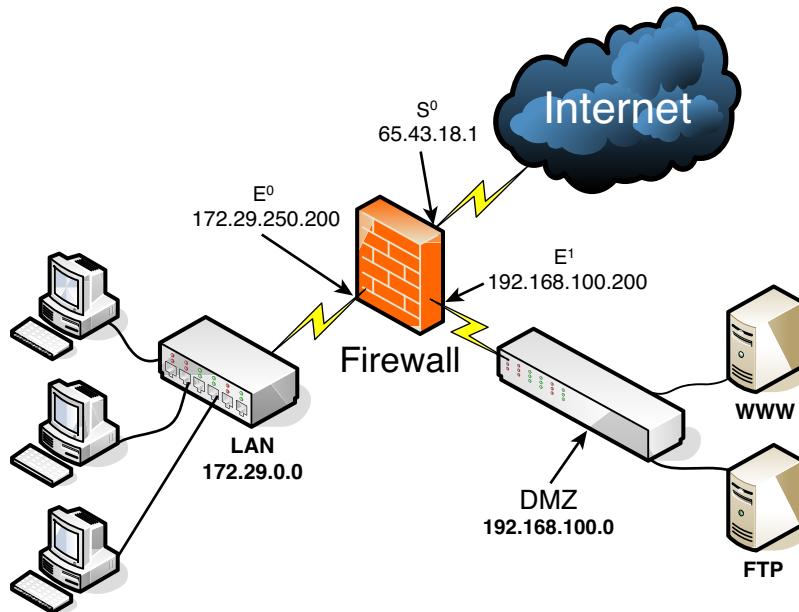


Figure 5-6 DMZ with 3-Leg Firewall Scheme

This 3-leg solution is an excellent way (though not the only method) of separating web servers, FTP servers, and mail servers from the rest of the LAN. A separate set of rules (ACLs) can be configured for the DMZ connection and the LAN connection. In this way, the DMZ can be accessed by users on the Internet (and by users on the LAN), but the resources on the LAN are fully protected from users on the Internet. A 3-leg firewall of this sort can be accomplished by using a hardware-based firewall with an Internet connection and two LAN connections (most common), or a server with three network adapters running special firewalling software.

Simulation: Complete the simulation “5-1: Creating a DMZ” on the accompanying disc.

Case Study 5-2 Solution

Subnetting is an excellent way of compartmentalizing the network. It reduces broadcast traffic between the various computers on the network, and secures different departments. This is because many types of traffic now cannot pass from one subnet to the next (without an expressed routing rule). So it is an effective security method.

In the scenario we were given the 192.168.100.0 Class C network to work with. To end up with eight subnets, we would need to use the 255.255.255.224 subnet mask. This can be represented as 192.168.100.0/27 because the subnet mask will have 27 masked bits (1s). Table 5-7 shows the eight possible subnets and their ranges. Though they are usable, in many cases, a network engineer will opt to not use the first and last subnets, so subnet IDs 1 to 6 become fair game.

Table 5-7 List of Subnets for 192.168.100.0/27 (255.255.255.224 Subnet Mask)

Subnet ID	Mathematical IP Range	Usable IP Range
ID 0	192.168.100.0–192.168.100.31	192.168.100.1–192.168.100.30
ID 1	192.168.100.32–192.168.100.63	192.168.100.33–192.168.100.62
ID 2	192.168.100.64–192.168.100.95	192.168.100.65–192.168.100.94
ID 3	192.168.100.96–192.168.100.127	192.168.100.97–192.168.100.126
ID 4	192.168.100.128–192.168.100.159	192.168.100.129–192.168.100.158
ID 5	192.168.100.160–192.168.100.191	192.168.100.161–192.168.100.190
ID 6	192.168.100.192–192.168.100.223	192.168.100.193–192.168.100.222
ID 7	192.168.100.224–192.168.100.255	192.168.100.225–192.168.100.254

Each subnet has 30 usable IP addresses. (Remember that you can't use the first or the last because they are reserved for the subnet IP and the broadcast IP.) So, for example, we could use subnet ID 1 for the Human Resources department, subnet ID 2 for the Accounting department, and subnet ID 3 for the Marketing department.

The computers within each of those networks would then need to be configured properly. There are a lot of ways to do this. Automation is the best way. For example, set up three DHCP scopes configured on a DHCP server (be it a Microsoft server or a router), each of which corresponds to the appropriate subnetwork within a router. The key is to make sure that the DHCP server hands out the correct subnet ID addresses to each department. This requires additional configuring that goes beyond the extent of this case study. However, for more information on defining DHCP scopes in Windows Server, see the following link:
<http://technet.microsoft.com/en-us/library/dd759218.aspx>

For more information about DHCP subnet configuration on Cisco routers, see the following link:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/8_5_1/ccmcfg/bccm-851-cm/b02dhsu.html

Or simply search for “Cisco DHCP subnet configuration.”

Video Solution: Watch the video solution “5-2: Subnetting a Network” on the accompanying disc. This reviews subnet masks and shows an example of subnetting.

Case Study 5-3 Solution

These web shells are programs (known under several permutations: C99, C Shell, Web Shell, Web Shell by Orb, and others) that are installed on the web server by an attacker, and are used to remotely access and reconfigure the server without the owner’s consent. They are *remote access Trojans*, but are also referred to as backdoors because they offer an alternative way of accessing the website for the attacker.

Most likely, the hacker stole the associate’s FTP password. Once the hacker had the password, it was just a matter of uploading the shell. Then the hacker could log in through the new web shell, and do just about anything they wanted to the web server. Many of these web shells allow the operator to access them through a proxy, thus hiding the location of the operator. Also, the shell can be bound to specific ports, and the information can be encrypted and hashed.

First, you should recommend increasing password security for all important FTP accounts. Make the passwords as complex as the web server would allow. Remove any unnecessary FTP accounts. Delete the original RAT files and run a full scan of the system, or at worst, restore data from an older backup. Have the associate verify the web host’s scanning techniques, or scan web files manually.

Simulation: Complete the simulation “5-3: Defending against the Web Shell.”



This chapter covers the following subjects:

- **Ports and Protocols:** In this section, you learn the ports and their associated protocols you need to know for the exam and how to secure those ports. Sometimes the port needs to be closed; sometimes it needs to remain open. Once you understand if the port is necessary, you can decide whether to lock it down or to keep it ajar in a secure manner.
- **Malicious Attacks:** This section covers the basics about network attacks and how to defend against them. Study this section carefully; the CompTIA Security+ exam is bound to ask you several questions about these concepts.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 1.2, 1.3, 1.4, 3.2, and 3.5.

Networking Protocols and Threats

Making client connections to servers means that the servers need to have open ports to facilitate their services. However, every open port is a vulnerability. It's important to know the common protocols used by servers and their respective ports and how to protect against threats that might try to exploit those server ports.

The threats are many. Malicious attacks such as denial-of-service attacks, man-in-the-middle attacks, replay attacks, and session hijacking can all be devastating to individual computers and to entire networks. But once you have built a decent knowledge of ports and protocols, you can use that intelligence to better protect your servers and network against the plethora of attacks you will face.

One thing to remember is that there are always new network attacks being developed, and many that currently exist but are unknown. Therefore, this chapter is incomplete in the sense that once it is written, it is out of date. Keep this in mind, and remember to always keep on top of your security bulletins, CVEs, and security updates.

Foundation Topics

Ports and Protocols

I can't stress enough how important it is to secure a host's ports and protocols. They are the doorways into an operating system. Think about it: An open doorway is a plain and simple invitation for disaster. And that disaster could be caused by one of many different types of malicious network attacks. The security administrator must be ever vigilant in monitoring, auditing, and implementing updated defense mechanisms to combat malicious attacks. Understanding ports and protocols is the first step in this endeavor.

Ports Ranges, Inbound Versus Outbound, and Common Ports

Although some readers of this book will be familiar with ports used by the network adapter and operating system, a review of them is necessary because they

play a big role in securing hosts and will most definitely appear on the exam in some way, shape, or form.

Ports act as logical communication endpoints for computers. Each protocol uses a specific port; for example, HTTP uses port 80 by default. These ports are ultimately controlled on the transport layer of the OSI model by protocols such as the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP is used for guaranteed, connection-oriented sessions such as the initial connection to a web page, and UDP is used for connectionless sessions such as the streaming of data. There are 65,536 ports altogether, numbering between 0 and 65,535. The ports are divided into categories, as shown in Table 6-1.

Table 6-1 Port Ranges

Port Range	Category Type	Description
0–1023	Well-Known Ports	This range defines commonly used protocols; for example, HTTP uses port 80. They are designated by the IANA (Internet Assigned Numbers Authority), which is operated by the ICANN (Internet Corporation for Assigned Names and Numbers).
1024–49,151	Registered Ports	Ports used by vendors for proprietary applications. These must be registered with the IANA. For example, Microsoft registered port 3389 for use with the Remote Desktop Protocol (RDP), aka Microsoft Terminal Server.
49,152–65,535	Dynamic and Private Ports	These ports can be used by applications but cannot be registered by vendors.

You need to understand the difference between inbound and outbound ports as described in the following two bullets and as illustrated in Figure 6-1.

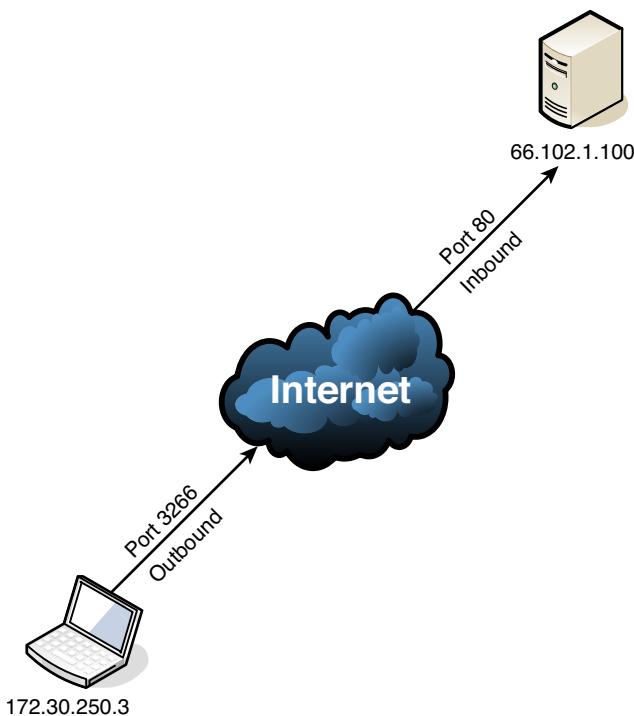


Figure 6-1 Inbound Versus Outbound Ports

- **Inbound ports:** Used when another computer wants to connect to a service or application running on your computer. Servers primarily use inbound ports so that they can accept incoming connections and serve data. For example, in Figure 6-1, the server with the IP address 66.102.1.100 has inbound port 80 open to accept incoming web page requests.
- **Outbound ports:** Used when your computer wants to connect to a service or application running on another computer. Client computers primarily use outbound ports that are assigned dynamically by the operating system. For example, in Figure 6-1, the client computer with the IP address 172.30.250.3 has outbound port 3266 open to make a web page request to the server.

NOTE For a refresher about TCP, UDP, and ports, see the short 5-minute video at the following link:

<http://www.davidlprowse.com/articles/?p=911>

It's the inbound ports that a security administrator should be most concerned with. Web servers, FTP servers, database servers, and so on have specific inbound ports opened to the public. Any other unnecessary ports should be closed, and any open ports should be protected and monitored carefully. Although there are 1,024 well-known ports, for the exam you need to know only a handful of them, plus some that are beyond 1,024, as shown in Table 6-2. Remember that these inbound port numbers relate to the applications, services, and protocols that run on a computer, often a server. When it comes to the OSI model, the bulk of these protocols are application layer protocols. Examples of these protocols include HTTP, FTP, SMTP, SSH, DHCP, and POP3, and there are many more. Because these are known as application layer protocols, their associated ports are known as *application service ports*. The bulk of Table 6-2 is composed of application service ports. Some of the protocols listed make use of TCP transport layer connections only (for example, HTTP, port 80). Some make use of UDP only (for example, SNMP, port 161). Many can use TCP or UDP transport mechanisms. Study Table 6-2 carefully now, bookmark it, and refer to it often!



Table 6-2 Ports and Their Associated Protocols

Port Number	Associated Protocol (or Keyword)	TCP/UDP Usage	Full Name	Usage
7	Echo	TCP or UDP	Echo	Testing round-trip times between hosts.
19	CHARGEN	TCP or UDP	Character Generator	Testing and debugging.
21	FTP	TCP	File Transfer Protocol	Transfers files from host to host.
22	SSH	TCP or UDP	Secure Shell	Remotely administers network devices and Unix/Linux systems. Also used by Secure Copy (SCP) and Secure FTP (SFTP), which both use TCP as the transport mechanism.
23	Telnet	TCP or UDP	TERminaL NETwork	Remotely administers network devices (deprecated).
25	SMTP	TCP	Simple Mail Transfer Protocol	Sends e-mail.

Port Number	Associated Protocol (or Keyword)	TCP/UDP Usage	Full Name	Usage
49	TACACS+	TCP	Terminal Access Controller Access-Control System Plus	Remote authentication. Can also use UDP, but TCP is the default. Compare with RADIUS.
53	DNS	TCP or UDP	Domain Name System	Resolves hostnames to IP addresses and vice-versa.
69	TFTP	UDP	Trivial File Transfer Protocol	Basic version of FTP.
80	HTTP	TCP	Hypertext Transfer Protocol	Transmits web page data.
88	Kerberos	TCP or UDP	Kerberos	Network authentication, uses tickets.
110	POP3	TCP	Post Office Protocol Version 3	Receives e-mail.
119	NNTP	TCP	Network News Transfer Protocol	Transports Usenet articles.
135	RPC/epmap/ dcom-scm	TCP or UDP	Microsoft End Point Mapper/ DCE Endpoint Resolution	Used to locate DCOM ports. Also known as RPC (Remote Procedure Call).
137–139	NetBIOS	TCP or UDP	NetBIOS Name, Datagram, and Session Services, respectively	Name querying, sending data, NetBIOS connections.
143	IMAP	TCP	Internet Message Access Protocol	Retrieval of e-mail, with advantages over POP3.
161	SNMP	UDP	Simple Network Management Protocol	Remotely monitor network devices.

Port Number	Associated Protocol (or Keyword)	TCP/UDP Usage	Full Name	Usage
162	SNMPTRAP	TCP or UDP	Simple Network Management Protocol Trap	Traps and InformRequests are sent to the SNMP Manager on this port.
389	LDAP	TCP or UDP	Lightweight Directory Access Protocol	Maintains directories of users and other objects.
443	HTTPS	TCP	Hypertext Transfer Protocol Secure	Secure transfer of hypertext through web pages (uses TLS or SSL).
445	SMB	TCP	Server Message Block	Provides shared access to files and other resources.
514	Syslog	UDP	Syslog Protocol	Used for computer message logging, especially for router and firewall logs. A secure version (Syslog over TLS) uses TCP as the transport mechanism and port 6514.
636	LDAP over TLS/SSL	TCP or UDP	Lightweight Directory Access Protocol (over TLS/SSL)	Secure version of LDAP.
860	iSCSI	TCP	Internet Small Computer System Interface	IP-based protocol used for linking data storage facilities. Also uses port 3260 for the iSCSI target.
989/990	FTPS	TCP or UDP	FTP Secure	Uses SSL/TLS to secure FTP transmissions. 990 is the control port and 989 is the data port.
1433	Ms-sql-s	TCP	Microsoft SQL Server	Opens queries to SQL server.

Port Number	Associated Protocol (or Keyword)	TCP/UDP Usage	Full Name	Usage
1701	L2TP	UDP	Layer 2 Tunneling Protocol	VPN protocol with no inherent security. Often used with IPsec.
1723	PPTP	TCP or UDP	Point-to-Point Tunneling Protocol	VPN protocol with built-in security.
1812/1813	RADIUS	UDP	Remote Authentication Dial-In User Service	An AAA protocol used for authentication (port 1812), authorization, and accounting (port 1813) of users that connect to networks and network services. UDP is the default but as of 2012 can use TCP as well. Compare with TACACS+. Other common ports include 1645 and 1646.
3225	FCIP	TCP or UDP	Fibre Channel over Internet Protocol	Encapsulates Fibre Channel frames within TCP/IP packets. Contrast with Fibre Channel over Ethernet (FCoE), which relies on the data link layer and doesn't rely on TCP/IP directly.
3389	RDP	TCP or UDP	Remote Desktop Protocol (Microsoft Terminal Server)	Remotely views and controls other Windows systems.

NOTE You can find a complete list of ports and their corresponding protocols at the following link:

<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

NOTE Not all protocols have set port numbers. For example, the Real-time Transport Protocol (RTP) uses a pair of port numbers determined by the application that is streaming the information via RTP. RFC 3550 for RTP recommends that they be even numbers, but no default port numbers are defined for that protocol.

The IP address of a computer and the port number it is sending or receiving on are combined together to form a network socket address. An example of this would be 66.102.1.100:80. That illustrates the IP address of the server in Figure 6-1 and the inbound port number accepting a connection from the client computer. Notice that the two are separated by a colon.

Figure 6-2 illustrates a few more examples of this within a Windows client computer. It shows some of the results of a netstat -an command after FTP, WWW, and mail connections were made by the client to two separate servers. Examine Figure 6-2 and then read on.

Key Topic

FTP Control Connection		FTP Data Connection	
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING
TCP	0.0.0.0:0:49204	0.0.0.0:0	LISTENING
TCP	10.254.254.285:139	0.0.0.0:0	LISTENING
TCP	10.254.254.285:55768	216.97.236.245:21	ESTABLISHED
TCP	10.254.254.285:55769	208.88.152.2:80	ESTABLISHED
TCP	10.254.254.285:55770	208.88.152.2:80	ESTABLISHED
TCP	10.254.254.285:55778	208.88.152.2:80	ESTABLISHED
TCP	10.254.254.285:55779	208.88.152.2:80	ESTABLISHED
TCP	10.254.254.285:55788	208.88.152.2:80	ESTABLISHED
TCP	10.254.254.285:55781	208.88.152.2:80	ESTABLISHED
TCP	10.254.254.285:55782	208.88.152.2:80	ESTABLISHED
TCP	10.254.254.285:55783	208.88.152.118:80	CLOSE_WAIT
TCP	10.254.254.285:55784	208.88.152.118:80	CLOSE_WAIT
TCP	10.254.254.285:55785	208.88.152.118:80	CLOSE_WAIT
TCP	10.254.254.285:55786	208.88.152.118:80	CLOSE_WAIT
TCP	10.254.254.285:55787	208.88.152.118:80	CLOSE_WAIT
TCP	10.254.254.285:55788	208.88.152.118:80	CLOSE_WAIT
TCP	10.254.254.285:55789	208.88.152.3:80	ESTABLISHED
TCP	10.254.254.285:55790	208.88.152.3:80	ESTABLISHED
TCP	10.254.254.285:55791	208.88.152.3:80	ESTABLISHED
TCP	10.254.254.285:55792	208.88.152.3:80	ESTABLISHED
TCP	10.254.254.285:55794	216.97.236.245:110	TIME_WAIT
TCP	10.254.254.285:55799	216.97.236.245:110	TIME_WAIT
TCP	127.0.0.1:2884	127.0.0.1:49190	ESTABLISHED
TCP	127.0.0.1:8100	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8100	127.0.0.1:55726	TIME_WAIT

HTTP Connection

POP3 Connection

Figure 6-2 IP Addresses and Ports

The first callout in Figure 6-2 is the initial FTP connection. This happens when a user first connects to an FTP server with FTP client software. Notice that the local computer has the IP address 10.254.254.205 and uses the dynamically assigned outbound port 55768 to connect to the FTP server. The remote computer, on the other hand, has the IP address 216.97.236.245 and uses inbound port 21 (known as a command port) to accept the connection. Keep in mind that this is only the initial connection and login to the FTP server. Subsequent data connections are normally done on the server side via dynamically assigned ports. For example, the second callout, FTP Data Connection, occurred when the client downloaded a file. It is a separate

session in which the client used the dynamically assigned port number 55769. In reality, this isn't quite dynamic anymore; the client operating system is simply selecting the next port number available; afterward, a subsequent and concurrent download would probably use port 55770. The server, on the other hand, used the dynamically assigned port number 31290.

Many FTP servers randomly select a different inbound port to use for each data connection, to increase security. However, some active FTP connections still use the original port 20 for data connections, which is not as secure, not only because it is well known, but also because it is static. To secure FTP communications, consider using software that enables dynamically assigned ports during data transfers; for example, Pure-FTPd (www.pureftpd.org) on the server side and FileZilla (<http://filezilla-project.org/>) on the client side. If your FTP server enables it, you can also consider IPv6 connections, and as always, be sure to use strong, complex passwords. (I don't mean to sound like a broken record!)

The third callout in Figure 6-2 shows an HTTP connection. Note that this is being made to a different server (208.80.152.118) and uses port 80. And finally, a POP3 connection that was previously made to the same server IP as the FTP connection, but note that the port number reflects POP3—it shows port number 110. These are just a few examples of many that occur between clients and servers all the time. Try making some connections to various servers from your client computer and view those sessions in the command-line.

Aside from servers, ports also become particularly important on router/firewall devices. These devices operate on the implicit deny concept, which means they deny all traffic unless a rule is made to open the port associated with the type of traffic desired to be let through. We talk more about firewalls in Chapter 7, "Network Perimeter Security."

You need to scan your servers, routers, and firewall devices to discern which ports are open. This can be done with the aforementioned `netstat` command, with an application such as Nmap (<http://nmap.org/>), or with an online scanner from a website, such as GRC's ShieldsUP! (www.grc.com). The most effective way is with an actual scanning application, which we show in depth in Chapter 11, "Vulnerability and Risk Assessment." However, there is a basic case study on port scanning referenced at the end of this chapter.

Afterward, unnecessary ports should be closed. This can be done in a few ways:

- **Within the operating system GUI:** For example, in Windows, open the Computer Management console. Then go to Services and Applications > Services. Right-click the appropriate service and select Properties. From here the service can be stopped and disabled.

- **Within the CLI:** For example, a service can be stopped in Windows by using the `net stop service` command, or with the `sudo stop service` command in Linux. (More about stopping services can be found in Chapter 3, “OS Hardening and Virtualization.”)
- **Within a firewall:** Simply setting up a firewall normally closes and shields all ports by default. But you might have a service that was used previously on a server, and therefore a rule might have been created on the firewall to enable traffic on that port. Within the firewall software, the rule can be deleted, disabled, or modified as needed. In general, network firewalls protect all the computers on the network, so this is where you would normally go to close particular ports.

Unnecessary ports also include ports associated with nonessential protocols. For example, TFTP (port 69) is usually considered a nonessential protocol, as is Finger (port 79). Telnet (port 23) is insecure and as such is also considered nonessential. However, the list of nonessential protocols differs from one organization to the next. Always rescan the host to make sure that the ports are indeed closed. Then, make the necessary changes in documentation. Depending on company policy, you might need to follow change management procedures before making modifications to ports and services. For more information on this type of documentation and procedures, see Chapter 16, “Policies, Procedures, and People.”

NOTE In some cases, you might find that a particular network interface is used either very infrequently or not at all. In these scenarios it is smart to consider disabling the entire interface altogether, either from the properties of the network adapter, in the Device Manager, or in the command-line of the OS in question. When the network adapter is disabled, all ports are effectively closed.

Port Zero Security

Let’s talk about port zero for a moment. Although there are a total of 65,536 ports, only 65,535 of them can normally be exploited. The reason is that port zero usually redirects to another dynamically assigned port. Although the IANA listings say it is reserved, it is not considered to exist and is often defined as an invalid port number. But programmers use port zero as a wildcard port, designing their applications to ask the operating system to assign a non-zero port. So, normally malware that exploits port zero will simply be redirected to another valid port. Again, this means that only 65,535 of the 65,536 ports can be exploited. In the future, port zero may become more of a security concern with the growth of legitimate raw socket programming.

This is programming directly to network ports, bypassing the transport layer; an example would be the Internet Control Message Protocol (ICMP) involving ping operations. However, historically, raw sockets have been used by hackers to perform *TCP reset attacks*, which set the reset flag in a TCP header to 1, telling the respective computer to kill the TCP session immediately. Until recently, raw socket programming has been generally frowned upon.

Protocols That Can Cause Anxiety on the Exam

Unfortunately, a lot of the protocols look similar, behave similarly, and can be downright confusing. Let's discuss a few of the more difficult ones and try to dispel some of the confusion. We start with FTP and its derivatives.

You know about the FTP protocol and what it does. You probably also know that FTP can be inherently insecure. There are several ways to make FTP sessions more secure. We mentioned previously that you can use FTP software that randomizes which ports are selected to transfer each file. You can also select passive mode instead of active mode (most FTP clients default to passive). The difference is that in passive mode the server is required to open ports for incoming traffic, and in active mode both the server and the client open ports. Then, you could use an FTP protocol that is secured through encryption. Two examples are Secure FTP (SFTP) and FTP Secure (FTPS). SFTP uses SSH port 22 to make connections to other systems. Because of this it is also known as SSH FTP. However, FTPS works with SSL or TLS, and (in implicit mode) it uses ports 990 (control port) and 989 (data port) to make secure connections and send data, respectively. FTPS can work in two modes: explicit mode and the previously mentioned implicit mode. In explicit mode the FTPS client must explicitly request security from an FTPS server and then mutually agree on the type of encryption to be used. In implicit mode, there is no negotiation, and the client is expected to already know the type of encryption used by the server. In general, implicit mode is considered to be more secure than explicit mode. So, in summary, regular FTP uses port 21 as the control port by default, and possibly port 20 to do data transfers—or (and more likely), it uses random ports for data transfers, if the software allows it. SFTP uses port 22. FTPS uses port 990 to make connections, and port 989 to transfer data by default. TFTP (which is not really secure) uses port 69.

On a separate note, another file transfer program, Secure Copy (SCP), is another example of a protocol that uses another protocol (and its corresponding port). It uses SSH, and ultimately uses port 22 to transfer data.

All those acronyms can be difficult to keep straight at times. Hopefully this section alleviates some of the confusion. For more help, be sure to memorize Table 6-2 to the best of your ability for the exam, and don't be afraid to ask me questions on my website!

Malicious Attacks

There are many types of malicious network attacks. We've mentioned some of these attacks in the preceding chapters as they relate to secure computing, but in this section we will better define them. Some attacks are similar to others, making it difficult to differentiate between them. Because of this, I've listed simple definitions and examples of each, plus mitigating techniques, and summarized them at the end of this section.

DoS

Denial-of-service (DoS) is a broad term given to many different types of network attacks that attempt to make computer resources unavailable. Generally this is done to servers but could also be perpetuated against routers and other hosts. DoS attacks can be implemented in several ways, as listed here:

- **Flood attack:** An attacker sends many packets to a single server or other host in an attempt to disable it. There are a few ways to accomplish this, including:
 - **Ping flood:** Also known as an ICMP flood attack, this is when an attacker attempts to send many ICMP echo request packets (pings) to a host in an attempt to use up all available bandwidth. This works only if the attacker has more bandwidth available than the target. To deter this attack, configure the system not to respond to ICMP echoes. You might have noticed that several years ago, you could ping large companies' websites and get replies. But after ping floods became prevalent, a lot of these companies disabled ICMP echo replies. For example, try opening the command prompt and typing `ping microsoft.com` (Internet connection required). It should result in Request Timed Out, which tells you that Microsoft has disabled this.
 - **Smurf attack:** Also sends large amounts of ICMP echoes, but this particular attack goes a bit further. The attacking computer broadcasts the ICMP echo requests to every computer on its network or subnet-work. In addition, in the header of the ICMP echo requests will be a spoofed IP address. That IP address is the target of the Smurf attack. Every computer that replies to the ICMP echo requests will do so to the spoofed IP. Don't forget that the original attack was broadcast, so, the more systems on the network (or subnetwork), the more echo replies that are sent to the target computer. There are several defenses for this attack, including configuring hosts not to respond to pings or ICMP echoes, configuring routers not to forward packets directed to broadcast addresses, implementing subnetting with smaller subnetworks, and employing network ingress filtering in an attempt to drop packets that contain forged or spoofed IP addresses (especially

addresses on other networks). These defenses have enabled most network administrators to make their networks immune to Smurf and other ICMP-based attacks. The attack can be automated and modified using the exploit code known as Smurf.c.

- **Fraggle:** Similar to the Smurf attack, but the traffic sent is UDP echoes. The traffic is directed to port 7 (Echo) and port 19 (CHARGEN). To protect against this attack, again, configure routers not to forward packets directed to broadcast addresses, employ network filtering, and disable ports 7 and 19. These ports are not normally used in most networks. The attack can be automated and modified using the exploit code known as Fraggle.c.

NOTE A similar attack is known as a UDP flood attack, which also uses the connectionless User Datagram Protocol. It is enticing to attackers because it does not require a synchronization process.

- **SYN flood:** Also known as a SYN attack, it occurs when an attacker sends a large amount of SYN request packets to a server in an attempt to deny service. Remember that in the TCP three-way handshake, a synchronization (SYN) packet is sent from the client to the server, then a SYN/ACK packet is sent from the server to the client, and finally, an acknowledgment (ACK) packet is sent from the client to the server. Attackers attempting a SYN flood either simply skip sending the ACK or spoof the source IP address in the original SYN. Either way, the server will never receive the final ACK packet. This ends up being a half-open connection. By doing this multiple times, an attacker seeks to use up all connection-oriented resources so that no real connections can be made. Some ways to defend against this include implementing **flood guards** (which can be implemented on some firewalls and other devices, otherwise known as attack guards), recycling half-open connections after a predetermined amount of time, and using intrusion detection systems (IDSs) to detect the attack. You can find more information about IDSs in Chapter 7 and more information about SYN flood attacks and mitigation techniques at the following link:
<http://tools.ietf.org/html/rfc4987>
- **Xmas attack:** Also known as the Christmas Tree attack or TCP Xmas Scan attack, it can deny service to routers and other devices, or simply cause them to reboot. It is based on the Christmas Tree packet, which can be generated by a variety of programs; for example, Nmap can be used (with the `-sx` parameter) to produce this scanning packet. This type of packet has the FIN, PSH, and URG flags set, which gives a

“Christmas Tree” appearance when viewing the flags in a network sniffer. If the packet is sent many times in a short period of time, it could possibly result in a DoS (why I placed this attack in the DoS flood section). But most routers and other devices today will block this type of packet, as it is a well-known attack. Otherwise, an IDS/IPS solution (if in place) can detect the packet and/or prevent the packet from denying service to a router or other device.

- **Ping of Death:** POD is an attack that sends an oversized and malformed packet to another computer. It is an older attack; most computer operating systems today will not be affected by it, and most firewalls will block it before it enters a network. It entails sending a packet that is larger than 65,535 bytes in length, which according to RFC 791 is the largest size packet that can be used on a TCP/IP network without fragmentation. If a packet is sent that is larger than 65,535 bytes, it might overflow the target system’s memory buffers, which can cause several types of problems, including system crashes. Windows computers do not allow ping sizes beyond 65,500 bytes. For example, `ping destination -l 65500` will work, but `ping destination -l 66000` will not work. However, on some systems, this maximum limitation can be hacked in the Registry, and there are also third-party applications that can send these “larger than life” packets. To protect against this type of attack, configure hosts not to respond to pings or ICMP echoes, make sure that operating systems run the latest service packs and updates, update the firmware on any hardware-based firewalls, and update any software-based firewalls as well. POD can be combined with a ping flood, but because most firewalls will block one or more PODs, it doesn’t make much sense to attempt the attack, so most hackers opt for some other sort of packet flooding nowadays. This was one of the first DoS attacks. It and other attacks such as Nuke and WinNuke are considered by the security community to be deprecated.
- **Teardrop attack:** Sends mangled IP fragments with overlapping and oversized payloads to the target machine. This can crash and reboot various operating systems due to a bug in their TCP/IP fragmentation reassembly code. For example, Windows 7 and Vista are particularly susceptible to teardrop attacks. Linux and Windows systems should be upgraded to protect from this attack. There are also software downloads available on the Internet for teardrop detection.
- **Permanent DoS attack:** Generally consists of an attacker exploiting security flaws in routers and other networking hardware by flashing the firmware of the device and replacing it with a modified image. This is also known as phflashing, or PDoS.
- **Fork bomb:** Works by quickly creating a large number of processes to saturate the available processing space in the computer’s operating system. Running

processes can be “forked” to create other running processes, and so on. They are not considered viruses or worms but are known as “rabbit malware,” “wabbits,” or “bacteria” because they might self-replicate but do not infect programs or use the network to spread. They are still considered DoS attacks though, due to their ability to stop a system from functioning.

There are other types of DoS attacks, but that should suffice for now. Keep in mind that new DoS attacks are always being dreamed up (and implemented), so as a security administrator, you need to be ready for new attacks and prepared to exercise new mitigation techniques.

DDoS

A **distributed denial-of-service (DDoS)** attack is when a group of compromised systems attacks a single target, causing a DoS to occur at that host. A DDoS attack often utilizes a botnet. The unsuspecting computers in the botnet that act as attackers are known as zombies. A hacker starts the DDoS attack by exploiting a single vulnerability in a computer system and making that computer the zombie master, or DDoS master. The master system communicates with the other systems in the botnet. The attacker often loads malicious software on many computers (zombies). The attacker can launch a flood of attacks by all zombies in the botnet with a single command. DDoS attacks and botnets are often associated with exploit kits (such as the Blackhole kit) and ransomware.

DoS and DDoS attacks are difficult to defend against. Other than the methods mentioned previously in the DoS section, these attacks can be prevented to some extent by updated stateful firewalls, switches, and routers with access control lists, intrusion prevention systems (IPSS), and proactive testing. Several companies offer products that simulate DoS and DDoS attacks. By creating a test server and assessing its vulnerabilities with simulated DoS tests, you can find holes in the security of your server before you take it live. A quick web search for “DoS testing” shows a few of these simulation test companies. An organization could also opt for a “clean pipe,” which attempts to weed out DDoS attacks, among other attacks. This solution is offered as a service by Verisign and other companies. Finally, if you do realize that a DDoS attack is being carried out on your network, call your ISP and request that this traffic be redirected.

Sinkholes and Blackholes

To combat DoS and DDoS attacks, security admins have the option to employ or make use of sinkholes, blackholes, and blackhole lists. A DNS sinkhole is a DNS server that can be configured to hand out false information to bots, and can detect and block malicious traffic by redirecting it to nonroutable addresses. However the

sinkhole can also be used maliciously to redirect unwary users to unwanted IP addresses and domains. A DNS blackhole is similar; it can be used to identify domains used by spammers, domains that contain malware, and so on, and block traffic to those domains. A DNS blackhole list (DNSBL) is a published list of IP addresses within DNS that contains the addresses of computers and networks involved in spamming and other malicious activity such as DDoS attacks initiated by botnets. The list can be downloaded and used on an organization's DNS server to help block zombie computers and botnets.

Spoofing

A **spoofing** attack is when an attacker masquerades as another person by falsifying information. There are several types of spoofing attacks. The man-in-the-middle attack is not only a form of session hijacking (which we discuss in the next section), but it is also considered spoofing. Internet protocols and their associated applications can also be spoofed, especially if the protocols were poorly programmed in the first place. Web pages can also be spoofed in an attempt to fool users into thinking they are logging in to a trusted website; this is known as URL spoofing and is used when attackers are fraudulently **phishing** for information such as usernames, passwords, credit card information, and identities. Phishing can also be done through a false e-mail that looks like it comes from a valid source. Often, this is combined with e-mail address spoofing, which hides or disguises the sender information. Defending against these types of spoofing attacks is difficult, but by carefully selecting and updating applications that your organization uses, and through user awareness, spoofing can be held down to a minimum and when necessary ignored.

Just about anything can be spoofed if enough work is put into it, and IP addresses are no exception. IP address spoofing is when IP packets are created with a forged source IP address in the header. This conceals where the packets originated from. Packet filtering and sessions that repeat authentication can defend against this type of spoofing. Also, updating operating systems and firmware and using newer operating systems and network devices helps to mitigate risks involved with IP spoofing. IP spoofing is commonly used in DoS attacks, as mentioned earlier, and is also common in TCP/IP hijacking, which we discuss more in the next section. MAC addresses can also be spoofed. MAC addresses are usually unique, which helps to identify a particular system. This is the best type of address to use to identify a malicious insider or other attacker, because it is more difficult to modify than an IP address. However, there are methods for attackers to change the MAC address of a network adapter (or mask it) so that the system cannot be identified properly.

A World Wide Name (WWN) can be spoofed too. World Wide Names (and their derivatives, pWWN and nWWN) are unique identifiers for SAS, ATA, and Fibre Channel equipment that are common to storage area networks (SANs). It's not

really a name, but a hexadecimal address that includes a 3-byte vendor identifier and a 3-byte vendor-specified serial number. An attacker that is masquerading as an authorized WWN can be prevented by challenging the attacker to give unique information only known to an authorized user or device. For a user this might be information that corresponds to a password. For devices, a secret is associated with the WWN of the port on the SAN switch. Proper authentication is also beneficial when combating these types of spoof attacks.

Session Hijacking

Session hijacking is the exploitation of a computer session in an attempt to gain unauthorized access to data, services, or other resources on a computer. A few types of session hijacks can occur:

- **Session theft:** Can be accomplished by making use of packet header manipulation (see Chapter 4, “Application Security”) or by stealing a cookie from the client computer, which authenticates the client computer to a server. This is done at the application layer, and the cookies involved are often based off their corresponding web applications (such as WWW sessions). This can be combated by using encryption and long random numbers for the session key, and regeneration of the session after a successful login. The Challenge Handshake Authentication Protocol (CHAP) can also be employed to require clients to periodically re-authenticate. However, session hijacking can also occur at the network layer—for example, TCP/IP hijacking.
- **TCP/IP hijacking:** A common type of session hijacking, due to its popularity among hackers. It is when a hacker takes over a TCP session between two computers without the need of a cookie or any other type of host access. Because most communications’ authentication occurs only at the beginning of a standard TCP session, a hacker can attempt to gain access to a client computer anytime after the session begins. One way would be to spoof the client computer’s IP address, then find out what was the last packet sequence number sent to the server, and then inject data into the session before the client sends another packet of information to the server. Remember the three-way handshake that occurs at the beginning of a session; this is the only authentication that occurs during the session. A synchronization (SYN) packet is sent by the client to the server, then a SYN/ACK packet is sent by the server to the client, and finally, an acknowledgment (ACK) packet is sent by the client to the server. An attacker can jump in anytime after this process and attempt to steal the session by injecting data into the data stream. This is the more difficult part; the attacker might need to perform a DoS attack on the client to stop it from sending anymore packets so that the packet sequence number doesn’t increase. In contrast, UDP sessions are easier to hijack because no packet

sequence numbers exist. Targets for this type of attack include online games and also DNS queries. To mitigate the risk of TCP/IP hijacking, employ encrypted transport protocols such as SSL, IPsec, and SSH. For more information about these encryption protocols, see Chapter 14, “PKI and Encryption Protocols.”

- **Blind hijacking:** When an attacker blindly injects data into a data stream without being able to see whether the injection was successful. The attacker could be attempting to create a new administrator account or gain access to one.
- **Man-in-the-middle (MITM):** These attacks intercept all data between a client and a server. It is a type of active interception. If successful, all communications now go through the MITM attacking computer. The attacking computer can at this point modify the data, insert code, and send it to the receiving computer. This type of eavesdropping is only successful when the attacker can properly impersonate each endpoint. Cryptographic protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) address MITM attacks by using a mutually trusted third-party certification authority (CA). These public key infrastructures (PKIs) should use strong mutual authentication such as secret keys and strong passwords. For more information about PKI, see Chapter 14.
- **Man-in-the-browser (MITB):** Similar to MITM, this attack makes use of a Trojan (from a proxy location) that infects a vulnerable web browser and modifies web pages and online transactions, in an attempt to ultimately steal money or data. For example, a user might make an online banking transaction, and the user would see confirmation of the exact transaction, but on the banking side, a different amount might have been actually transferred, with some of it going to a different location altogether. This can be prevented by updating the web browser, using transaction verification (often third-party), and updating the anti-malware on the computer in question.
- **Watering hole attack:** This targeted attack is when an attacker profiles the websites that the intended victim accesses. The attacker then scans those websites for possible vulnerabilities. If the attacker locates a website that can be compromised, the website is then injected with a JavaScript or other similar code injection that is designed to redirect the user when the user returns to that site (also known as a pivot attack). The user is then redirected to a site with some sort of exploit code...and the rest is, well, history. The purpose is to infect computers in the organization’s network, thereby allowing the attacker to gain a foothold in the network for espionage or other reasons. Watering hole attacks are often designed to profile users of specific organizations, and as such, an organization should develop policies to prevent these attacks. This can be done by updating anti-malware applications regularly, and by other

security controls mentioned in Chapters 2 and 3, but also by using secure virtual browsers that have little connectivity to the rest of the system and the rest of the network. To avoid having a website compromised as part of this attack, the admin should use proper programming methods (discussed in Chapter 4) and scan the website for malware regularly.

On a semi-related note, *cross-site scripting (XSS)* is a type of vulnerability found in web applications that is used with session hijacking. The attacker manipulates a client computer into executing code that is considered trusted as if it came from the server the client was connected to. In this way, the hacker can acquire the client computer's session cookie (enabling the hacker to steal sensitive information) or exploit the computer in other ways. See Chapter 4 for ways on how to prevent XSS.

Replay

A **replay attack** is a network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This differs from session hijacking in that the original session is simply intercepted and analyzed for later use. In a replay attack a hacker might use a packet sniffer to intercept data and retransmit it later. In this way the hacker can impersonate the entity that originally sent the data. For example, if customers were to log in to a banking website with their credentials while an attacker was watching, the attacker could possibly sniff out the packets that include the usernames and passwords and then possibly connect with those credentials later on. Of course, if the bank uses SSL or TLS to secure login sessions, then the hacker would have to decrypt the data as well, which could prove more difficult. An organization can defend against this attack in several ways. The first is to use session tokens that are transmitted to people the first time they attempt to connect, and identify them subsequently. They are handed out randomly so that attackers cannot guess at token numbers. The second way is to implement timestamping and synchronization as in a Kerberos environment. A third way would be to use a time-stamped **nonce**, a random number issued by an authentication protocol that can be used only one time. We talk more about SSL, TLS, Kerberos, and other cryptographic solutions in Chapter 14.

NOTE A replay attack should not be confused with SMTP relay, which is when one server forwards e-mail to other e-mail servers.

Null Sessions

A **null session** is a connection to the Windows interprocess communications share (IPC\$). The null session attack is a type of exploit that makes unauthenticated NetBIOS connections to a target computer. The attack uses ports 139 and 445, which are the NetBIOS session port and the Server Message Block port, respectively. If successful, an attacker could find user IDs, share names, and various settings and could possibly gain access to files, folders, and other resources. An example of the initial code an attacker might use is

```
net use \\IP address\ipc$ "" /U: ""
```

Afterward, the attacker might use a program such as enum.exe or something similar to extract information from the remote computer, such as usernames. Finally, an attacker might use a brute-force attack in an attempt at cracking passwords and gaining more access.

To protect against this attack, computers should be updated as soon as possible. However, the best way to defend against this attack is to filter out traffic on ports 139 and 445 with a firewall or a host-based intrusion prevention system. When a firewall is enabled, ports 139 and 445 will not appear to exist.

NOTE Command-line scripting in general can be used for legitimate and illegitimate purposes: The former by security administrators, and the latter by malicious insiders. Tools such as the Command Prompt, PowerShell, Windows Scripting Host, and the command-line in general, can all be used for malevolent purposes. To that effect, operating systems should be updated and patched often, and access to these programs should be secured through the use of permissions, UAC, and other similar tools.

Transitive Access and Client-Side Attacks

Transitive access is not really a specific attack, but a way or means of attacking a computer. It is based on the transitive property in mathematics, which states that whenever A is equal to B, and B is equal to C, then A is equal to C, summed up as

If $A = B$ and $B = C$, then $A = C$

That's just a piece of the transitive property, but you get the gist of it. What we are really dealing with here is trust. Does one computer on the LAN trust another? Can that trust be manipulated? For example, let's say that computer C is a server that hosts a database. Now, let's say that computer B is a client on the LAN that

frequently accesses the database and is authorized to do so. This is all well and good, and is normal. However, add in the attacker, at computer A. If the attacker can somehow create a trusted environment between computer A and computer B, then by way of transitivity, the attacker can obtain a trust with computer C, and then the database can become compromised. Normally, the attacker at computer A cannot access the database at computer C. But by compromising computer B, the attacker can then launch a client-side attack, one that is coming from a computer on the LAN that would otherwise be harmless.

Trusting relationships are created between computers (and sometimes networks) to save time and to bypass authentication methods. It would seem like a good idea at first, but when you think of all the vulnerable operating systems and applications on client computers, each one of which is a possible opening for transitive access, it makes sense that nowadays the general rule is to have every client computer authenticated whenever any session is started to another computer (perhaps even twice!). Implementing this practice along with the use of firewalls, intrusion detection/prevention systems, and updates is the best way to prevent transitive access and client-side attacks. In many environments, the rule is that no one computer should trust any other by default, and if a computer needs to do so, it happens only temporarily, and in a secure fashion.

DNS Poisoning and Other DNS Attacks

DNS poisoning (or DNS cache poisoning) is the modification of name resolution information that should be in a DNS server's cache. It is done to redirect client computers to incorrect websites. This can happen through improper software design, misconfiguration of name servers, and maliciously designed scenarios exploiting the traditionally open architecture of the DNS system. Let's say a client wants to go to www.comptia.org. That client's DNS server will have a cache of information about domain names and their corresponding IP addresses. If CompTIA's site were visited in the recent past by any client accessing the DNS server, its domain name and IP should be in the DNS server's cache. If the cache is poisoned, it could be modified in such a way to redirect requests for www.comptia.org to a different IP address and website. This other site could be a phishing site or could be malicious in some other way. This attack can be countered by using Transport Layer Security (TLS) and digital signatures or by using Secure DNS (DNSSEC), which uses encrypted electronic signatures when passing DNS information, and finally, by patching the DNS server.

Unauthorized zone transfers are another bane to DNS servers. Zone transfers replicate the database that contains DNS data; they operate on top of TCP. If a zone transfer is initiated, say through a reconnaissance attack, server name and IP address information can be stolen, resulting in the attacker accessing various

hosts by IP address. To defend against this, zone transfers should be restricted and audited in an attempt to eliminate unauthorized zone transfers and to identify anyone who tries to exploit the DNS server in this manner. Vigilant logging of the DNS server and the regular checking of DNS records can help detect unauthorized zone transfers.

A Windows computer's hosts file can also be the victim of attack. The hosts file is used on a local computer to translate or resolve hostnames to IP addresses. This is the predecessor to DNS, and although the file is normally empty of entries, it is still read and parsed by Windows operating systems. Attackers may attempt to hijack the hosts file in an attempt to alter or poison it or to try to have the client bypass DNS altogether. The best defense for this is to modify the computer's hosts file permissions to read-only. It is located at the following path: \SystemRoot\System32\drivers\etc.

If the file has already been hijacked, and you don't use the file for any static entries, delete it, and Windows should re-create it automatically at the next system startup. If Windows does not, then a standard hosts file can be easily re-created by simply making a blank hosts.txt file and placing it in the path mentioned previously. The hosts file is used by some people as a security measure as well. This is done by adding entries that redirect known bad domains to other safe locations or the localhost. Generally this is done in conjunction with disabling the DNS client service. However, in general, the DNS client service is required by the average Windows user.

Hosts files and vulnerable DNS software can also be victims of pharming attacks. **Pharming** is when an attacker redirects one website's traffic to another website that is bogus and possibly malicious. Pharming can be prevented by carefully monitoring DNS configurations and hosts files. Unfortunately, if an ISP's DNS server is compromised, that will be passed on to all the small office/home office routers that the ISP services. So it becomes more important for end users to be conscious of pharming. They can prevent it by turning on phishing and pharming filters within the browser, and by being careful of which websites they access. Users can also check their local hosts files. By default, the file doesn't have any entries, so if they see entries and have never modified the file themselves, they should either delete the entries or delete the file entirely.

Although it is less of an actual attack, **domain name kiting** (or simply domain kiting) is the process of deleting a domain name during the five-day grace period (known as the add grace period, or AGP) and immediately reregistering it for another five-day period. This process is repeated any number of times with the end result of having the domain registered without ever actually paying for it. It is a malicious attack on the entire Domain Name System by misusing the domain-tainting grace period. The result is that a legitimate company or organization often cannot secure the domain name of its choice.

As you can see, the DNS server can be the victim of many attacks due to its visibility on the Internet. It should be closely monitored at all times. Other highly visible servers such as web servers and mail servers should be likewise monitored, audited, and patched as soon as updates are available.

ARP Poisoning

The Address Resolution Protocol (ARP) resolves IP addresses to MAC addresses. Any resolutions that occur over a set amount of time are stored in the ARP table. The ARP table can be poisoned or spoofed. **ARP poisoning** is an attack that exploits Ethernet networks, and it may enable an attacker to sniff frames of information, modify that information, or stop it from getting to its intended destination. The spoofed frames of data contain a false source MAC address, which deceives other devices on the network. The idea behind this is to associate the attacker's MAC address with an IP address of another device, such as a default gateway or router, so that any traffic that would normally go to the gateway would end up at the attacker's computer. The attacker could then perpetuate a man-in-the-middle attack, or a denial-of-service attack, in addition to MAC flooding. Some of the defenses for ARP poisoning include VLAN segregation/VLAN separation (creating multiple virtual LANs in an effort to thwart the attack), DHCP snooping, and an open source program called ArpON (<http://arp0n.sourceforge.net/>).

Summary of Network Attacks

Table 6-3 lists important network attacks and mitigation techniques.

Table 6-3 Summary of Important Network Attacks and Mitigation Techniques to Know for the Exam



Network Attack	Description	Mitigation Techniques
MAC flooding	A MAC flood sends numerous packets to the switch, each of which has a different source MAC address, in an attempt to use up the memory on the switch.	Implement 802.1X. Use port security. Implement dynamic VLANs and NIDSs. Consistently monitor the network.

Network Attack	Description	Mitigation Techniques
VLAN hopping	The act of gaining access to traffic on other VLANs that would not normally be accessible by jumping from one VLAN to another.	<p>Put unplugged ports on the switch into an unused VLAN.</p> <p>Configure the switch ports in charge of passing tagged frames to be trunks and to explicitly forward specific tags.</p>
Ping flood	Type of DoS. When an attacker sends many ICMP echo request packets (pings) to a host in an attempt to use up all available bandwidth.	<p>Pick an unused VLAN as the default VLAN for all trunks, and do not use it for any other intent.</p> <p>Avoid using default VLAN names such as VLAN or VLAN1.</p>
Smurf attack	Type of DoS. Sends large amounts of ICMP echoes, broadcasting the ICMP echo requests to every computer on its network or subnetwork. The header of the ICMP echo requests will have a spoofed IP address. That IP address is the target of the Smurf attack. Every computer that replies to the ICMP echo requests will do so to the spoofed IP.	<p>Configure the system not to respond to ICMP echoes.</p> <p>Configure hosts not to respond to pings or ICMP echoes.</p> <p>Configure routers not to forward packets directed to broadcast addresses.</p> <p>Implement subnetting with smaller subnetworks.</p> <p>Employ network ingress filtering.</p>
Fraggle	Type of DoS. Similar to the Smurf attack, but the traffic sent is UDP echo traffic as opposed to ICMP echo traffic.	<p>Configure routers not to forward packets directed to broadcast addresses.</p> <p>Employ network filtering, disabling ports 7 and 19.</p>
SYN flood	Type of DoS. When an attacker sends a large amount of SYN request packets to a server in an attempt to deny service.	<p>Recycle half-open connections after a predetermined amount of time.</p> <p>Use intrusion detection systems (IDSs) to detect the attack.</p>

Network Attack	Description	Mitigation Techniques
Ping of Death	Type of DoS. Sends an oversized and malformed packet to another computer.	<p>Configure hosts not to respond to pings or ICMP echoes.</p> <p>Verify operating systems are running the latest service packs and updates.</p> <p>Update the firmware on any hardware-based firewalls, and update any software-based firewalls as well.</p>
Teardrop attack	Type of DoS. Sends mangled IP fragments with overlapping and oversized payloads to the target machine.	<p>Upgrade operating systems.</p> <p>Consider third-party downloads.</p>
DDoS	When a group of compromised systems attacks a single target, causing a DoS to occur at that host, usually using a botnet.	<p>Update firewalls.</p> <p>Use IPS.</p> <p>Utilize a “clean pipe.”</p>
Spoofing	When an attacker masquerades as another person by falsifying information.	<p>Carefully select applications.</p> <p>User awareness.</p> <p>In the case of IP spoofing, incorporate packet filtering, and repeat authentication schemes.</p>
Session theft	When an attacker attempts to steal a user’s session using the owner’s cookie and authentication information.	<p>Use encryption.</p> <p>Use CHAP.</p>
TCP/IP hijacking	When a hacker takes over a TCP session between two computers without the need of a cookie or any other type of host access.	<p>Employ encrypted transport protocols such as SSL, IPsec, and SSH.</p>
Man-in-the-middle (MITM)	Form of eavesdropping that intercepts all data between a client and a server, relaying that information back and forth.	<p>Implement SSL/TLS using a mutually trusted third-party certification authority.</p>
Man-in-the-browser (MITB)	Infects a vulnerable web browser in the hopes of modifying online transactions.	<p>Update the web browser.</p> <p>Use a virtual browser.</p> <p>Use transaction verification.</p> <p>Update anti-malware.</p>

Network Attack	Description	Mitigation Techniques
Watering hole attack	When websites the victim visits are profiled, infected, and ultimately redirect the victim to illegitimate sites.	Update the browser or use a virtual browser or VM. Update anti-malware programs. Harden the system.
Replay attack	Valid data transmission is maliciously or fraudulently repeated or delayed.	Use session tokens. Implement timestamping and synchronization. Use a nonce.
Null session	A connection to the Windows interprocess communications share (IPC\$).	Update computers. Filter ports 139 and 445.
Transitive access	When one computer uses a second computer to attack a third, based on the trust of the second and third computers.	Authentication. Firewalls. IDS/IPS. Updates.
DNS poisoning	The modification of name resolution information that should be in a DNS server's cache.	Use TLS. Utilize Secure DNS.
Unauthorized zone transfers	Unauthorized transfer of DNS information from a DNS server.	Log the DNS server. Restrict and audit the DNS server.
Altered hosts file	When an attacker attempts to hijack the hosts file and have the client bypass the DNS server or access incorrect websites.	Change permission on the hosts file to read-only.
Domain name kiting	The process of deleting a domain name during the 5-day grace period (known as the add grace period, or AGP) and immediately reregistering it for another 5-day period.	Not many ways to defend against this other than creating rules that charge fees for people who kite domain names.
ARP poisoning	An attack that exploits Ethernet networks, and it may enable an attacker to sniff frames of information, modify that information, or stop it from getting to its intended destination.	VLAN segregation. DHCP snooping. Third-party tools like ArpON.

Chapter Summary

Just as cracks in a dam are vulnerabilities to anything standing in a nearby valley, open ports are vulnerabilities to computer networks. The teaming flood of network attacks is seemingly endless; and though new network attacks are constantly being devised, these threats have to be dealt with in a proactive manner.

All metaphors aside, this means you are required to have a thorough understanding of the many networking protocols in use today, and their corresponding port numbers. Knowledge of inbound ports is the most important because they correlate to the services that run on a server; these are the doorways that attackers use to access a system. Servers that run protocols such as HTTP, FTP, SMTP, and so on should be updated, hardened, and secured appropriately. Any nonessential protocols and services (such as the deprecated Telnet or, for instance, TFTP) should be stopped and disabled. This effectively closes the ports in question. You should memorize the ports mentioned in this chapter because you will be scanning for open ports such as these in upcoming chapters. If there is ever confusion about a port or protocol, remember to access the IANA website for more information.

The whole point of reducing the attack surface of a system is so that malicious network attacks will have a more difficult time accessing that system. For example, let's say you have a server running Microsoft Internet Information Services (IIS) and have a website running on it that uses HTTP, but you unknowingly also have FTP running on that server, using port 21. The server could be easy prey for attacks designed to infiltrate via port 21. But it doesn't have to be this way! Closing ports, disabling services, and, of course, using firewalls are vital defenses. Chapter 7 covers additional equipment such as network intrusion detection systems, proxies, and the varying types of firewalls.

In this day and age there is a cornucopia of network attacks. When observing your network and servers, attacks such as denial-of-service (DoS), distributed DoS (DDoS), spoofing, session hijacking, replay, and DNS/ARP poisoning should be at the top of your list. But the security administrator must wear multiple hats. In addition to investigator, one of your roles is that of researcher. You must study the latest attacks and CVEs for a system, watch for updates and bulletins, and visit online forums and discussion groups often. However, the role of "watcher" is probably one of the best descriptive terms for a security administrator. You must constantly scrutinize your servers and network equipment. This everlasting vigil is part of the job. Those who are alert and observant shall prevail, and those who are not...well, they risk the danger of becoming enveloped by the flood of threats that lurks just outside (and sometimes inside) the computer network.

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 6-4 lists a reference of these key topics and the page number on which each is found.

Table 6-4 Key Topics for Chapter 6

Key Topic Element	Description	Page Number
Table 6-2	Ports and their associated protocols	228
Figure 6-2	IP addresses and ports	232
Table 6-3	Summary of network attacks and mitigation techniques	247

Define Key Terms

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

denial-of-service (DoS), ping flood, Smurf attack, Fragle, SYN flood, flood guard, Ping of Death, teardrop attack, permanent DoS attack, fork bomb, distributed denial-of-service (DDoS), spoofing, phishing, TCP/IP hijacking, man-in-the-middle (MITM), man-in-the-browser (MITB), watering hole attack, replay attack, nonce, null session, DNS poisoning, pharming, domain name kit-ing, ARP poisoning

Review Questions

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

1. Which of the following is an example of a nonessential protocol?
 - A. DNS
 - B. ARP
 - C. TCP
 - D. TFTP

2. A person attempts to access a server during a zone transfer to get access to a zone file. What type of server are they trying to manipulate?
 - A. Proxy server
 - B. DNS server
 - C. File server
 - D. Web server
3. Which one of the following can monitor and protect a DNS server?
 - A. Ping the DNS server.
 - B. Block port 53 on the firewall.
 - C. Purge PTR records daily.
 - D. Check DNS records regularly.
4. Which TCP port does LDAP use?
 - A. 389
 - B. 80
 - C. 443
 - D. 143
5. From the list of ports select two that are used for e-mail. (Select the two best answers.)
 - A. 110
 - B. 3389
 - C. 143
 - D. 389
6. Which port number does the Domain Name System use?
 - A. 53
 - B. 80
 - C. 110
 - D. 88

7. John needs to install a web server that can offer SSL-based encryption. Which of the following ports is required for SSL transactions?
 - A. Port 80 inbound
 - B. Port 80 outbound
 - C. Port 443 inbound
 - D. Port 443 outbound
8. If a person takes control of a session between a server and a client, it is known as what type of attack?
 - A. DDoS
 - B. Smurf
 - C. Session hijacking
 - D. Malicious software
9. Making data appear as if it is coming from somewhere other than its original source is known as what?
 - A. Hacking
 - B. Phishing
 - C. Cracking
 - D. Spoofing
10. Which of the following enables a hacker to float a domain registration for a maximum of five days?
 - A. Kiting
 - B. DNS poisoning
 - C. Domain hijacking
 - D. Spoofing
11. What is the best definition for ARP?
 - A. Resolves IP addresses to DNS names
 - B. Resolves IP addresses to hostnames
 - C. Resolves IP addresses to MAC addresses
 - D. Resolves IP addresses to DNS addresses

- 12.** You have three e-mail servers. What is it called when one server forwards e-mail to another?
- A.** SMTP relay
 - B.** Buffer overflows
 - C.** POP3
 - D.** Cookies
- 13.** A coworker goes to a website but notices that the browser brings her to a different website and that the URL has changed. What type of attack is this?
- A.** DNS poisoning
 - B.** Denial of service
 - C.** Buffer overflow
 - D.** ARP poisoning
- 14.** Which of the following misuses the Transmission Control Protocol handshake process?
- A.** Man-in-the-middle attack
 - B.** SYN attack
 - C.** WPA attack
 - D.** Replay attack
- 15.** For a remote tech to log in to a user's computer in another state, what inbound port must be open on the user's computer?
- A.** 21
 - B.** 389
 - C.** 3389
 - D.** 8080
- 16.** A DDoS attack can be best defined as what?
- A.** Privilege escalation
 - B.** Multiple computers attacking a single server
 - C.** A computer placed between a sender and receiver to capture data
 - D.** Overhearing parts of a conversation

- 17.** When users in your company attempt to access a particular website, the attempts are redirected to a spoofed website. What are two possible reasons for this?
 - A.** DoS
 - B.** DNS poisoning
 - C.** Modified hosts file
 - D.** Domain name kiting
- 18.** What kind of attack is it when the packets sent do not require a synchronization process and are not connection-oriented?
 - A.** Man-in-the-middle
 - B.** TCP/IP hijacking
 - C.** UDP attack
 - D.** ICMP flood
- 19.** How many of the TCP/IP ports can be attacked?
 - A.** 1,024 ports
 - B.** 65,535
 - C.** 256
 - D.** 16,777,216
- 20.** Which of the following attacks is a type of DoS attack that sends large amounts of UDP echoes to ports 7 and 19?
 - A.** Teardrop
 - B.** IP spoofing
 - C.** Fraggle
 - D.** Replay
- 21.** Don must configure his firewall to support TACACS+. Which port(s) should he open on the firewall?
 - A.** Port 53
 - B.** Port 49
 - C.** Port 161
 - D.** Port 22

- 22.** Which of the following ports is used by Kerberos by default?
- A.** 21
 - B.** 80
 - C.** 88
 - D.** 443
- 23.** Which of the following is the best option if you are trying to monitor network devices?
- A.** SNMP
 - B.** Telnet
 - C.** FTPS
 - D.** IPsec
- 24.** What is a secure way to remotely administer Linux systems?
- A.** SCP
 - B.** SSH
 - C.** SNMP
 - D.** SFTP
- 25.** Your web server that conducts online transactions crashed, so you examine the HTTP logs and see that a search string was executed by a single user masquerading as a customer. The crash happened immediately afterward. What type of network attack occurred?
- A.** DDoS
 - B.** DoS
 - C.** MAC spoofing
 - D.** MITM
- 26.** Which port number is used by SCP?
- A.** 22
 - B.** 23
 - C.** 25
 - D.** 443

- 27.** A malicious insider is accused of stealing confidential data from your organization. What is the best way to identify the insider's computer?
- A.** IP address
 - B.** MAC address
 - C.** Computer name
 - D.** NetBIOS name
- 28.** What is the best way to utilize FTP sessions securely?
- A.** FTPS
 - B.** FTP passive
 - C.** FTP active
 - D.** TFTP
- 29.** Which of the following is the most secure protocol for transferring files?
- A.** FTP
 - B.** SSH
 - C.** FTPS
 - D.** Telnet
- 30.** Which of the following protocols allow for the secure transfer of files? (Select the two best answers.)
- A.** SNMP
 - B.** SFTP
 - C.** TFTP
 - D.** SCP
 - E.** ICMP

Answers and Explanations

- 1. D.** TFTP (Trivial File Transfer Protocol) is a simpler version of FTP that uses a small amount of memory. It is generally considered to be a nonessential protocol. The Domain Name System service (or DNS service) is required for Internet access and on Microsoft domains. The Address Resolution Protocol (ARP) is necessary in Ethernet networks that use TCP/IP. TCP stands for Transmission Control Protocol, an essential part of most network communications.

2. **B.** DNS servers are the only types of servers listed that do zone transfers. The purpose of accessing the zone file is to find out what hosts are on the network.
3. **D.** By checking a DNS server's records regularly, a security admin can monitor and protect it. Blocking port 53 on a firewall might protect it (it also might make it inaccessible depending on the network configuration) but won't enable you to monitor it. Pinging the server can simply tell you whether the server is alive. Purging pointer records (PTR) cannot help to secure or monitor the server.
4. **A.** The Lightweight Directory Access Protocol (LDAP) uses port TCP 389. Port 80 is used by HTTP. Port 443 is used by HTTPS. Port 143 is used by IMAP.
5. **A. and C.** POP3 uses port 110; IMAP uses port 143; 3389 is used by the Remote Desktop Protocol; and 389 is used by LDAP.
6. **A.** The Domain Name System (DNS) uses port 53. Port 80 is used by HTTP; port 110 is used by POP3; and port 88 is used by Kerberos.
7. **C.** For clients to connect to the server via SSL, the server must have inbound port 443 open. The outbound ports on the server are of little consequence for this concept, and inbound port 80 is used by HTTP.
8. **C.** Session hijacking (or TCP/IP hijacking) is when an unwanted mediator takes control of the session between a client and a server (for example, an FTP or HTTP session).
9. **D.** Spoofing is when a malicious user makes data or e-mail appear to be coming from somewhere else.
10. **A.** Kiting is the practice of monopolizing domain names without paying for them. Newly registered domain names can be canceled with a full refund during an initial five-day window known as an AGP, or add grace period.
11. **C.** The Address Resolution Protocol, or ARP, resolves IP addresses to MAC addresses. DNS resolves from IP addresses to hostnames, and vice versa. RARP is Reverse ARP; it resolves MAC addresses to IP addresses.
12. **A.** The SMTP relay is when one server forwards e-mail to other e-mail servers. Buffer overflows are attacks that can be perpetuated on web pages. POP3 is another type of e-mail protocol, and cookies are small text files stored on the client computer that remember information about that computer's session with a website.
13. **A.** DNS poisoning can occur at a DNS server and can affect all clients on the network. It can also occur at an individual computer. Another possibility is that spyware has compromised the browser. A denial-of-service is a single

attack that attempts to stop a server from functioning. A buffer overflow is an attack that, for example, could be perpetuated on a web page. ARP poisoning is the poisoning of an ARP table, creating confusion when it comes to IP address-to-MAC address resolutions.

14. **B.** A synchronize (SYN) attack misuses the TCP three-way handshake process. The idea behind this is to overload servers and deny access to users.
15. **C.** Port 3389 must be open on the inbound side of the user's computer to enable a remote tech to log in remotely and take control of that computer. Port 21 is the port used by FTP, and 389 is used by LDAP. 8080 is another port used by web browsers that takes the place of port 80.
16. **B.** When multiple computers attack a single server, it is known as a distributed denial-of-service attack, or DDoS. Privilege escalation is when a person who is not normally authorized to a server manages to get administrative permissions to resources. If a computer is placed between a sender and receiver, it is known as a man-in-the-middle attack. Overhearing parts of a conversation is known as eavesdropping.
17. **B.** and **C.** DNS poisoning and a DNS server's modified hosts files are possible causes for why a person would be redirected to a spoofed website. DoS, or denial-of-service, is when a computer attempts to attack a server to stop it from functioning. Domain name kiting is when a person renews and cancels domains within five-day periods.
18. **C.** User Datagram Protocol (UDP) attacks, or UDP flood attacks, are DoS attacks that use a computer to send a large number of UDP packets to a remote host. The remote host will reply to each of these with an ICMP Destination Unreachable packet, which ultimately makes it inaccessible to clients.
19. **B.** The best answer to this question is 65,535. The Internet Assigned Numbers Authority (IANA) list of ports starts at 0 and ends at 65,535. Although this equals 65,536 ports, it should be known that normally port 0 (zero) will forward packets to another port number that is dynamically assigned. So port 0 should not be affected by attacks, because it actually doesn't act as a normal port.
20. **C.** A Fraggle attack is a type of DoS attack that sends large amounts of UDP echoes to ports 7 and 19. This is similar to the Smurf attack. Teardrop DoS attacks send many IP fragments with oversized payloads to a target. IP spoofing is when an attacker sends IP packets with a forged source IP address. The replay attack is when valid data transmissions are maliciously repeated or delayed.
21. **B.** Port 49 is used by TACACS+. Port 53 is used by DNS, port 161 is used by SNMP, and port 22 is used by SSH.

- 22.** C. Port 88 is used by Kerberos by default. Port 21 is used by FTP, port 80 is used by HTTP, and port 443 is used by HTTPS (TLS/SSL).
- 23.** A. SNMP (Simple Network Management Protocol) is the best protocol to use to monitor network devices. Telnet is a deprecated protocol that is used to remotely administer network devices. FTPS provides for the secure transmission of files from one computer to another. IPsec is used to secure VPN connections and other IP connections.
- 24.** B. SSH (Secure SHell) is used to remotely administer Unix/Linux systems and network devices. SCP (Secure Copy) is a way of transferring files securely between two hosts—it utilizes SSH. SNMP is used to remotely monitor network equipment. SFTP is used to securely transfer files from host to host—it also uses SSH.
- 25.** B. A denial-of-service (DoS) attack probably occurred. The attacker most likely used code to cause an infinite loop or repeating search, which caused the server to crash. It couldn't have been a DDoS (distributed denial-of-service) because only one attacker was involved. MAC spoofing is when an attacker disguises the MAC address of their network adapter with another number. MITM stands for the man-in-the-middle attack, which wasn't necessary since the attacker had direct access to the search fields on the web server.
- 26.** A. SCP (Secure Copy) uses SSH, which runs on port 22 by default. Port 23 is Telnet, port 25 is SMTP, and port 443 is HTTPS (SSL/TLS).
- 27.** B. The MAC address is the best way because it is unique and is the hardest to modify or spoof. IP addresses are often dynamically assigned on networks and are easily modified. Computer names (which are effectively NetBIOS names) can easily be changed as well.
- 28.** A. FTPS (FTP Secure) uses encryption in the form of SSL or TLS to secure file transfers. The other three options are basically variations on FTP; they do not use encryption, making them less secure.
- 29.** C. FTPS (FTP Secure) is the most secure protocol (listed) for transferring files. It uses SSL or TLS to secure FTP transmissions utilizing ports 989 and 990. FTP by itself is inherently insecure and uses port 21 by default. The truly distracting answer here, SSH, allows a person to remotely access another computer securely, but it's the Secure FTP (SFTP) protocol that works on top of SSH that is considered a secure way of transferring files. Telnet is outdated and insecure. Because of this it is not found on most of today's operating systems, but if it is, it should be removed, or at least stopped and disabled.
- 30.** B. and D. The Secure FTP (SFTP) and Secure Copy (SCP) protocols provide for the secure transfer of files. The Simple Network Management Protocol

(SNMP) is used to monitor various parts of the network. Trivial FTP (TFTP) is not secure by default. The Internet Control Message Protocol (ICMP) is the protocol initiated by ping to invoke responses from other computers.

Case Studies for Chapter 6

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

Case Study 6-1: Scanning Ports

Scenario: Your organization has some concerns about the attack surface of its servers. It is unknown what the vulnerabilities to the servers are at this point. Your task is to find out what ports are open on a web server and an FTP server. If any are unnecessary, you are to close or shield them.

Question 1: Which command-line tools can you use to find out which ports are open?

Question 2: Where would you go in Windows to secure the unnecessary ports?

Question 3: What is an example of a deprecated and most likely unnecessary port?

Case Study 6-2: Identifying Network Attacks

Scenario: You are interviewing for a job with a marketing company. The company's servers have been victims of various DoS attacks and other malicious network attacks over the past year. The company wants to employ a resourceful server technician who can quickly identify the different types of network attacks common today.

Your task is to research the three types of DoS attacks listed below and give a few examples of how they can be prevented.

- Smurf attack
-
-
-

- **SYN flood**

- **Teardrop attack**

Case Study Solutions

Case Study 6-1 Solution

There are many command-line tools available that can be used to scan for open ports on a computer. For example, in Windows you could use the `netstat` command, or download the `TCPView.exe` or `PortQry.exe` tools from Microsoft's website. A third-party tool, `Nmap`, is very popular and can be used on Windows and Linux platforms. A common way to use this tool is to type the following syntax:

```
nmap -sS [IP address]
```

You can also scan Internet-facing network adapters with syntax such as:

```
nmap -P0 [public IP address]
```

If there are nonessential ports open, turn off their corresponding unnecessary services. For instance, if the web server shows port 21 is open but doesn't need FTP running, stop the service (and disable it) in the services console window (`Run > services.msc`), or by using the `net` and `sc` commands in the Command Prompt. You could also configure the Windows Firewall (best option is with Advanced Security) to block or shield the appropriate ports, and create filters and rules.

An example of a deprecated port is port 23, used by Telnet. This utility is insecure and should be avoided. Windows XP was the last Microsoft operating system to use it, but you could easily find that operating system in use, in addition to the fact that some routers might have the Telnet protocol installed as well. You never know exactly what you might find on a network, even your own network. Port scanning allows you to find the open doorways.

Video Solution: Watch the video solution “6-1: Scanning Ports” on the accompanying disc.

Simulation: Complete the simulation “6-1: Understanding Port Numbers” Parts A, B, and C.

Case Study 6-2 Solution

DoS (and DDoS) attacks can harm routers and other various hosts, but are most commonly used to flood servers, causing them to only give intermittent data to clients, or fail altogether.

The Smurf attack sends large amounts of ICMP packets to multiple targets on a network in an attempt to flood their network interfaces, and the network in general. The most obvious defense is to filter ICMP traffic at the router or firewall. However, you could also use a NIDS solution, filter for spoofed IP addresses, or utilize subnetworking.

The SYN flood is when large amounts of SYN packets are sent to a server, rendering it inoperable. One way to prevent this is to implement flood control at the firewall (which can also help with Smurf and other DoS attacks). Another is to use an IDS.

The teardrop attack sends broken IP packets (fragments) in an attempt to crash the computer. To prevent this, utilize filtering and update and harden the OS.

Try to memorize the various network attacks covered in this chapter. This will undoubtedly help you on the job interview, as well as on the job itself. To help you remember them, run the following simulation from the disc.

Simulation: Complete the simulation “6-2: Identifying Network Attacks” Parts A, B, C, and D.

This page intentionally left blank



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 covers a portion of the CompTIA Security+ SY0-401 objectives 1.1, 1.2, and 3.6.

Network Perimeter Security

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.

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 a 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 11, “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. I’ll give some examples in the “Case Studies” section at the end of this chapter.

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 2, “Computer Systems Security,” 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 7-1.

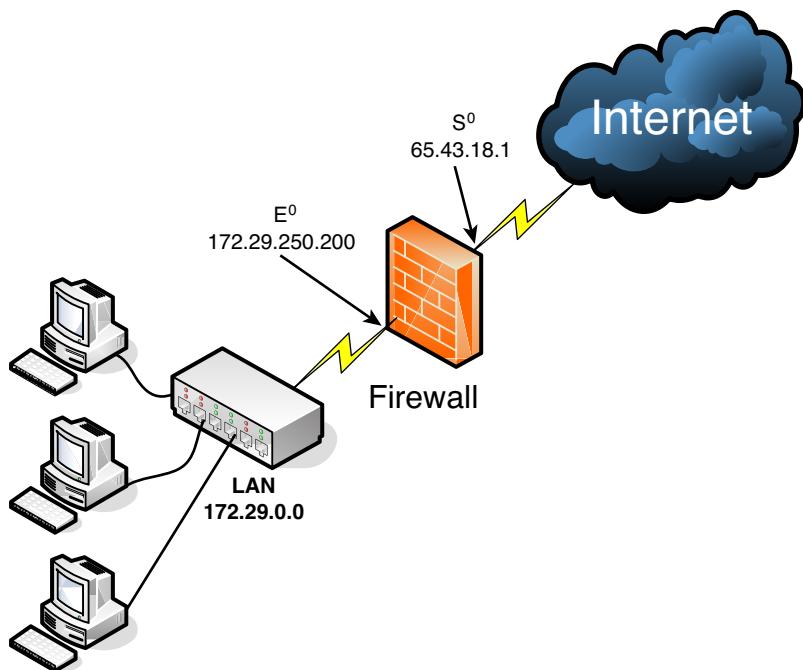


Figure 7-1 Diagram of a Basic Firewall Implementation

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 7-1, 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 a third-party application such as Nmap (www.nmap.org) or with a web-based port scanning utility such as ShieldsUP! (www.grc.com), as was shown in the Chapter 6 Case Study Video Solution. 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 11.

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). When dealing with 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 10, “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.davidlprowse.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:

- **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.

NOTE See the video solution “7-2: Configuring Packet Filtering and NAT” on the accompanying disc.

- **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 5, “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 7-2, or as a 3-leg perimeter configuration.

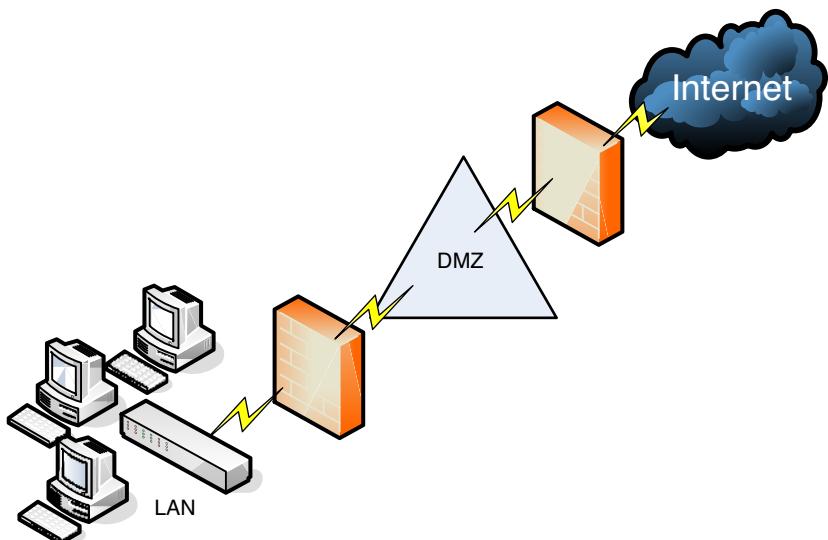
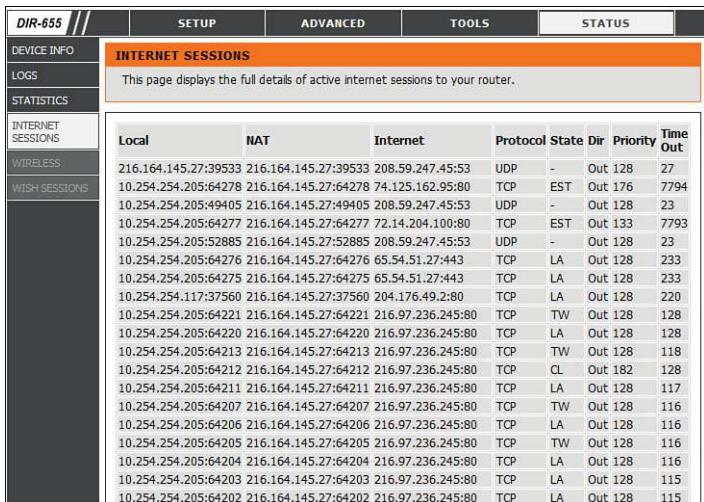


Figure 7-2 Back-to-Back Firewall/DMZ Configuration

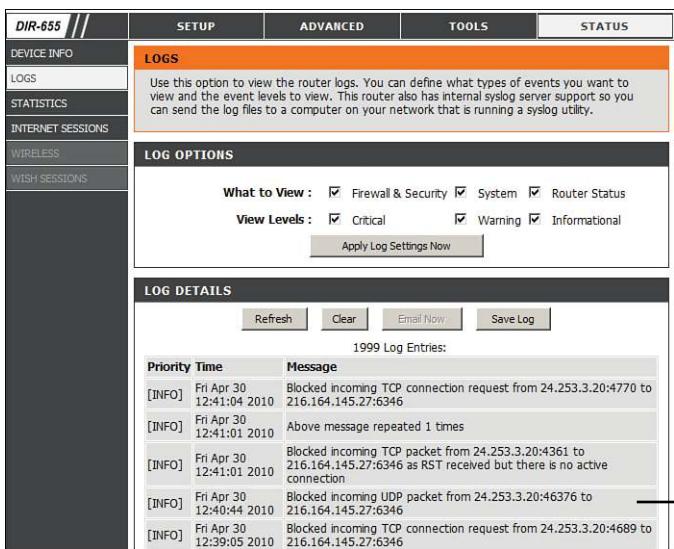
Generally, there will be one firewall with the network and all devices and computers residing “behind” it. By the way, if a device is “behind” the firewall, it is also considered to be “after” the firewall, and if the device is “in front of” the firewall, it is also known as being “before” the firewall. 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 7-3 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 a 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 everyone possible.



The screenshot shows the 'INTERNET SESSIONS' page of the D-Link DIR-655 router's web interface. The left sidebar has tabs for 'DEVICE INFO', 'LOGS', 'STATISTICS', 'INTERNET SESSIONS' (which is selected), 'WIRELESS', and 'WISH SESSIONS'. The main content area has tabs for 'SETUP', 'ADVANCED', 'TOOLS', and 'STATUS'. The 'INTERNET SESSIONS' tab is selected, displaying the following table:

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
10.254.254.205:64277	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



The screenshot shows the 'LOGS' page of the D-Link DIR-655 router's web interface. The left sidebar has tabs for 'DEVICE INFO', 'LOGS' (which is selected), 'STATISTICS', 'INTERNET SESSIONS', 'WIRELESS', and 'WISH SESSIONS'. The main content area has tabs for 'SETUP', 'ADVANCED', 'TOOLS', and 'STATUS'. The 'LOGS' tab is selected, displaying the following table:

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

A red arrow points from the text 'Blocked Gnutella packet' to the third log entry.

Figure 7-3 D-Link 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. Examples of network firewalls include basic devices such as the D-Link DIR-655 SOHO router/firewall, as shown in Figure 7-3, and more advanced appliances such as Cisco PIX/ASA Security Appliances and Juniper NetScreens. These are often referred to simply as "network firewalls." A firewall could also be incorporated into a server as a software package, which is a type of **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. Other well-known application firewall tools are offered by Barracuda Networks, Citrix, and F5. Some of these tools are designed to specifically protect HTTP sessions from XSS attacks and SQL injection. These types of tools are known as *web application firewalls*.

A network firewall usually has more than one network adapter so that it can connect to more than one network; this is known as a *multihomed connection*. An application firewall needs to be dual-homed at minimum (two adapters), and it is recommended that the server has three network adapters, in case that 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 home 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 8, “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:

- **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 5, 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 7-4. 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.

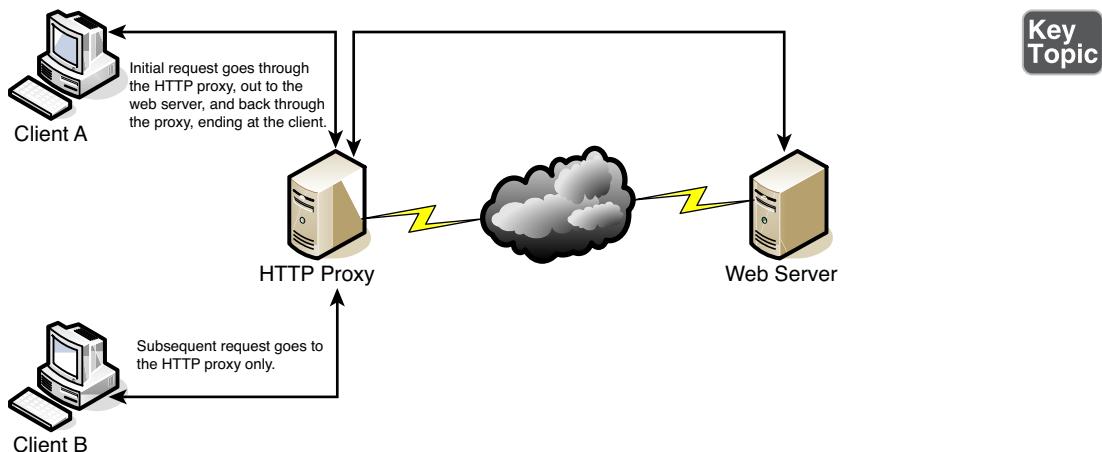


Figure 7-4 Illustration of an HTTP Proxy in Action

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.

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 (layer 7) 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 14, "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 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*.

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 bane 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)

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 often 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. There are three types of DLP systems:

- **Network-based DLP:** These systems deal with data in motion and are usually located on the perimeter of the network. If particular 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.
- **Endpoint-based DLP:** These systems operate on individual client computers or servers, but to be effective, need to be installed to every computer on the network (if a network-based DLP is not used). In some cases the software that controls these systems can notify the user (or an administrator) of any attempted confidentiality breach, whether inadvertent or deliberate.
- **Storage-based DLP:** These systems are usually software-based and are used to find out whether confidential information has found its way into long-term storage and data centers where, according to policy, it is not supposed to be.

Organizations such as Check Point offer DLP solutions, and a free open source application called MyDLP also has network-based, endpoint-based, and web server-based versions.

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 and 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 3, "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 (www.snort.org/), Bro (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 7-5 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

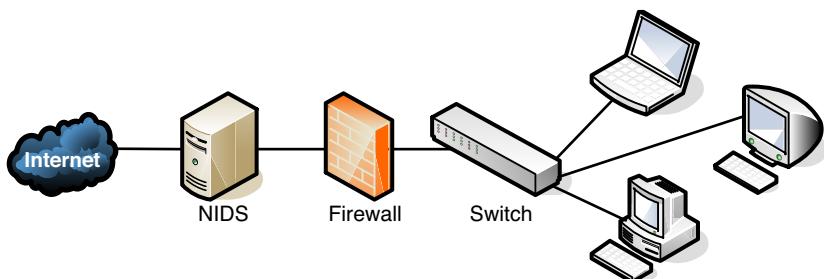


Figure 7-5 Illustration of NIDS Placement in a Network

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 only *detects* attacks; to protect against, or *prevent*, these attacks, 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 Extreme Networks' Intrusion Prevention System (www.extremenetworks.com), Check Point security appliances (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 about false positives and false negatives can be found in Chapter 9, “Physical Security and Authentication Models.” More information on signatures can be found in Chapter 3 and Chapter 12, “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 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 give 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 7-1 summarizes NIDS versus NIPS.



Table 7-1 Summary of NIDS Versus NIPS

Type of System	Summary	Disadvantage/Advantage	Example
NIDS	Detects malicious network activities	Pro: Only a limited amount of NIDSs are necessary on a network. Con: Only detects malicious activities.	Snort Bro IDS
NIPS	Detects, removes, deters, 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.	Extreme Networks & 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.

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. Companies such as Cisco, Fortinet, and McAfee (to name a few) offer UTM 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 have to 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. Access control lists (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. The clear and present danger is real, and should be enough to convince you to take strong measures to protect your network.

Oftentimes, the act of securing the network can also provide increased efficiency and productivity. For example, a proxy server can act to filter content, but saves time and bandwidth for commonly accessed web pages. 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.

If you can find the right balance of security and performance while employing your UTM 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 7-2 lists a reference of these key topics and the page number on which each is found.

Table 7-2 Key Topics for Chapter 7

Key Topic Element	Description	Page Number
Bullet list	Types of firewalls	271
Figure 7-2	Back-to-back firewall/DMZ configuration	272
Bullet list	Types of proxies	274

Key Topic Element	Description	Page Number
Figure 7-4	Illustration of an HTTP proxy in action	275
Figure 7-5	Illustration of NIDS placement in a network	280
Table 7-1	Summary of NIDS versus NIPS	282

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, proxy server, IP proxy, HTTP proxy (web proxy), 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

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. 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
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 hackers?
- 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?
- A. NIPS**
 - B. Firewall**
 - C. NIDS**
 - D. HIDS**
- 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.
- 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 entire 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, you 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. 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.
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 hackers. 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.
16. **A.** Access control lists can stop particular 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, www.comptia.org). Load balancing is the act of dividing up workload between multiple computers; we'll discuss that more in Chapter 15, "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 we mentioned in Chapter 6, “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 we 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.

Case Studies for Chapter 7

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

Case Study 7-1: Configuring a Firewall's Rule Set

Scenario: You are the security administrator for a company with 200 computers, five of which are servers. Your company wants you to devise a firewall rule set for a specific client computer and allow it specific access to a server.

Details:

Server IP: 10.18.255.101

Client IP: 10.18.255.16

Access needed to server: HTTPS

In Table 7-3, fill out the required information given the previous details.

Table 7-3 Firewall Rule Set

Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

Case Study 7-2: Configuring Packet Filtering and NAT

Scenario: You are consulting for a small company that has seven computers connected to an all-in-one SOHO router (also known as a multifunction network device). The owner is concerned whether data passed through the device is being inspected and/or filtered properly. The owner is also not sure how the internal IP addresses of his computers are being protected from the Internet properly. Your tasks are to make sure packet filtering is functioning, and explain to the owner how NAT works on this device.

Consider your options when it comes to packet filtering for a device such as this. Make a recommendation based on today's SOHO routers. If the owner wanted to take packet filtering further, what could you suggest?

In your own words, explain to the owner (as if you were actually speaking to the person) how NAT functions within a SOHO router.

Case Study 7-3: Configuring an Inbound Filter

Scenario: Your boss is concerned with the repeated intrusion attempts from a group of IP addresses on the Internet. They are all part of a single IP network and range between 12.46.14.66 and 12.46.14.100. The main concern is that they are trying to insert unwanted packets into the network. Your public IP address is 65.13.82.14.

Your job is to block these IP addresses at the firewall. What can you implement that will filter out the unwanted IP addresses? How would this work from a logical standpoint?

Case Study Solutions

Case Study 7-1 Solution

In this scenario you created a basic rule allowing HTTPS access from a client computer to a server. Table 7-4 has the solution for the proper configuration.

Table 7-4 Firewall Rule Set Solution

Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny
10.18.255.16	10.18.255.101	443	TCP	Allow

The client is the source IP and the server is the destination IP as it is the device that runs the service. The port number is 443, the one used by HTTPS. HTTPS, like HTTP, uses TCP as its transport mechanism; it is a guaranteed packet delivery

system, otherwise known as connection-oriented. Finally, the rule is that connections are allowed.

Consider practicing with hardware- and software-based firewalls. If you can't get access to a Cisco, Check Point, or similar device, try working with Windows or Linux in the command-line. For Windows, configure the Windows Firewall with Advanced Security using the Command Prompt and netsh.exe. For more information on how to add rules with netsh.exe, see the following link:

[http://technet.microsoft.com/en-us/library/dd734783\(v=ws.10\).aspx#BKMK_3_add](http://technet.microsoft.com/en-us/library/dd734783(v=ws.10).aspx#BKMK_3_add)

For Linux, use iptables or nftables in the command-line. For more information on iptables, see the following MAN page link:

<http://ipset.netfilter.org/iptables.man.html>

Try to practice working with firewall rules. You are bound to get questions on this topic when you take the exam. Plus, it is a necessary skill for the security administrator.

Simulation: Complete the simulation “7-1: Configuring a Firewall’s Rule Set.”

Case Study 7-2 Solution

First, you should make sure that stateful packet inspection (SPI) is being implemented. SPI keeps track of the individual sessions running through the router. It can differentiate between good and bad packets to a small extent. Small office/home office (SOHO) routers usually have the ability to run SPI, at least at a basic level. However, you should test this ability. How much does it slow down communications?—for example, VPN or remote connectivity connections. If the difference in communication speed between SPI being enabled and being disabled is great, you might recommend a newer SOHO router.

If the owner requires a greater level of packet filtering, you can suggest a NIDS/ NIPS solution that sits inline on the network, and perhaps a proxy server of sorts.

Your explanation of NAT to the owner should include a description of how it translates the private internal IP addresses of the network to the public external IP address. This, you can tell the owner, protects the internal IP addresses from discovery. The public IP address is connected to the Internet, but if firewalled properly, it should be virtually invisible.

Most small four- and eight-port SOHO routers also offer NAT filtering that can filter out TCP and UDP traffic in a variety of ways depending on the IP address and

port in question. This is something you should also examine, and see if the filtering capability can be increased without undue slowdown of the network.

Video Solution: Watch the video solution “7-2: Configuring Packet Filtering and NAT” on the accompanying disc.

Case Study 7-3 Solution

Intrusion attempts to a network are extremely common. A public IP address can expect to be scanned and have intrusion attempts multiple times every day. This is because of the plethora of bots and automatic scanning systems on the Internet.

The first and most obvious defense is to make sure the firewall is on, and test it by scanning it with an online program or with a command-line program such as Nmap. If at all possible, make sure all ports are closed and shielded.

Next, recommend creating an inbound filter for the IP addresses in question. This firewall rule will block all attempts by those IP addresses to access the network. This is often done graphically, but can also be done in the command-line. In essence what you are trying to accomplish can be represented as the following:

```
deny TCP/UDP 12.46.14.66 - 12.46.14.100 65.13.82.14 all ports
```

In this example, you are denying all TCP and UDP port connections for computers with the IP range of 12.46.14.66 to 12.46.14.100. Again, this is just a representation. The actual syntax for how this is implemented will vary from one system to the next. Or it might simply be done within the GUI of the firewall. That will depend on a variety of factors, including the level of complexity of your hardware and software.

Whatever the case is, keep track of your firewall rules. Too many rules and you can end up blocking access to known good IP addresses. Finally, if you are worried that external attackers are trying to insert unwanted packets on your network, you should strongly consider a NIDS or NIPS solution, and possibly a honeypot. These might be implemented as individual technologies or as a part of the overall UTM solution.

Video Solution: Watch the video solution “7-3: Configuring an Inbound Filter” on the accompanying disc.



This chapter covers the following subjects:

- **Securing Wired Networks and Devices:** In this section, you learn about how to reduce the risk of attack to your wired networks and the central connecting devices that control access to those networks. Concepts covered include security for common network devices such as SOHO routers and firewalls, and how to secure twisted-pair, fiber-optic, and coaxial cables.
- **Securing Wireless Networks:** Here, we delve into wireless networks, how you can secure your wireless access points and protect your wireless network from intruders, inside or outside the building. Wireless concepts covered include Wi-Fi security and Bluetooth security.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 1.4, 1.5, 3.4, and 6.2.

Securing Network Media and Devices

Imagine if you will that you are in charge of securing your organization’s wired and wireless networks, and all the devices associated with them. There are several questions you should ask yourself: What kind of cables does your network use, what are the vulnerabilities of those cables, and how can they be secured? What are your future cabling plans? Do you have wireless networks, and if so, how can you protect data that is flinging through the air? How many devices can be accessed either from users on the network or remotely? And are there any older devices that need to be updated, or simply removed?

Verifying that all network devices, cables, and other mediums are secure might sound like a daunting task at first, but let’s take it step by step and discuss how this can be done. We begin with wired networks, cables, and the devices you might find on a wired network; then we move onto wireless transmissions. At the end of the chapter, we show a final piece of network documentation that sums up many of the security precautions we implemented in Chapters 5 through 8.

Foundation Topics

Securing Wired Networks and Devices

Implementing a security plan for your wired network is critical. In Chapter 5, “Network Design Elements,” we talked about the design elements of your network. In Chapter 6, “Networking Protocols and Threats,” we discussed the possible threats to those design elements and to the computers and servers on the network. In Chapter 7, “Network Perimeter Security,” we talked about some of the security tools, such as firewalls, that could be used to protect the network. But what connects it all together? Usually the wired network. Now let’s get into the nitty-gritty of the wired network. Not only are the devices wired to the network targets for attack, but the wires could be targets as well. Some attacks could come from inside the network, whereas other attacks could be external. Let’s start with some of the common vulnerabilities to network devices.

Network Device Vulnerabilities

Devices that reside on your network might include hubs, switches, routers, firewalls, NIDS/NIPS appliances, and more. Each of these devices can be vulnerable in its default state. Most devices are sold with simple default accounts and blank or weak passwords. In some cases, it's easy for users to escalate their privileges to gain access to resources that they normally would not have access to. Some devices and computers can be the victim of backdoors that programmers did not remove, or forgot to remove, which enable access for attackers. And of course, a good network administrator will protect against network attacks such as denial-of-service. Let's go through each of these one by one and show how to protect against these vulnerabilities to help mitigate risk.

Default Accounts

Many of the networking devices available to organizations are initially installed with a default set of user credentials; this is the **default account**. The default account might be called administrator, or admin, or something else similar. If possible, this default account should be changed to a new name, because attackers are aware of default account names. This also applies to computers and servers, as we mentioned in Chapter 3, "OS Hardening and Virtualization." By renaming the default account, or by removing it altogether, you add a layer of security that makes it more difficult for an attacker to figure out which account has administrative access to the device. One example of this is the D-Link SOHO router mentioned in the previous chapter. It is common knowledge that these devices (and many other SOHO routers) are set up by default with the username admin and a blank password. This is one of the first things you should change before you connect it to the Internet. Although some SOHO routers will not enable you to change the username, they certainly enable you to change the password. And a lot of these devices allow a separate user account as well, which might have varying levels of access depending on the device. This should either be set with a complex password or be disabled altogether.

If any guest accounts exist, it is recommended that you disable these accounts. And again, this applies to network devices and computers. The guest account will usually not be enabled, but you should always check this just in case. Of course, more important than the account name or the username is the password. If you have to use a guest account, set a complex password!

Weak Passwords

Passwords should be as complex as possible. A weak password can be cracked by an attacker in a short time. Many network devices come stock with no password at all;

so, your first order of business should be to create a complex password. It is common knowledge that a strong password is important for protecting a user account, whether the account is with a bank, at work, or elsewhere. The same goes for network devices. But what is a strong password? As of 2014, many organizations define a *strong* password as a password with at least eight (even ten) characters, including at least one uppercase letter, one number, and one special character. The *best* passwords have the same requirements but are 15 characters or more. Many password checker programs are available on the Internet; for example, the Password Meter or Microsoft's password checker, available at the following links, respectively:

<http://www.passwordmeter.com/>

<https://www.microsoft.com/security/pc-security/password-checker.aspx>

Let's look at Table 8-1, which gives some examples of weak passwords and strong passwords.

Table 8-1 Weak, Strong, and Stronger Passwords

Key Topic

Password	Strength of Password
Prowse	Weak
DavidProwse	Medium (also known as "good")
locrIan7	Strong
This1sV#ryS3cure	Very strong (also known as "best")

NOTE Be aware that password checking programs can change their criteria over time.

The first password in Table 8-1 is weak; even though it has an uppercase P, it is only 6 characters in length. The second password is only medium strength; it has 11 characters but only 2 uppercase characters, and nothing else is special about it. However, notice the third password is using the pipe symbol instead of the letter L. This is a special character that shares the \ backslash key on the keyboard. Because the third password has a special character, an uppercase I, and a number, and is 8 characters in total, it is considered to be a strong password. In the last password, we have 16 characters, including 3 uppercase letters, 2 numbers, and 1 special character. These methods make for an extremely strong password that would take a supercomputer many years to crack.

Privilege Escalation

When an attacker exploits a bug or other flaw in an operating system or application in order to gain protected access to resources, it is known as **privilege escalation**. The original developer does not intend for the attacker to gain higher levels of access, but probably doesn't enforce a need-to-know policy properly and/or hasn't validated the code of the application appropriately. This technique is used by attackers to gain access to protected areas of operating systems, or to applications; for example, if a particular user can read another user's e-mail without authorization. Other programs, such as Cisco Unified Communications Manager (CallManager), have also been the victim of privilege escalations, although patches are regularly released if issues like these are discovered. Buffer overflows are used on Windows computers to elevate privileges as well. To bypass digital rights management (DRM) on games and music, attackers use a method known as jailbreaking, another type of privilege escalation, most commonly found on mobile devices. Malware also attempts to exploit privilege escalation vulnerabilities, if any exist on the system. Privilege escalation can also be attempted on network devices. Generally, the fix for this is simply to update the device and to check on a regular basis if any updates are available. For example, a typical SOHO router has a user account and an admin account. If a device like this isn't properly updated, an attacker can take advantage of a bug in the firmware to elevate the privileges of the user account. Couple this with the fact that a person forgot to put a password on the user account (or disable it) and your network could be in for some "fun." It is also possible on some devices to encrypt the firmware component. Following are a couple different types of privilege escalation:

Key Topic

- **Vertical privilege escalation:** When a lower privileged user accesses functions reserved for higher privileged users; for example, if a standard user can access functions of an administrator. This is also known as privilege elevation and is the most common description. To protect against this, update the network device firmware. In the case of an operating system, it should again be updated, and usage of some type of access control system is also advisable, for example, User Account Control (UAC).
- **Horizontal privilege escalation:** When a normal user accesses functions or content reserved for other normal users; for example, if one user reads another's e-mail. This can be done through hacking or by a person walking over to other people's computers and simply reading their e-mail! Always have your users lock their computer (or log off) when they are not physically at their desk!

There is also privilege de-escalation, when high privileged but segregated users can downgrade their access level to access normal users' functions. Sneaky admins can attempt this to glean confidential information from an organization. It's a two-way

street when it comes to security; you should think three-dimensionally when securing your network!

Back Doors

A **backdoor** is a way of bypassing normal authentication in a system, securing illegal remote access to a computer, or gaining access to a cryptosystem through circumvention of the normal system of rules.

As mentioned in Chapter 2, “Computer Security Systems,” backdoors were originally used by developers as a legitimate way of accessing an application, but quickly became known to attackers and utilized as an illegitimate means of gaining access to the system. The beauty of the backdoor attack is that the attacker can easily remain undetected. Backdoors can take the form of programs such as RATs, or could be accessed via a rootkit.

Backdoors are less common nowadays, because their practice is usually discouraged by software manufacturers and by makers of network devices. So, as long as the *design* of the application or device was secure (and tested), attackers should not be able to gain access via the backdoor.

Network Attacks

Denial-of-service and many other network attacks can wreak havoc on your network devices. It is important to keep abreast of these latest attacks and to verify that all systems and network devices are updated accordingly. Use smart network intrusion prevention systems (NIPSS) to identify new attacks and prevent them from causing trouble on your networks. For more information on denial-of-service attacks and other types of network attacks, see the section “Malicious Attacks” in Chapter 6.

Other Network Device Considerations

Some network administrators use remote ports on their network devices to remotely administer those devices. These ports can be used maliciously as well. If the remote port is not to be used, it should be disabled. If it is to be used, a strong authentication system should be employed, and data encryption should be considered. This applies to routers, switches, servers, and PBX equipment. For more specific ways to protect your network devices, see the section “Network Design” in Chapter 5.

In some cases a network administrator uses the Telnet program to access network equipment remotely from another site or from within the local area network. This practice should be shunned because Telnet by default is not secure; it does not

encrypt data, including passwords, and default implementations of Telnet have no authentication scheme that ensures that communications will not be intercepted. In addition most Telnet programs have other vulnerabilities and risk associated with them. Instead of using Telnet, administrators should opt for another protocol such as Secure Shell (SSH).

Cable Media Vulnerabilities

The most commonly overlooked item in a network is the cabling. The entire cabling infrastructure (or cabling plant) includes the cables themselves, network jacks, patch panels, punch blocks, and so on. You need to think about what types of cabling you are using, what vulnerabilities they have, and how to combat those vulnerabilities in an attempt to reduce risk. Following are three types of cabling that you might have implemented in your network:

Key Topic

- **Twisted-pair:** A copper-based cable with four pairs of wires (for a total of eight wires), each of which is twisted together along the length of the cable. It is the most common type of network cable; it sends electrical signals to transfer data and uses RJ45 plugs to connect to ports on hosts. The most common security problem with twisted-pair cable is crosstalk, which we discuss later.
- **Fiber-optic:** A glass/plastic-based cable that sends light (photons) instead of electricity. It is composed of one or more thin strands known as fibers that transfer the data. Generally, this is the most secure type of cable that can be used in a network. It is not susceptible to EMI, RFI, or data emanations and is the least susceptible cable to wiretapping. The two main categories of fiber-optic cables are single-mode (for the longest distances) and multi-mode (for shorter distances but longer than twisted-pair). Examples of places where fiber-optic cables are used include high-bandwidth networking technologies such as Fibre Channel (FCoE and FCIP) that use SC and LC connectors.
- **Coaxial:** A less used copper-based cable that has a single copper core. Although not used for connections to hosts anymore, you might see it used with special connections, perhaps for the Internet or for video. In smaller companies' networks, it is common to see an RG-6 cable used for the Internet connection. The most common security risk with coaxial cable is data emanation, which we discuss later.

Each of these cables has its own inherent vulnerabilities; let's talk about a few of these now.

Interference

Interference is anything that disrupts or modifies a signal traveling along a wire. There are many types of interference, but you should know about only a few for the exam, including the following:

- **Electromagnetic interference (EMI):** A disturbance that can affect electrical circuits, devices, and cables due to electromagnetic conduction or radiation. Just about any type of electrical device can cause EMI: TVs, microwaves, air-conditioning units, motors, unshielded electrical lines, and so on. Copper-based cables and network devices should be kept away from these electrical devices if at all possible. If not possible, shielded cables can be used, for example, shielded twisted-pair (STP). Or the device that is emanating EMI can be shielded. For example, an air-conditioning unit could be boxed in with aluminum shielding in an attempt to keep the EMI generated by the AC unit's motor to a minimum. In addition, electrical cables should be BX (encased in metal) and not Romex (not encased in metal); most municipalities require this to meet industrial and office space building code. EMI can also be used in a mischievous manner, known as radio jamming. But the methods listed here can help defend against this as well.
- **Radio frequency interference (RFI):** Interference that can come from AM/FM transmissions and cell towers. It is often considered to be part of the EMI family and is sometimes referred to as EMI. The closer a business is to one of these towers, the greater the chance of interference. The methods mentioned for EMI can be employed to help defend against RFI. In addition, filters can be installed on the network to eliminate the signal frequency broadcast by a radio tower, though this usually does not affect standard-wired Ethernet networks. Wireless signals from wireless networks and cell phones can interfere with speakers and other devices; try to keep speakers and monitors away from cell phones and wireless network adapters. Try to keep wireless access points away from computers, printers, monitors, and speakers; and switches, routers, and other network equipment.

Key Topic

Another common type of interference is crosstalk, discussed next.

Crosstalk

Crosstalk is when a signal transmitted on one copper wire creates an undesired effect on another wire; the signal “bleeds” over, so to speak. This first occurred when telephone lines were placed in close proximity to each other. Because the phone lines were so close, the signal could jump from one line to the next intermittently. If you have ever heard another conversation while talking on your home phone (not cell

phones mind you) you have been the victim of crosstalk. This can happen with connections made by a modem as well, causing considerable havoc on the data transfer.

NOTE With cell phones, crosstalk is also known as co-channel interference, or CCI.

To combat crosstalk, you can use twisted-pair cable. This helps when regular analog signals are sent across the wires and applies only to standard POTS connections and computer modems that use POTS connections. The beauty of the twists in twisted-pair cabling is that the signal has less chance of leaking to other wires, in comparison to straight wires next to each other and bundled together. If the signals are digital—for example, Ethernet data transfers or Voice over IP—you already have an environment less susceptible to crosstalk, in comparison to an analog environment. Data can still bleed over to other wires, but it is less common because the twists of the wires have been precisely calculated by the manufacturer. Sometimes crosstalk occurs due to bunches of cables bundled too tightly, which could also cause crimping or other damage to the cable. If this is the case, a trusty continuity tester will let you know which cable has failed; normally this would have to be replaced. When it comes to twisted-pair cabling, crosstalk is broken down into two categories: near end crosstalk (NEXT) and far end crosstalk (FEXT). NEXT is when measured interference occurs between two pairs in a single cable, measured on the cable end nearest the transmitter. FEXT is when like interference occurs but is measured at the cable end farthest from the transmitter.

If crosstalk is still a problem, even though twisted-pair cable has been employed and digital data transmissions have been implemented, shielded twisted-pair (STP) could be used. Although twisting individual pairs can minimize crosstalk between wire pairs within a cable, shielding an entire cable minimizes crosstalk between cables. Normally, companies opt for regular twisted-pair cabling, which is unshielded (also known as UTP), but sometimes, too much interference exists in the environment to send data effectively, and STP must be utilized.

Data Emanation

Data emanation (or signal emanation) is the electromagnetic (EM) field generated by a network cable or network device, which can be manipulated to eavesdrop on conversations or to steal data. Data emanation is sometimes also referred to as eavesdropping, although this is not accurate.

Data emanation is the most commonly seen security risk when using coaxial cable, depending on the type of coaxial cable, but can also be a security risk for other copper-based cables. There are various ways to tap into these EM fields to get unauthorized access to confidential data. To alleviate the situation, there are several solutions. For example, you could use shielded cabling or run the cabling through metal conduits. You could also use electromagnetic shielding on devices that might be emanating an electromagnetic field. This could be done on a small scale by shielding the single device or on a larger scale by shielding an entire room, perhaps a server room; this would be an example of a **Faraday cage**. If an entire room is shielded, electromagnetic energy cannot pass through the walls in either direction. So, if a person attempts to use a cell phone inside the cage, it will not function properly, because the signal cannot go beyond the cage walls. More important, devices such as cell phones, motors, and wireless access points that create electromagnetic fields and are outside the cage cannot disrupt electromagnetic-sensitive devices that reside inside the cage. Server rooms and cabling should be protected in some way, especially if the data that travels through them is confidential. Studies are constantly done about signal emanations and how to contain them. A group of standards known as **TEMPEST** refers to the investigations of conducted emissions from electrical and mechanical devices, which could be compromising to an organization.

Tapping into Data and Conversations

This is a huge subject, and we could talk about it for days without scratching the surface. One item of note: ANY system can be tapped or hacked. It's just the lengths you must go to that can vary; it depends on the network, cabling, and security precautions already in place.

One older technology is called the *vampire tap*. This deals with coaxial cable, namely 10BASE5 or “thicknet,” which uses a bus topology. The vampire tap works by piercing (biting) into the 10BASE5 cable. The device surrounds the cable and actually taps into the copper core. It was used by administrators to quickly tap into the network, but was also used for more insidious purposes by attackers, but only if they had physical access to the coaxial cable. When attackers had access by using a vampire tap, they could monitor the network in a transparent fashion; meaning, the network admin wouldn’t even know that the monitoring is taking place. Again, this is an older type of technology, and an older way of hacking in to a system, but the term “vampire tap” is still used by some computer pros to refer to a variety of wire tapping scenarios.

“Tapping” today takes on a whole new meaning. **Wiretapping** can mean any one of the following and more:

- **Connecting to a punch block, or RJ11 jack with a butt set:** A **butt set** (or **lineman's handset**) is a device that looks similar to a phone but has alligator clips that can connect to the various terminals used by phone equipment, enabling a person to test a new line or listen in to a conversation. The device is used primarily by telecommunications technicians but can obviously be used for malicious purposes as well. There are analog versions of this device (for POTS systems) and digital versions (for digital systems such as VoIP and so on) that act as packet capturing devices (sniffers). To protect against this, keep all punch blocks and other phone equipment in a locked server room or wiring closet. Although expensive, there are also lockable RJ11 jacks, but it would probably be less costly to install a network of cameras in the building, especially if your organization wants them for other purposes as well.
- **Plugging in to an open port of a twisted-pair network:** This could be either at an RJ45 wall plate or in the server room (not as easy) at an open port of a hub or switch. Unused ports, whether on a hub or switch or at a computer station's RJ45 jack, should be disabled. Also, central connecting devices such as hubs and switches should be locked in the server room, and only properly authenticated individuals should have access.
- **Splitting the wires of a twisted-pair connection:** This can be done anywhere along a cable but would disrupt communications for that individual computer or segment while it is being done. By cutting the twisted-pair cable and soldering a second twisted-pair cable to the appropriate wires (for example, Ethernet 568B networks use the orange and green pairs of wires by default), a person could eavesdrop on all communications on that segment. Cables should not be exposed if at all possible. Cable runs should be above the drop ceiling and inside the walls, perhaps run in conduit. It is understandable that computers need to connect to RJ45 jacks by way of patch cables; if a computer suddenly loses its connection to the network, an alert can be sent to junior administrators, prompting them to investigate why it occurred.
- **Using a spectral analyzer to access data emanations:** Spectral analyzers can measure the composition of electrical waveforms at specific frequencies (for example, 100 MHz on a 100BASE-T twisted-pair network). These can also decode encrypted transmissions. These types of devices should not be allowed in the building (unless used by authorized personnel). A metal detector could be used at the entrance of the building, and again, video cameras can help detect this, and perhaps even prevent mischievous people from attempting to do so, just because they think they might be under surveillance.
- **Using a passive optical splitter for fiber-optic networks:** This is a more expensive device and would need access to a cable. Plus the process of getting it to work is difficult. (And again, this would disrupt communications for a time.)

The preceding listed methods apply to defending against this as well. Because it is difficult to implement an optical splitter properly, this could cause chromatic dispersion on the particular fiber segment. Chromatic dispersion (and subsequent loss of data) could also occur if the fiber-optic cable is too long. Administrators could monitor the network for dispersion and have alerts sent to them in the case that it occurs. The most common example of chromatic dispersion is the rainbow. For example, if light is sent through a prism, the light will be refracted (dispersed) into the rainbow of colors. Although not exactly how it would occur on a fiber-optic cable, if this were to happen, data transmissions would fail.

Some organizations and government agencies require the use of a **protected distribution system (PDS)** for wired connections. These *approved circuits* use all of the techniques mentioned previously in this section to secure the unencrypted transmission of classified information. It is all-encompassing: cables, terminals, and other equipment, including safeguards for electrical, electromagnetic, and acoustical concerns.

Keep in mind that the Security+ exam does not go too far in depth for this subject, but realize that you might get a question on wire tapping, and remember that any network can be hacked! It is more common to attempt hacking into wireless networks. So let's delve into the basics of that immense subject next.

Securing Wireless Networks

Wireless networks pose a whole new set of problems for a network administrator. Wireless access points and wireless network adapters need to be secure from attackers that could be just about anywhere as long as they're within range of the wireless network. Several points we cover can help you secure your wireless access point, wireless network adapters, and any other wireless devices. In this section, you learn how to watch out for wireless transmission vulnerabilities and some of the Bluetooth vulnerabilities that you should be aware of.

Wireless Access Point Vulnerabilities

The wireless access point is the central connecting device for wireless network adapters that might exist in PCs, laptops, handheld computers, mobile devices, and other computers. You need to secure any broadcasts that the wireless access point might make and verify that transmissions are encrypted with a strong encryption technique. It's also important to watch out for rogue access points and round up any nomads on your network.

The Administration Interface

The first thing you should look at when it comes to wireless access points is the administration interface, or console. The act of accessing the administration interface is sometimes referred to as “romming” into the access point. By default, most access points have a blank password or a simple and weak password (for example, “password”). The first step you want to take is to access the administration interface and modify the password; change it to a complex password. Next, consider disabling remote administration if it is not necessary. Your organization might require it, but it depends on several factors. If you are dead set on leaving it enabled, be completely sure that the remote administration password is complex.

SSID Broadcast

The **service set identifier (SSID)** is one of several broadcasts that a wireless access point makes. It identifies the network and is the name of the access point used by clients to connect to the wireless network. It is on by default. After all your clients have been connected to the wireless network, consider disabling the SSID broadcast. Though there will still be ways for hackers to get into your access point, this at least provides a preliminary level of security. The average user cannot see the SSID and cannot connect to the wireless network. In the future if you need to add clients, simply enable the SSID temporarily, connect the client, and then disable the SSID. This might not be a factor if you are in a large building. But if you are in a smaller structure, the wireless access point’s broadcast range may leak out beyond your organization’s property. You can also try reducing the transmitter power of the wireless access point. Although not all access points have this function, some do and it can help to fine-tune the area that the access point serves.

NOTE It wasn’t mentioned yet, but clients can still connect to a wireless network that is not broadcasting the SSID. This can be done manually within the proprietary third-party wireless adapter settings, or by first starting the WLAN Auto-Config service and then accessing the Managing Wireless Networks link within the Network and Sharing Center (Windows Wireless Zero Configuration in older versions of Windows). However, the person connecting must know the SSID, the type of encryption being used, and the encryption key. Some third-party wireless software applications won’t allow for this to be manually entered. If that is the case, and the user needs to connect manually, the third-party software should be disabled and the client should connect using Windows.

Just remember, by default when the SSID broadcast is disabled, no new wireless clients can connect, unless they do so manually.

Rogue Access Points

Rogue access points can be described as unauthorized wireless access points/routers that allow access to secure networks. Sometimes companies lose track of the wireless access points on their network. Keep track of all your devices with network documentation. Use network mapping programs and Microsoft Visio to detect and document any rogue access points. Older access points, especially ones with weak encryption, should be updated, disabled, or simply disconnected from the network. Some companies may have a dozen wireless access points and additional wireless devices such as repeaters, and it may be difficult to keep track of these. In this case, a network mapping program can be one of your best friends. In addition, you can search for rogue access points with a laptop or handheld computer with Windows' wireless application, the wireless network adapter's built-in software, or third-party applications such as AirMagnet or NetStumbler. If traffic from a rogue access point does enter your network, a NIDS or NIPS solution can be instrumental in detecting and preventing that data and data that comes from other rogue devices. Organizations commonly perform site surveys to detect rogue access points, and other unwanted wireless devices. We'll discuss more details about site surveys later in this chapter.

Evil Twin

An **evil twin** is a rogue, counterfeit, and unauthorized wireless access point that uses the same SSID name as a nearby wireless network, often public hotspots. Like an evil twin antagonist found in many sci-fi books, the device is identical in almost all respects to the authorized wireless access point. While the antagonist in the sci-fi book usually has a beard or goatee, the wireless access point is controlled by a person with the same types of motives as the bearded evil twin. One of these motives is phishing. For example, an attacker might attempt to fool wireless users at an Internet café to connect to the counterfeit WAP to gain valuable information and passwords from the users. If the user is unlucky enough to connect to the evil twin, all the information within the session can easily be recorded and digested later on by the attacker. This attack can also be enacted upon organizations. To protect against this, virtual private networks can be implemented that require external authentication outside the wireless access point. Administrators should scan the network often for rogue access points that might be evil twins. Users in general should be trained not to send passwords, credit card numbers, and other sensitive information over wireless networks.

Weak Encryption

Weak encryption or no encryption can be a couple of the worst things that can happen to a wireless network. This can occur for several reasons—for example, if

someone wanted to connect an older device or a device that hasn't been updated, and that device can run only a weaker, older type of encryption. It's important to have strong encryption in your network; as of this writing, WPA2 is the best wireless protocol you can use. It can be used with TKIP or, better yet, AES. Remember that the encryption level of the wireless access point and the encryption level of the network adapters that connect to it need to be the same. Table 8-2 defines some of the available wireless protocols and encryption types.



Table 8-2 Wireless Protocols

Wireless Protocol	Description	Encryption Level (Key Size)
WEP	Wired Equivalent Privacy (Deprecated)	64-bit Also 128-bit but uncommon
WPA	Wi-Fi Protected Access	128-bit
WPA2	Wi-Fi Protected Access Version 2	256-bit
TKIP	Temporal Key Integrity Protocol (Deprecated) Encryption protocol used with WEP and WPA	128-bit
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol Encryption protocol used with WPA2 Addresses the vulnerabilities of TKIP Meets requirements of IEEE 802.11i	128-bit
AES	Advanced Encryption Standard Encryption protocol used with WPA/WPA2 Strongest encryption method in this table	128-bit, 192-bit, and 256-bit

WEP is the weakest type of encryption; WPA is stronger, and WPA2 is the strongest of the three. However, it is better to have WEP as opposed to nothing. If this is the case, use encryption keys that are difficult to guess, and consider changing those keys often. Some devices can be updated to support WPA, whether it is through a firmware upgrade or through the use of a software add-on. Figure 8-1 shows a typical wireless access point with WPA2 and AES configured; AES is the cipher type. The preshared key (PSK) used to enable connectivity between wireless

clients and the access point is a complex passphrase. PSK is automatically used when you select WPA-Personal in the Security Mode section. The other option is WPA-Enterprise, which uses a RADIUS server in this AP. So, if you ever see the term “WPA2-PSK,” that means that the AP is set up to use the WPA2 protocol with a preshared key, and not an external authentication method such as RADIUS.

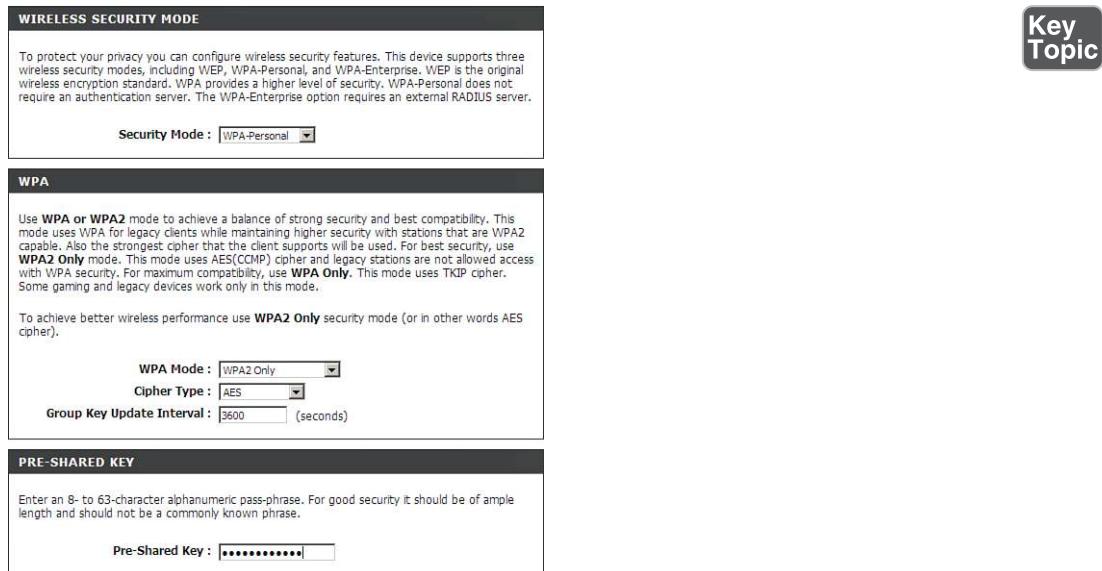


Figure 8-1 Wireless Security Configuration on a Typical Access Point

Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) is in of itself a security vulnerability. Created originally to enable users easy connectivity to a wireless access point, it was later suggested by all major manufacturers that it be disabled (if possible). In a nutshell, the problem with WPS was the eight-digit code. It effectively worked as two separate smaller codes that collectively could be broken by a brute-force attack within hours.

There isn't much that can be done to prevent the problem other than disabling WPS altogether in the access point's firmware interface or, if WPS can't be disabled, upgrading to a newer device. In summary, WPS is a deprecated and insecure technology that should not be allowed on a wireless network.

VPN over Open Wireless

VPN connections are meant to be secure sessions accomplished through an encrypted tunnel. They are best secured in a wired environment, but sometimes a wireless VPN connection is required. Some devices offer this but in an inherently insecure manner—this is known as VPN over *open* wireless, with “open” being the operative word, meaning insecure and unencrypted. In most business scenarios this is unacceptable, and should be scanned for with a wireless scanning utility. Just the presence of a VPN is not enough; some kind of encryption is necessary, whether it be PPTP, IPsec, or another secure protocol.

For example, in a standard Cisco wireless VPN configuration, the wireless client initiates a tunnel to a VPN server (a Cisco router), but it is done in a pass-through manner via a Wireless LAN Controller (WLC). (A Lightweight Access Point is often also part of the solution.) It’s the router that has to be set up properly, and in this scenario IPsec should be installed and configured. That will allow for the encryption of session data between the wireless client and the WLC.

In other scenarios, especially in smaller offices or home offices, a single device will act as the all-in-one solution. Though wireless VPN connections are uncommon in SOHO environments, this solution presents only a single layer of defense and it can be easy to forget to initiate the proper encryption. There are many authentication mechanisms and possibilities, and several ways to encrypt the session. The key here is to remember to have clients authenticate in a secure manner, and handshake on an encryption protocol that will protect the data. We discuss authentication and concepts such as VPN in more depth in Chapter 9, “Physical Security and Authentication Models.”

Wireless Access Point Security Strategies

Strategic placement of a WAP is vital. Usually, the best place for a WAP is in the center of the building. This way, equal access can be given to everyone on the perimeter of the organization’s property, and there is the least chance of the signal bleeding over to other organizations. If needed, attempt to reduce the transmission power levels of the antenna, which can reduce the broadcast range of the WAP. Also, to avoid interference in the form of EMI or RFI, keep wireless access points away from any electrical panels, cables, devices, motors, or other pieces of equipment that might give off an electromagnetic field. If necessary, shield the device creating the EM field, or shield the access point itself. Sheesh, I am starting to sound bossy! (Must be those two years I spent as a building contractor...)

Anyway, in order to really know how to best arrange and secure your wireless connections, you need to understand the different wireless systems and antenna types

available. The most common wireless system is point-to-multipoint. This system is commonly used in WLANs where a single central device (such as a SOHO wireless router) will connect to multiple other wireless devices that could be located in any direction. Specifically, it makes use of omnidirectional antennas such as vertical omnis, ceiling domes, and so on. A typical wireless router might have two, three, four, or more vertical omnidirectional antennas. For example, a SOHO 802.11n wireless router might have three antennas that use multiple-input multiple-output (MIMO) technology to combine multiple data streams for significantly higher data throughput (up to eight streams for 802.11ac). These antennas can be rotated so that they are parallel to each other, or at an angle to each other; for example, 180 degrees is often a good configuration to in essence “sweep” the area for wireless transmissions. However, you might choose a different method. For example, you might have 100 computers on one floor and two WAPs to work with. The best method might be to position them at vertical angles from each other. One would be in the building’s northeast corner and the other in the southwest corner. Then, each set of three antennas could be positioned in a 90-degree sweep as shown in Figure 8-2. As long as the building isn’t larger than the range of the antennas (which for 802.11n is approximately 70 meters/230 feet indoors), then this should allow for excellent wireless coverage.

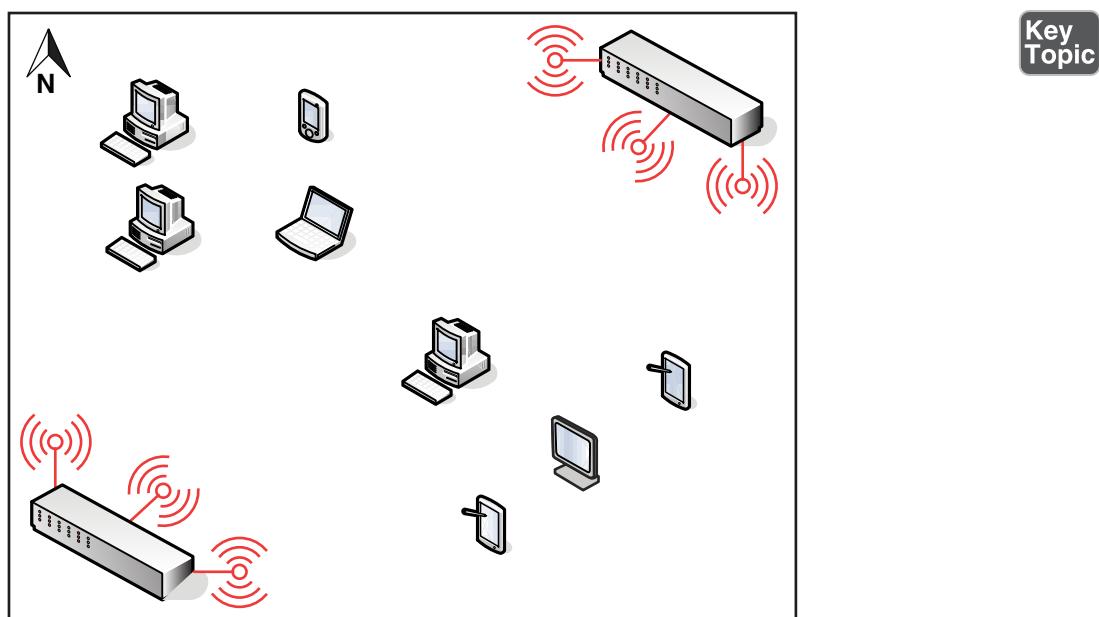


Figure 8-2 Wireless Point-to-Multipoint Layout

There are also more simplistic point-to-point wireless systems where only two points need to be connected; these points are usually fixed in location. In this case you would use directional antennas; for example, a parabolic antenna (dish) or a Yagi antenna.

Whatever you implement, it's a good idea to perform a wireless site survey. There are three kinds of wireless surveys you might perform, each with its own purpose, and all of which are usually based on software that collects WLAN data and signal information (though hardware can also be used to measure radio frequencies). A passive site survey listens to WLAN traffic and measures signal strength. An active survey actually sends and receives data to measure data transfer rate, packet loss, and so on. A predictive survey is a simulated survey based on real data such as the WAP to be used, the distance between the average computer and WAP, and so on.

Surveys can be instrumental in uncovering nonaggressive interference such as neighboring radiowaves and electrical equipment (RFI and EMI, mentioned earlier). Surveys can also be used to locate aggressive *jamming* techniques often caused by wireless signal jammers. A signal jammer can easily be purchased online and can be used to initiate a denial-of-service attack to the wireless network. This is done by creating random noise on the channel used by the WAP, or by attempting to short out the device with powerful radio signals. The right wireless software (such as NetStumbler) can be used to locate signal jammers in or around your building so that you can remove them. Wireless software can also be used to identify potential wireless replay attacks that might exist within the network infrastructure.

Many WAPs come with a built-in firewall. If the firewall is utilized, the stateful packet inspection (SPI) option and NAT filtering should be enabled. The wireless access point might also have the capability to be configured for **MAC filtering** (a basic form of network access control), which can filter out which computers can access the wireless network. The WAP does this by consulting a list of MAC addresses that have been previously entered. Only the network adapters with those corresponding MAC addresses can connect; everyone else cannot join the wireless network. In some cases, a device might broadcast this MAC table. If this is the case, look for an update for the firmware of the access point, and again, attempt to fine-tune the broadcast range of the device so that it does not leak out to other organizations. Because MAC filtering and a disabled SSID can be easily circumvented using a network sniffer, it is very important to also use strong encryption, and possibly consider other types of network access control (such as 802.1X) and external authentication methods (such as RADIUS).

Some access points also support isolation. **AP isolation** (also known as isolation mode) means that each client connected to the AP will not be able to communicate with any other clients connected to the AP. Each client can still access the Internet (or other network that the AP is connected to), but every wireless user will be segmented from the other wireless users.

It is also possible to include the IEEE 802.1X standard for port-based network access control that can provide for strong authentication. For a wireless access point to incorporate this kind of technology, it must also act as a router, which adds the duty of wireless gateway to the access point.

Another option is to consider encryption technologies on the application layer, such as SSL, SSH, or PGP; these and others can help to secure data transmissions from attackers that have already gained access to the wireless network. For more information on encryption types, see the section “Security Protocols” in Chapter 14, “PKI and Encryption Protocols.” When it comes down to it, authentication and a strong wireless protocol such as WPA2 with AES are the two security precautions that will best help to protect against network attacks.

Finally, another option is to not run wireless at all. It’s tough to hack into a wireless network that doesn’t exist! Some companies opt for this, as strange and difficult as it may seem, because they have deduced that the costs of implementation, administration, maintenance, and security outweigh the benefits of having a wireless network. (Personally, my home is cabled up 100 percent—bedrooms, bathrooms, attic, you name it...but I still use wireless devices!) However, if you decide to go down the anti-wireless road, make sure that any devices that enable wireless access have those wireless functions disabled. This includes wireless access points, laptops, and other mobile devices that have wireless adapters, and any Bluetooth, infrared, or other wireless transmitters.

Wireless Transmission Vulnerabilities

Because wireless networks can transmit information through air or space, data emanations are everywhere and can easily be identified by people using the right tools. One deed that can be considered an attack on wireless networks is known as **war-driving**; this is the act of searching for wireless networks by a person in a vehicle, through the use of a device with a wireless antenna, often a particularly strong antenna. A basic example of this would be a person in a car with a laptop, utilizing the freely downloadable NetStumbler software. When war-drivers find a network, they can attempt to crack the password or passphrase to gain access to the wireless network. This might be done by guessing; you’d be surprised how much this works. It is estimated that more than 40 percent of wireless networks are unprotected. It could also be done with dictionary or brute-force attacks. You can find more information on password cracking in the section “Assessing Vulnerability with Security Tools” in Chapter 11, “Vulnerability and Risk Assessment.”

Ways to protect against war-driving include hiding the SSID of the wireless access point, proper positioning of the WAP, decreasing the power levels to the point where the signal doesn’t leak past the organization’s building, using strong encryption, and changing the passphrase (encryption key) at regular intervals.

An interesting item connected with public Wi-Fi is **war-chalking**. This is the act of physically drawing symbols in public places that denote open, closed, or protected wireless networks. This is done by attackers to let other attackers know about open wireless networks. However, some organizations use the symbols as well to let people know that they have an open wireless network available to the public. In this case, the symbols will be professionally presented. Various symbols are used including the open node (two half circles back to back), the closed node (a closed circle), and a circle with a W, which stands for a WEP- or WPA-encrypted network.

IV attacks are another vulnerability of wireless networks. The **IV attack** is a type of related-key attack, which is when an attacker observes the operation of a cipher using several different keys, and finds a mathematical relationship between those keys, allowing the attacker to ultimately decipher data. IV stands for initialization vector, a random fixed-sized input that occurs in the beginning of every WEP or WPA packet. For WEP, the IV size was small (24-bit) and led to many successful attacks on WEP. This is why WEP is considered to be deprecated and insecure. The best way to prevent IV attacks is to use stronger wireless protocols such as WPA2 and AES.

We've mentioned DoS attacks several times in this book already. These can be run against WAPs in a variety of ways. One way is through the use of spoofed MAC addresses. If an attacker emulates a large number of wireless clients, each with a different spoofed MAC address, and never allows authentication for these clients to finish, then legitimate clients will no longer be able to be serviced by the WAP, because all of the session spots will have been taken. This is a type of denial-of-service due to incomplete authentication. It can be prevented by configuring expiration timeouts for all sessions that have not had activity for a certain period of time. It can also be prevented by updating the WAP and implementing wireless frame protection. (Different providers will have different names for this; for example, Cisco Management Frame Protection.)

We previously pointed out that a WAP can fall victim to brute-force attacks if WPS is used. The key of the WAP can also be compromised by a brute-force attack known as an exhaustive key search. This can be prevented by limiting the number of times a password/passphrase can be tried, using time delays between attempts, and requiring complex answers during the authentication process. Also, as a corrective security control, attacking IP addresses can be blacklisted. We'll discuss brute-force/exhaustive key searches more in Chapter 13, "Encryption and Hashing Concepts."

Bluetooth Vulnerabilities

Bluetooth, like any wireless technology, is vulnerable to attack as well. Bluejacking and bluesnarfing are two types of vulnerabilities to Bluetooth-enabled devices. Bluetooth is also vulnerable to conflicts with other wireless technologies. For example,

some WLAN (or Wi-Fi) standards use the 2.4-GHz frequency range, as does Bluetooth, and even though Bluetooth uses frequency hopping, conflicts can occur between 802.11g or 802.11b networks and Bluetooth personal area networks. To avoid this, use Bluetooth version 1.2 devices or greater, which employ adaptive frequency hopping, improving resistance to radio interference. Also, consider placing Bluetooth access points (if they are used) and WLAN access points in different areas of the building. Some companies have policies governing Bluetooth usage; in some cases, it is not allowed if 802.11 standards are in place, and in some cases a company will enforce rules that say Bluetooth can be used only outside the building. In other cases, a company will put its 802.11 devices on specific channels or use WLAN standards that use the 5-GHz range.

Bluetooth equipped devices can use *near field communication* (NFC), which allows two mobile devices (or a mobile device and a stationary computer) to be automatically paired and transmit data. NFC is not limited to Bluetooth, but Bluetooth is probably the most common technology used to transmit data wirelessly over short distances. Of course, even though the distance is short, it can still be eavesdropped on. In addition, NFC is a data transmission protocol, but not necessarily secure. Data can be destroyed by use of a jammer, and users are also at risk of replay attacks. At the writing of this book, NFC does not offer preventive security in this aspect, but a user can prevent these attacks by only using applications that offer SSL/TLS or other secure channels during an NFC session.

Bluejacking

Bluejacking is the sending of unsolicited messages to Bluetooth-enabled devices such as mobile phones and tablets. Bluejacking is usually harmless, but if it does occur, it may appear that the Bluetooth device is malfunctioning. Originally, bluejackers would send only text messages, but with newer Bluetooth-enabled mobile devices, it is possible to send images and sounds as well. Bluejacking is used in less-than-reputable marketing campaigns. Bluejacking can be stopped by setting the affected Bluetooth device to “undiscoverable” or by turning off Bluetooth altogether.

Bluesnarfing

I know what you are thinking: The names of these attacks are starting to get a bit ridiculous! I guarantee it will improve as we progress through the rest of this book! Anyway, **bluesnarfing** is the unauthorized access of information from a wireless device through a Bluetooth connection. Generally, bluesnarfing is the theft of data (calendar information, phonebook contacts, and so on). It is possible to steal other information as well, but to pilfer any of this data, a pairing must be made between the attacking Bluetooth device and the Bluetooth victim. Ways of discouraging

bluesnarfing include using a pairing key that is not easy to guess; for example, stay away from 0000 or similar default Bluetooth pairing keys! Otherwise, Bluetooth devices should be set to “undiscoverable” (only after legitimate Bluetooth devices have been set up, of course), or Bluetooth can be turned off altogether, especially in areas that might be bluesnarfing playgrounds, such as Times Square in New York City. Bluesnarfing is considered by some to be a component of bluejacking, but for the exam, try to differentiate between the two.

More details about how to protect phones, laptops, and other devices that use Bluetooth can be found in Chapter 2.

Final Network Documentation

As promised in the beginning of this chapter, Figure 8-3 sums up a lot of the devices and security implementations that we discussed in Chapters 5 through 8. Note the different network elements, devices, cabling, and wireless connectivity included in the illustration. Also note that the firewall has four connections, one each to the LAN, DMZ, extranet, and Internet. Also worth noting is that the 802.11n WAP and the Bluetooth access point are located in different areas of the network. Try to define each network element that you see, and remember the various ways to secure them. Then create your own set of documentation for your own dream network (with security implementations, of course) that includes all the elements discussed in Chapters 5–8.

Key Topic

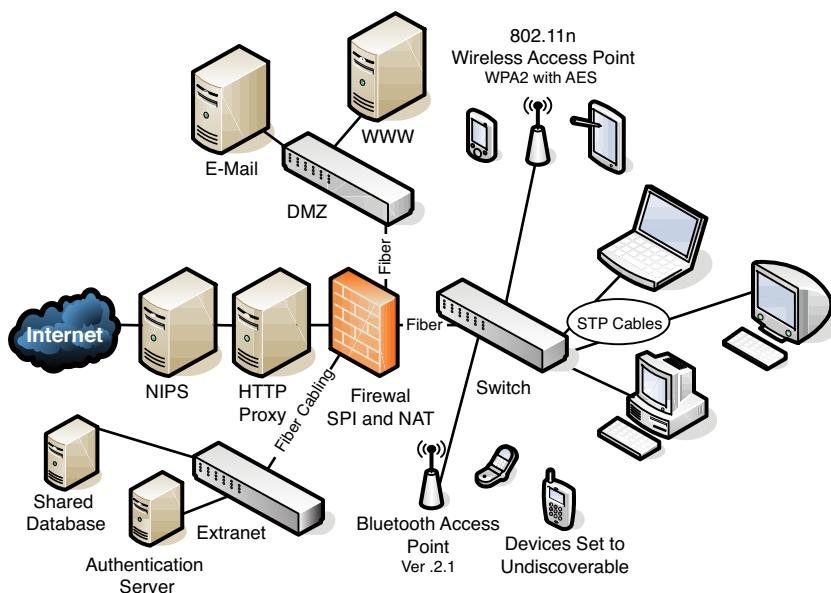


Figure 8-3 Final Network Documentation

Chapter Summary

If we all operated computers that never made any connections to other systems, we could say that those computers were pretty secure. What a wonderful world it would be, and for many end users, that was the world...in 1986. Today's computers usually *require* networking connections; otherwise they become useless. These past four chapters have shown that the majority of security concerns are network related...not all, but a huge chunk. Now here's a newsflash that even some technicians don't think of—disable the wired or wireless networking connection when the computer is not in use. Yes! In some cases this method is feasible today. For example, configure a mobile device to go to airplane mode while you are sleeping. A good rule of thumb for end users is that, unless they have a server, their computers should sleep when they sleep. As another example, configure an unused server to effectively shut down its network interface automatically between the hours of 2 a.m. and 7 a.m. (if there is little activity then). This kind of mentality can add up over time, and equate to a cleaner and more efficiently running network.

However, that is somewhat of a utopian mindset when it comes to the hardcore company that needs to do business 24/7. Therefore, we have to employ the measures discussed in this chapter. In this chapter we focused on the wired and wireless connections of networks. Devices that control these wired and wireless networks often have weak security when it comes to account names and especially passwords. If you can change the administrator account name (or create a secondary admin account and disable the first) and set a complex password, you will have implemented the most important layer of security. And by complex, I mean COMPLEX! (That was me practically yelling the word.)

Today's complexity is multifaceted compared to last decade's complexity. There are various reasons for this—which we will discuss more in later chapters—but in essence, having a 10-character password for normal environments and a 15-character password for highly confidential environments is now the status quo (as of the writing of this book). Add on numerals, uppercase letters, and special characters, and you have the beginnings of an uncrackable password. But remember, password cracking programs (and the computers that run them) are always getting stronger and faster. For example, an eight-character password that was considered uncrackable in 1999 might only take a week to crack today. This progression is directly related to Moore's Law, and as such will most likely continue. "But wait, Dave!" you say, "Does this mean that, at some point, all passwords can be cracked?" Theoretically, yes, but that time probably won't come soon. But it is better to be safe than sorry, and so you might also want to incorporate multifactor authentication, of which we will speak in the following chapter.

Devices should have their firmware updated often to help close backdoors and weed out privilege escalation attempts. These updates will often have patches for the various network attacks that we have mentioned in the past few chapters.

Wired connections are still the lifeblood of a company. Wireless is great, but you don't run it in a server room or data center; and for stationary workstations, wired connections are king. The bulk of these connections are twisted-pair, which is inherently vulnerable to tapping. Use shielded cables to block EMI, resist wire tapping, and reduce data emanation and crosstalk. On a larger scale, consider shielding such as a Faraday cage or TEMPEST, especially in server rooms. Disable unused ports on switches and RJ45 wall terminals, remove any network cabling that is not hidden from view, and, if you are really security conscious, consider using fiber-optic cabling. Your servers may already utilize this, but your clients probably do not. For computers that send the most confidential of information, a secure channel is great, but secure media (such as fiber-optic cabling) seals the deal.

Of course, when you have data that flies all over the air in your building, it can be more difficult to secure. It is more abstract, and not as easily measured. But it is still possible to secure a wireless network. It's really all about scanning the wireless network. Is your SSID easy to find? Is it possible that you could hide the SSID? Are there other SSIDs that show up on your scan? Rogue access points and evil twins need to be sniffed out and eliminated immediately. But that isn't as much a preventative security control as it is a detective security control. The real way to prevent issues on the wireless network is to employ encryption—strong encryption such as WPA2 and AES (with a powerful preshared key), or perhaps utilize a RADIUS server in combination with those. Get rid of WPS once and for all, and make sure that VPN connections made wirelessly are heavily encrypted. Then it's just a matter of doing a site survey, and maximizing your data transfer rate in a secure way by using smart placement techniques of your WAPs and antennas. These methods will help to reduce the chance of a successful war-driving attack, or IV attack, or a brute-force attempt.

And wireless is not limited to WLAN. You might have Bluetooth, IR, GSM, 4G, and the list goes on. All wireless transmissions should be thoroughly scanned and tested before they are allowed in your organization. But that's another book (and certification) altogether. Where the Security+ certification expects a basic level of wireless security knowledge, other certifications such as the Certified Wireless Network Administrator (CWNA) take it to the next level and require in-depth knowledge of all wireless communications security techniques, especially WLAN. If your organization is highly dependent on its wireless communications, consider a wireless certification such as the CWNA to bolster your resume.

Every chapter in this book effectively deals with network security on some level. But these past four chapters are at the core of it. Remember the content in these

chapters as you progress throughout the rest of the book—they build your foundation of networking and network security knowledge. Finally, when it comes to your network security, attempt to think outside the box. If necessary, take it to the next level and work out solutions that, even if they seem unorthodox, fit into your organization’s business model. You might surprise yourself and come up with some great answers that work very well for you and your organization.

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 8-3 lists a reference of these key topics and the page number on which each is found.

Table 8-3 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
Table 8-1	Weak, strong, and stronger passwords	301
Bullet list	Privilege escalation types	302
Bullet list	Cable types	304
Bullet list	Interference types	305
Table 8-2	Wireless protocols	312
Figure 8-1	Wireless security configuration on a typical WAP	313
Figure 8-2	Wireless point-to-multipoint layout	315
Figure 8-3	Final network documentation	320

Define Key Terms

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

default account, privilege escalation, backdoors, electromagnetic interference (EMI), radio frequency interference (RFI), crosstalk, data emanation, Faraday cage, butt set, TEMPEST, wiretapping, protected distribution system (PDS),

service set identifier (SSID), evil twin, Wi-Fi Protected Setup (WPS), Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP), MAC filtering, AP isolation, war-driving, war-chalking, IV attack, bluejacking, bluesnarfing

Review Questions

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

1. Which of the following is the most secure protocol to use when accessing a wireless network?
 - A. WEP
 - B. WPA
 - C. WPA2
 - D. TKIP

2. What type of cabling is the most secure for networks?
 - A. STP
 - B. UTP
 - C. Fiber-optic
 - D. Coaxial

3. What should you configure to improve wireless security?
 - A. Enable the SSID
 - B. IP spoofing
 - C. Remove repeaters
 - D. MAC filtering

4. In a wireless network, why is an SSID used?
 - A. To secure the wireless access point
 - B. To identify the network
 - C. To encrypt data
 - D. To enforce MAC filtering

5. What is the most commonly seen security risk of using coaxial cable?
 - A. Data that emanates from the core of the cable
 - B. Crosstalk between the different wires
 - C. Chromatic dispersion
 - D. Time domain reflection
6. Of the following, what is the most common problem associated with UTP cable?
 - A. Crosstalk
 - B. Data emanation
 - C. Chromatic dispersion
 - D. Vampire tapping
7. What two security precautions can best help to protect against wireless network attacks?
 - A. Authentication and WEP
 - B. Access control lists and WEP
 - C. Identification and WPA2
 - D. Authentication and WPA
8. Which of the following cables suffers from chromatic dispersion if the cable is too long?
 - A. Twisted-pair cable
 - B. Fiber-optic cable
 - C. Coaxial cable
 - D. USB cables
9. Which of the following cable media is the least susceptible to a tap?
 - A. Coaxial cable
 - B. Twisted-pair cable
 - C. Fiber-optic cable
 - D. CATV cable

- 10.** Which of the following, when removed, can increase the security of a wireless access point?
 - A.** MAC filtering
 - B.** SSID
 - C.** WPA
 - D.** Firewall

- 11.** A wireless network switch has connectivity issues but only when the air-conditioning system is running. What can be added to fix the problem?
 - A.** Shielding
 - B.** A wireless network
 - C.** A key deflector
 - D.** Redundant air-conditioning systems

- 12.** Which of the following is the most secure type of cabling?
 - A.** Unshielded twisted-pair
 - B.** Shielded twisted-pair
 - C.** Coaxial
 - D.** Category 5

- 13.** Which of the following is the least secure type of wireless encryption?
 - A.** WEP 64-bit
 - B.** WEP 128-bit
 - C.** WPA with TKIP
 - D.** WPA2 with AES

- 14.** Which of the following is the unauthorized access of information from a Bluetooth device?
 - A.** Bluejacking
 - B.** Bluesnarfing
 - C.** Deep Blue
 - D.** The Blues Brothers

- 15.** Which of the following can be described as the act of exploiting a bug or flaw in software to gain access to resources that normally would be protected?
- A.** Privilege escalation
 - B.** Chain of custody
 - C.** Default account
 - D.** Backdoor
- 16.** What does isolation mode on an AP provide?
- A.** Hides the SSID
 - B.** Segments each wireless user from every other wireless user
 - C.** Stops users from communicating with the AP
 - D.** Stops users from connecting to the Internet
- 17.** You scan your network and find a rogue access point with the same SSID used by your network. What type of attack is occurring?
- A.** War-driving
 - B.** Bluesnarfing
 - C.** Evil twin
 - D.** IV attack
- 18.** Which of the following is an unauthorized wireless router that allows access to a secure network?
- A.** Rogue access point
 - B.** Evil twin
 - C.** War-driving
 - D.** AP isolation
- 19.** Your boss asks you to limit the wireless signal of a WAP from going outside the building. What should you do?
- A.** Put the antenna on the exterior of the building.
 - B.** Disable the SSID.
 - C.** Enable MAC filtering.
 - D.** Decrease the power levels of the WAP.

20. Which of the following should be considered to mitigate data theft when using Cat 6 wiring?
- A. Multimode fiber
 - B. EMI shielding
 - C. CCTV
 - D. Passive scanning

Answers and Explanations

1. C. Wi-Fi Protected Access 2 (WPA2) is the most secure protocol listed for connecting to wireless networks. It is more secure than WPA and WEP. **Wired Equivalent Privacy (WEP)** is actually a deprecated protocol that should be avoided. The WEP algorithm is considered deficient for encrypted wireless networks. TKIP is also deprecated and is replaceable with CCMP.
2. C. Fiber-optic is the most secure because it cannot be tapped like the other three copper-based cables; it does not emit EMI. Although shielded twisted-pair (STP) offers a level of security due to its shielding, it does not offer a level of security like that of fiber-optic and is not the best answer.
3. D. MAC filtering disallows connections from any wireless clients unless the wireless client's MAC address is on the MAC filtering list.
4. B. The SSID is used to identify the wireless network. It does not secure the wireless access point; one of the ways to secure a wireless access point is by disabling the SSID. The SSID does not encrypt data or enforce MAC filtering.
5. A. Some types of coaxial cables suffer from the emanation of data from the core of the cable, which can be accessed. Crosstalk occurs on twisted-pair cable. Chromatic dispersion occurs on fiber-optic cable. Time domain reflection is a concept that is used by a TDR.
6. A. Of the listed answers, crosstalk is the most common problem associated with UTP cable. Older versions of UTP cable (for example, Category 3 or 5) are more susceptible to crosstalk than newer versions such as Cat 5e or Cat 6. Although data emanation can be a problem with UTP cable, it is more common with coaxial cable, as is vampire tapping. Chromatic dispersion is a problem with fiber-optic cable.
7. D. The best two security precautions are authentication and WPA. Although WPA2 is more secure than WPA, the term "Identification" is not correct. WEP is a deprecated wireless encryption protocol and should be avoided.

8. **B.** Fiber-optic cable is the only one listed that might suffer from chromatic dispersion, because it is the only cable based on light. All the other answers are based on electricity.
9. **C.** Fiber-optic cable is the least susceptible to a tap because it operates on the principle of light as opposed to electricity. All the other answers suffer from data emanation because they are all copper-based.
10. **B.** By removing the SSID (security set identifier), the wireless access point will be more secure, and it will be tougher for war-drivers to access that network. Of course, no new clients can connect to the wireless access point (unless they do so manually). MAC filtering, WPA, and firewalls are all components that increase the security of a wireless access point.
11. **A.** By shielding the network switch, we hope to deflect any interference from the air-conditioning system. Another option would be to move the network switch to another location.
12. **B.** Shielded twisted-pair is the most secure type of cabling listed. It adds an aluminum sheath around the wires that can help mitigate data emanation. By far, fiber-optic would be the most secure type of cabling because it does not suffer from data emanation because the medium is glass instead of copper.
13. **A.** WEP 64-bit is the least secure type of wireless encryption listed in the possible answers. The answers are listed in order from least secure to most secure.
14. **B.** Bluesnarfing is the unauthorized access of information from a Bluetooth device—for example, calendar information, phonebook contacts, and so on. Bluejacking is the sending of unsolicited messages to Bluetooth-enabled devices. Deep Blue is not a valid answer to this question as it was a chess-playing computer developed by IBM. And if you answered the Blues Brothers, you should re-read this entire chapter, and then watch the movie if you have some free time.
15. **A.** Privilege escalation is the act of exploiting a bug or flaw in software to gain access to resources that normally would be protected. Chain of custody is the chronological paper trail used as evidence. A default account is an account such as admin set up by the manufacturer on a device; it usually has a blank or simple password. A backdoor is used in computer programs to bypass normal authentication and other security mechanisms that might be in place.
16. **B.** AP isolation mode segments every wireless user so they can't communicate with each other. They can still communicate with the AP and access the Internet (or other network that the AP connects to). It does not hide the SSID.
17. **C.** An evil twin is a rogue access point that has the same SSID as another access point on the network. War-driving is when a person attempts to access a

wireless network, usually while driving in a vehicle. Bluesnarfing is the unauthorized access of information through a Bluetooth connection. An IV attack is one that attempts to break the encryption of wireless protocols.

18. **A.** A rogue access point is an unauthorized wireless router (or WAP) that allows access to a secure network. An evil twin is a type of rogue AP, but it also uses the same SSID as the legitimate network. War-driving is the act of trying to access a wireless network. AP isolation blocks each wireless user from communicating with each other.
19. **D.** To limit the wireless signal, decrease the power levels! This can easily be done in most WAP control panels. Putting the antenna on the exterior of the building would make it easier for war-drivers to access the network, and more difficult for actual users. Disabling the SSID has no effect on the signal level. Nor does MAC filtering, though both of those methods can increase the security of your wireless network.
20. **B.** You should implement EMI shielding. This will help to eliminate EMI and data emanation from the Cat 6 wiring (which by default is UTP and therefore not shielded). Multimode fiber would solve the problem, but only if you tore out all of the twisted-pair cabling and replaced it. Questions of this nature don't expect you to take those kinds of measures or accept those types of expenses. Instead, you should focus on securing the cabling that is already in place. CCTV is a detective control that allows you to monitor what transpires in your building via video. Passive scanning is a technique used to check the vulnerabilities of a computer.

Case Studies for Chapter 8

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

Case Study 8-1: Securing a Wireless Device

Scenario: You have a new client, a small marketing office with six computers and a SOHO router/WAP. The client wants you to secure the device so that the internal computers will be safe and so that the wireless network will be difficult to attack.

Define eight ways that you can protect this wireless network.

Case Study 8-2: Enabling MAC Filtering

Scenario: As part of the previous scenario, you decide to enable MAC filtering on the client's WAP. Your task is to allow access only to specific MAC addresses for three Windows computers, a Linux computer, and a Mac computer. Explain how you would find out the MAC addresses for those computers, and give an example of a MAC address. Then, describe how MAC filtering can be enabled given this setting.

Case Study 8-3: War-driving...and the Cure

Scenario: Your boss has heard of these “war-drivers” and has obvious concerns of unauthorized access to your wireless network. He wants to have proof that it will be difficult for a war-driver to access the network, and that there are no jamming devices or other interference-based devices within the perimeter of the building.

Your job is to scan the building, make any configurations necessary, and explain how you have configured the wireless network to be war-driver-proof.

Case Study 8-4: Planning Network Security

Scenario: You have been given a new assignment at your organization's newly built sister office. You have been tasked with installing several security technologies to protect the LAN and WLAN.

Take a look at Table 8-4, which includes a list of problems that you need to tackle. In the Your Solution column, enter the device, technology, or other solution that you would employ for each situation. Be concise and brief in your answers. This Case Study spans the content within Chapters 5 through 8.

Table 8-4 LAN and WLAN Security Issues

Issue	Your Solution
E-mail and web servers need to be separated from the LAN.	
The WAP is not running any encryption.	
Your boss wants additional authentication for the wireless network above and beyond the WAP's inherent ability.	
You have discovered that several computers' wired connections suffer from EMI. They have confidential information and are potential victims for wiretapping.	
The firewall is not configured for the proper type of packet filtering.	
Users on the network need to be protected from malicious content on websites.	
You are concerned about anomalous packets and want them to be removed from the network if they are found.	
There is a long distance wired connection between the firewall and the extranet.	
There are areas of the building that are not particularly secure and could be accessed by malicious insiders who could possibly attempt wiretapping.	

Case Study Solutions

Case Study 8-1 Solution

There are a host of things you can do to secure a wireless network. The following eight-step list should be incorporated into most plans to secure a WAP, but you will undoubtedly add your own zest to the mix!

- Step 1.** Update firmware. Download the latest firmware, install it, and test it before implementation. Any hotfixes and updates (if the device accepts those) should be installed as well. Check for updates automatically, and have the device's manufacturer e-mail you if new updates are released.
- Step 2.** Set passwords! Enter separate, complex passwords for the administrator and the user accounts.
- Step 3.** Disable remote administration. If it is not necessary, remove this functionality by disabling it. Or, if it is necessary, consider changing the port from the commonly used 8080 to something less well-known.
- Step 4.** Disable SSID broadcasting. Once all computers have been connected, make the wireless network invisible by disabling the SSID. Computers can still connect, in a manual, step-by-step fashion, but at least it will be more difficult to scan for the SSID.

NOTE Before anyone ever connects to the WAP, change the SSID from the default name to something less common.

- Step 5.** Enable encryption. As of the writing of this book, WPA2 and AES are the best options. (But anything is better than nothing.) Select a complex preshared key. If possible, use a RADIUS server for authentication.
- Step 6.** Reduce the output transmitting power of the WAP. Sometimes, the wireless network is too powerful and reaches far beyond the physical perimeter of the office. Antennas are set to a specific output power by default (for example, 90 mW). This can be reduced on some WAPs, which will ultimately reduce the range of the wireless network.
- Step 7.** Enable MAC filtering. This configuration allows you to allow or deny specific MAC addresses.

Step 8. Configure other rules and ACLs. This might include inbound filters, access control policies, application rules, and so on. Depending on your organization’s function, you might decide to implement other options such as captive portals and secure VPN.

In Steps 7 and 8, be sure that you don’t lock down your WAP too tightly, or you might end up restricting access to clients that legitimately need to access your wireless network.

Video Solution: Watch the video solution: “8-1: Securing a Wireless Device” on the accompanying disc.

Case Study 8-2 Solution

MAC addresses are groups of six hexadecimal numbers, separated by hyphens or by colons.

Example: 00-1C-C0-A1-54-1B

Find out the MAC address of a Windows computer by accessing the Command Prompt and typing `ipconfig /all`.

Find out the MAC address of a Linux or Mac computer by opening the Terminal and typing `ifconfig`.

Write down all MAC addresses that are to be given access to the WAP. Then, access the WAP’s firmware, usually from your web browser.

NOTE Consider a secure web browser such as Firefox when doing this type of work. Regardless, make sure the browser is updated, and verify that no one is attempting to shoulder surf your computer while you access the WAP!

Access the MAC filter configuration area (sometimes also called *network filter*). Select the Allow Only These Computers option, or similar name. Add each individual MAC address and save the settings. Then test the system to make sure the computers in question can access the wireless network.

Video Solution: Watch the video solution: “8-2: Enabling MAC Filtering” on the accompanying disc.

Case Study 8-3 Solution

The first step is to scan the area to find out what wireless networks are visible. This can be done in several ways. For example, you could use just about any mobile device with Wi-Fi enabled, and search for wireless networks. From that you can glean the name of the wireless network, the connection speed/type, and whether encryption is used. Or, you could do this from a wireless-enabled desktop or laptop computer by using the built-in wireless network finding software, either by Microsoft, by another OS manufacturer, or by a network adapter manufacturer. But, one of the best ways is to use a third-party program such as NetStumbler. This can give very detailed information about the wireless networks that are available. In fact, it is the type of tool that war-drivers would use, so it makes sense for you, as the security administrator, to use it as well, and see what your enemy sees.

Next, based on your wireless scans and physical inspections, you want to locate and shut down any unauthorized WAPs, rogue devices, or evil twins, and remove any devices causing interference or jamming.

Then, for the authorized WAPs, reduce the power level of the antennas until you can scan them from inside the perimeter of the office but not from the outside. This may take several attempts to get it just right, but it pretty much eliminates the attacker's ability to scan for your network. This is a common method, especially if you are using 802.11n or 802.11ac, which have powerful ranges. Of course, this does not address malicious insiders, but other solutions such as authentication, NIDS/NIPS, and so on can be used to deal with them.

If possible, disable the SSID to make it invisible. The SSID broadcast is not the only way that a WAP can be located, but disabling it is a good first step.

Finally, secure the authorized WAPs in the manner you did during Case Studies 1 and 2. Update the device, set complex passwords, use strong encryption, and consider MAC filtering.

Video Solution: Watch the video solution: "8-3: War-driving...and the Cure" on the accompanying disc.

Case Study 8-4 Solution

As you can see, being in charge of the security for a network can be a lot of work—a full-time job perhaps, given the size of a network. Remember that you are attempting to do the following:

- Ensure that *confidential* files remain secret.
- Keep the *integrity* of your data intact.
- Make sure that data is still *available* to the appropriate persons.

Use the CIA approach to help govern your actions as a security administrator. Add layers of security so that you end up with a solid defense-in-depth plan, ultimately protecting your network and data on multiple levels. See Table 8-5 for some possible solutions to the issues you face.

Table 8-5 LAN and WLAN Security Issues and Solutions

Issue	Your Solution
E-mail and web servers need to be separated from the LAN.	Implement a DMZ.
The WAP is not running any encryption.	Configure WPA2 and AES.
Your boss wants additional authentication for the wireless network above and beyond the WAP's inherent ability.	Utilize a RADIUS server or similar external authentication device.
You have discovered that several computers' wired connections suffer from EMI. They have confidential information and are potential victims for wiretapping.	Replace unshielded twisted-pair (UTP) connections with shielded twisted-pair (STP).
The firewall is not configured for the proper type of packet filtering.	Implement SPI, and increase the level of NAT filtering if necessary.
Users on the network need to be protected from malicious content on websites.	Use a proxy server with a content filter.
You are concerned about anomalous packets and want them to be removed from the network if they are found.	Install an inline NIPS between the firewall and the Internet or in between the firewall and the switch.
There is a long distance wired connection between the firewall and the extranet. There are areas of the building that are not particularly secure and could be accessed by malicious insiders who could possibly attempt wiretapping.	Use fiber-optic connections between the firewall and extranet. Install a CCTV system.

Simulation: Complete the simulation: “8-4: Planning Network Security.”

This page intentionally left blank



This chapter covers the following subjects:

- **Physical Security:** An organization's building is one of its greatest assets and as such it should be properly protected. This section details door access, biometric readers, access logs, and video surveillance to teach you some of the ways to protect the building, its contents, and its inhabitants and to ensure proper authentication when a person enters a building.
- **Authentication Models and Components:** You can use various methods and models to authenticate a person who wants to access computer networks and resources. This section delves into local authentication technologies such as Kerberos, LDAP, and 802.1X, and remote authentication types such as RAS and VPN.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 2.7, 2.9, 3.6, 4.3, 5.1, and 5.2.

Physical Security and Authentication Models

I suppose that at times life on this planet is all about proving oneself. The world of security is no different. To gain access to an organization’s building and ultimately to its resources, you must first prove yourself in a physical manner, providing indisputable evidence of your identity. Then, perhaps you can gain access by being authenticated, as long as the system authenticating you accepts your identification. Finally, if all this goes through properly, you should be authorized to specific resources such as data files, printers, and so on.

Some people use the terms identification, authentication, and authorization synonymously. Although this might be somewhat acceptable in everyday conversation, we need to delve a bit deeper and attempt to make some distinctions between the three.

- **Identification:** When a person is in a state of being identified. It can also be described as something that identifies a person such as an ID card.
- **Authentication:** When a person’s identity is confirmed or verified through the use of a specific system. Authorization to specific resources cannot be accomplished without previous authentication of the user. This might also be referred to as access control, but generally authentication is considered to be a component of access control.
- **Authorization:** When a user is given permission to access certain resources. This can be accomplished only when authentication is complete.

The CompTIA Security+ exam concentrates most on the terms authentication and access control. This chapter focuses mostly on the authentication portion of access control. The rest of access control is covered in Chapter 10, “Access Control Methods and Models.”

First, we cover the physical ways that a person can be authenticated. Then, we move on to ways that a person can be authenticated to a computer network, whether they are attempting to connect locally (for example, on the LAN) or attempting to connect remotely (for example, via a VPN).

Authentication is required to gain access to a secure area of the building or to gain access to secure data. A person might authenticate themselves in one of

several ways depending on the authentication scheme used, by presenting one of the following:

Key Topic

- **Something the user knows:** Such as a password or pin
- **Something the user has:** Such as a smart card or ID card
- **Something the user does:** Such as a signature or gesture
- **Something the user is:** Such as a thumbprint or retina scan or other biometric
- **Somewhere the user is:** Such as “at work,” “at the home office,” or “on the road”

Another term you might hear in your travels is **identity proofing**, which is an initial validation of an identity. For example, when employees working for a government agency want to enter a restricted building, the first thing they must do is show their ID. A guard or similar person then does an initial check of that ID. Additional authentication systems would undoubtedly ensue. Identity proofing is also when an entity validates the identity of a person applying for a certain credential with that entity. It could be used for anonymous access as well.

As you go through this chapter and read about the following physical and logical authentication technologies, try to remember this introduction and apply these concepts to each of those authentication types.

Foundation Topics

Physical Security

To control access, physical security can be considered the first line of defense, sort of like a firewall is the first line of defense for a network. Implementing physical access security methods should be a top priority for an organization. Unfortunately, securing physical access to the organization’s building sometimes slumps to the bottom of the list. Or a system is employed, but it fails to mitigate risk properly. In some cases, the system is not maintained well. Proper building entrance access and secure access to physical equipment are vital. And anyone coming and going should be logged and surveyed. Let’s discuss a few of the ways that we can secure physical access to an organization’s building.

General Building and Server Room Security

Protecting an organization’s building is an important step in general security. The more security a building has, the less you have to depend on your authentication system. A building’s perimeter should be surveyed for possible breaches; this

includes all doors, windows, loading docks, and even the roof. The area around the building should be scanned for hiding places; if there are any they should be removed. The area surrounding the building should be well lit at night. Some companies may opt to use security guards and guard dogs. It is important that these are trained properly; usually an organization will enlist the services of a third-party security company. Video surveillance can also be employed to track an individual's movements. Video cameras should be placed on the exterior perimeter of the building in an area hard to access, for example, 12 feet or higher with no lateral or climbing access. The more well hidden the cameras are the better. Video cameras can also be placed inside the building, especially in secure areas such as executive offices, wiring closets, server rooms, and research and development areas. Many organizations use **closed-circuit television (CCTV)**, but some opt for a wired/wireless IP-based solution. Either way, the video stream may be watched and recorded, but it should not be broadcast. Video cameras are an excellent way of tracking user identities. However, proper lighting is necessary inside and outside in order for the cameras to capture images well. Motion detectors are also common as part of a total alarm system. They are often infrared-based (set off by heat) or ultrasonic-based (set off by certain higher frequencies). We could go on and on about general building security, but this chapter focuses on authentication. Besides, I think you get the idea. If your organization is extremely concerned about building security, and doubts that it has the knowledge to protect the building and its contents properly, consider hiring a professional.

The server room is the lifeblood in today's organizations. If anything happens to the server room, the company could be in for a disaster. We talk more about how an organization can recover from disasters in Chapter 15, "Redundancy and Disaster Recovery," but the best policy is to try to avoid disasters before they happen. So there are some things you should think about when it comes to server room security. First, where is the server room to be placed? It's wise to avoid basements or any other areas that might be prone to water damage. Second, the room should be accessible only to authorized IT persons. This can be accomplished by using one of many door access systems. The room should also have video surveillance saved to a hard drive located in a different room of the building or stored offsite. All devices and servers in the server room should have complex passwords that only the authorized IT personnel have knowledge of. Devices and servers should be physically locked down with cable locks to prevent theft. If necessary, network cabling to each server should be approved circuits and meet the requirements for protected distribution systems. We discuss wired security in Chapter 8, "Securing Network Media and Devices," and talk more about server room security and building security in Chapter 15 and Chapter 16, "Policies, Procedures, and People."

NOTE Security doesn't just mean securing data; it also means user safety—keeping an organization's employees secure. To this end, properly planned fire drills, exit signs, escape plans, and escape routes are all vital. We'll discuss this more in Chapter 16.

For now, let's focus on how to impede unauthorized access. Secure door access is the number one way to stop intruders from getting into the building or server room. If the system is set up properly, then the intruder cannot be authenticated. Let's talk about door access in a little more depth.

Door Access

Lock the door! Sounds so simple, yet it is often overlooked. As a person in charge of security for a small business or even a midsized business, you have to think about all types of security, including entrances to the building. Door locks are essential. When deciding on a locking system to use, you should take into account the type of area your building is in and the crime rate, and who will have authorized access to the building. If you purchase regular door locks that work with a key, it is recommended that you get two or three of them. The first one should be tested. Can you break in to it with a credit card, jeweler's screwdriver, or other tools? And a backup should always be on hand in case the current door lock gets jimmied in an attempt to force a break-in. Cipher locks are a decent solution when regular key locks are not enough but you don't want to implement an electronic system. The cipher lock uses a punch code to lock the door and unlock it. Though it will have a relatively low number of combinations, the fact that they have to be attempted manually makes it difficult to get past them.

Of course, many organizations (and especially government) get more technical with their door access systems. Electronic access control systems such as cardkey systems are common. These use scanning devices on each door used for access to the building. They read the cardkeys that you give out to employees and visitors. These cardkeys should be logged; it should be known exactly who has which key at all times. The whole system is guided by a cardkey controller. This controller should be placed in a wiring closet or in a server room, and that room should be locked as well (and protected by the cardkey system). Some companies implement separate cardkey systems for the server room and for the main entrances. Some systems use photo ID badges for identification and authentication to a building's entrance. They might have a magnetic stripe similar to a credit card, or they might have a barcode or use an RFID chip. A key card door access system is another good practice for tracking user identities.

NOTE Hardware-based **security tokens** are physical devices given to authorized users to help with authentication. These devices might be attached to a keychain or are part of a card system. Hardware-based tokens might be used as part of the door access system or as something that gives access to an individual computer. As one example, RSA tokens carry and generate rolling one-time passwords (OTPs), each of which is valid for only one login session or transaction.

Another possibility is the smart card. The smart card falls into the category of “something a person has” and is known as a token. It’s the size of a credit card and has an embedded chip that stores and transacts data for use in secure applications such as hotel guest room access, prepaid phone services, and more. Smart cards have multiple applications, one of which is to authenticate users by swiping the card against a scanner, thus securing a computer or a computer room. The smart card might have a photo ID as well. Examples of smart cards include the PIV card (Personal Identity Verification), which is required for all US government employees and contractors, and the Common Access Card (CAC), which is used to identify Department of Defense (DoD) military personnel, other DoD civilian government employees, and so on. These cards not only identify the person and are responsible for authentication to buildings and systems, but can also encrypt and digitally sign e-mails. These cards might be used as part of a multifactor authentication scheme in which there is a combination of username/password (or PIN) and a smart card. Advanced smart cards have specialized cryptographic hardware that can use algorithms such as RSA and 3DES but generally use private keys to encrypt data. (More on encryption and these encryption types is provided in Chapter 13, “Encryption and Hashing Concepts.”) A smart card might incorporate a microprocessor (as is the case with the PIV and CAC cards). A smart card security system usually is composed of the smart card itself, smart card readers, and a back-office database that stores all the smart card access control lists and history.

Older technologies use proximity sensors, but this is not considered very secure today. However, the more complex the technology, the more it costs. Often, in these situations, budgeting becomes more important to organizations than mitigating risk; and generally the amount of acceptable risk increases as the budget decreases. So, you will probably see proximity-based door access systems. HID (also known as HID Global) is an example of a company that offers various levels of door access control systems. Figure 9-1 shows an example of a proximity-based door access card.

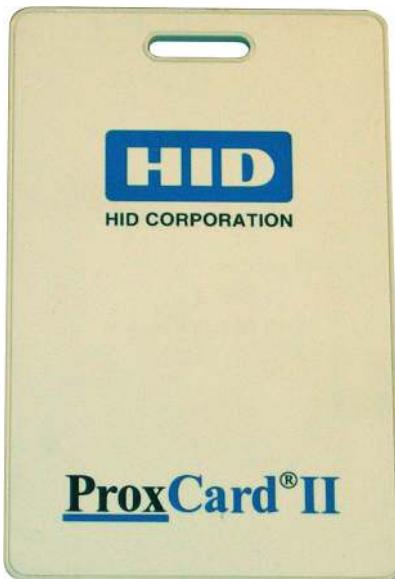


Figure 9-1 Example of a Proximity-Based Door Access Card

To increase security of the entrances of the building, some organizations implement **mantraps**, which are areas between two doorways, meant to hold people until they are identified and authenticated. This might be coupled with security guards, video surveillance, multifactor authentication, and sign-in logs. The main purpose of a physical access log or sign-in log is to show who entered the facility and when.

Door access systems are considered by many to be the weakest link in an enterprise. This can be taken to the next level by also incorporating biometrics, thus creating a different type of multifactor authentication scheme.

Biometric Readers

Biometrics is the science of recognizing humans based on one or more physical characteristics. Biometrics is used as a form of authentication and access control. It is also used to identify persons who might be under surveillance.

Biometrics falls into the category of “something a person is.” Examples of bodily characteristics that are measured include fingerprints, retinal patterns, iris patterns, and even bone structure. Biometric readers (for example, fingerprint scanners) are becoming more common in door access systems and on laptops or as USB devices. Biometric information can also be incorporated into smart card technology. An example of a biometric door access system provider is Suprema, which has various levels of access systems including some that incorporate smart cards and biometrics,

together forming a multifactor authentication system. There are lots of providers of fingerprint scanners (also called fingerprint *readers*) including Verifi, SecuGen, and Nitgen. These fingerprint recognition systems are usually USB-based.

Biometrics can be seen in many movies and TV shows. However, many biometric systems over the past decade have been easily compromised. It has only been of late that readily available biometric systems have started to live up to the hype. Thorough investigation and testing of a biometric system is necessary before purchase and installation. In addition, it should be used in a multifactor authentication scheme. The more factors the better, as long as your users can handle it. (You would be surprised what a little bit of training can do.) Voice recognition software has made great leaps and bounds since the turn of the millennium. A combination of biometrics, voice recognition, and pin access would make for an excellent three-factor authentication system. But as always, only if you can get it through budgeting!

Authentication Models and Components

Now that we've covered some physical authentication methods, let's move into authentication models, components, and technologies used to grant or deny access to operating systems and computer networks.

The first thing a security administrator should do is plan what type of authentication model to use. Then, consider what type of authentication technology and how many factors of authentication will be implemented. Also for consideration is how the authentication system will be monitored and logged. Getting more into the specifics, will only local authentication be necessary? Or will remote authentication also be needed? And which type of technology should be utilized? Will it be Windows-based or a third-party solution? Let's discuss these concepts now and give some different examples of the possible solutions you can implement.

Authentication Models

Many small businesses and even some midsized businesses often have one type of authentication to gain access to a computer network—the username and password. In today's security conscious world, this is not enough for the average organization. Some companies share passwords or fail to enforce password complexity. In addition, password-cracking programs are becoming more and more powerful and work much more quickly than they did just five years ago, making the username and password authentication scheme limiting. Not to say that it shouldn't be used, but perhaps it should be enforced, enhanced, and integrated with other technologies.

Because of the limitations of a single type of authentication such as username and password, organizations sometimes use multiple factors of authentication. **Multifactor authentication** is when two or more types of authentication are used when

dealing with user access control. An example of multifactor authentication would be when a user needs to sign in with a username and password and swipe some type of smart card or use some other type of physical token at the same time. Adding factors of authentication makes it more difficult for a malicious person to gain access to a computer network or an individual computer system. Sometimes an organization uses three factors of authentication—perhaps a smart card, biometrics, and a username/password. The disadvantages of a multifactor authentication scheme are that users need to remember more information and remember to bring more identification with them, and more IT costs and more administration will be involved.

Some organizations have several or more computer systems that an individual user might need access to. By default, each of these systems will have a separate login. It can be difficult for users to remember the various logins. **Single sign-on (SSO)** is when a user can log in once but gain access to multiple systems without being asked to log in again. This is complemented by single sign-off, which is basically the reverse; logging off signs off a person from multiple systems. Single sign-on is meant to reduce password fatigue, or password chaos, which is when a person can become confused and possibly even disoriented when having to log in with several different usernames and passwords. It is also meant to reduce IT help desk calls and password resets. By implementing a more centralized authentication scheme such as single sign-on, many companies have reduced IT costs significantly. If implemented properly, single sign-on can also reduce phishing. In large networks and enterprise scenarios, it might not be possible for users to have a single sign-on, and in these cases it might be referred to as *reduced* sign-on. Single sign-on can be Kerberos-based, integrated with Windows authentication, or token- or smart card-based.

SSO is a derivative of **federated identity management** (also called FIM or FIIdM). This is when a user's identity, as well as the user's attributes, is shared across multiple identity management systems. These various systems can be owned by one organization; for example, Microsoft offers the Forefront Identity Manager software, which can control user accounts across local and cloud environments. Also, Google, Yahoo!, and Amazon are examples of companies that utilize this federation approach. But, some providers join forces so that information can be shared across multiple services and environments between the companies, yet still allow the user a single login.

While an SSO is easier for the user to remember, it acts as a single point of failure as well. In addition, sometimes a company might not be watching out for the user's best interests—either unwittingly or otherwise—and might fail to realize that multiple systems have been configured as a transitive trust. We mentioned the transitive trust concept in Chapter 6, “Networking Protocols and Threats.” When it comes to authentication, it can be especially damaging. Let's say that a user has an account with Company A, and has a separate account with Company B. Imagine that Companies A and B have a two-way trust. Now, let's say there is a third organization,

Company C, that has a two-way trust with Company B. At this point, the user's account information from Companies A and B could be shared with Company C, even though the user never signed up with that company. This kind of activity is frowned upon, but the user might not even know when it happens—two companies might merge, or a company might be bought out or otherwise absorbed by another. So, when it comes to authentication, it is sometimes wise to avoid trust relationships, and strongly consider whether single sign-on will ultimately be more beneficial or costly to your organization.

NOTE Web-based SSO can be problematic due to disparate proprietary technologies. To help alleviate this problem, Security Assertion Markup Language (SAML) and the OpenID protocol were developed. These specify separate roles for the user, the service provider, and the identity provider.

Whatever the type of authentication scheme used, it needs to be monitored periodically to make sure that it's working properly. The system should block people who cannot furnish proper identification, and should allow access to people who do have proper identification. Sometimes there are failures in which an authentication system will improperly authenticate people. A few examples of these include the following:

- **False positive:** This is when a system authenticates a user who should not be allowed access to the system. A similar example of this in biometric systems is the false acceptance error.
- **False negative:** This is when a system denies a user who actually should be allowed access to the system. A similar example of this in biometric systems is the false rejection error.

The previous two examples are the ones you should know for the exam. Other terminology used when dealing with authentication systems includes true positive, which is when legitimate persons are authenticated properly and given access to the system, and true negative, which is when illegitimate persons are denied access as they should be. Both of these are proper functions so they usually don't come up as a conversation piece.

The type of authentication technology used will factor into the number of false positives and false negatives that occur in any authentication scheme. Let's talk about some of those authentication technologies now.

Localized Authentication Technologies

There are several types of technologies for authenticating a user to a local area network. Examples that are software-based include LDAP and Kerberos, whereas an example that includes physical characteristics would be 802.1X. Keep in mind that there is a gray area between localized and remote authentication technologies. I've placed each technology in the category in which it is used the most commonly.

During this section and the next one, we mention several encryption concepts that work with the various authentication technologies. These encryption concepts and protocols are covered in detail in Chapter 13 and Chapter 14, "PKI and Encryption Protocols."

802.1X and EAP

802.1X is an IEEE standard that defines port-based network access control (PNAC). Not to be confused with 802.11x WLAN standards, **802.1X** is a data link layer authentication technology used to connect hosts to a LAN or WLAN. 802.1X allows you to apply a security control that ties physical ports to end-device MAC addresses, and prevents additional devices from being connected to the network. It is a good way of implementing port security, much better than simply setting up MAC filtering.

It all starts with the central connecting device such as a switch or wireless access point. These devices must first enable 802.1X connections; they must have the 802.1X protocol (and supporting protocols) installed. Vendors that offer 802.1X-compliant devices (for example, switches and wireless access points) include Cisco, Symbol Technologies, and Intel. Next, the client computer needs to have an operating system, or additional software, that supports 802.1X. The client computer is known as the supplicant. All recent Windows versions support 802.1X, including Windows 8, 7, Vista, and XP, though each comes with its own set of advantages and disadvantages. OS X offers support as well, and Linux computers can use Open1X to enable client access to networks that require 802.1X authentication.

802.1X encapsulates the **Extensible Authentication Protocol (EAP)** over wired or wireless connections. EAP is not an authentication mechanism in itself, but instead defines message formats. 802.1X is the authentication mechanism and defines how EAP is encapsulated within messages. An example of an 802.1X-enabled network adapter is shown in Figure 9-2. In the figure, you can see that the box for enabling 802.1X has been checked, and that the type of network authentication method for 802.1X is EAP.

Key Topic

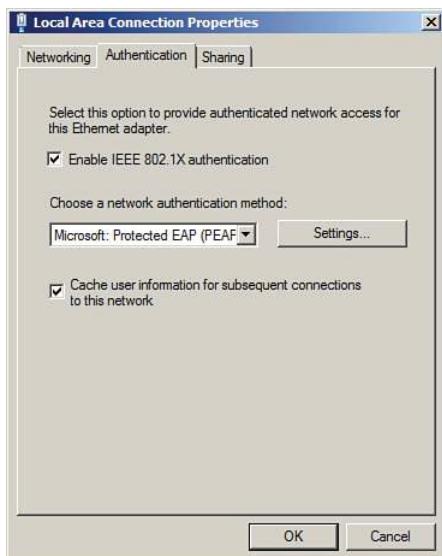


Figure 9-2 Example of an 802.1X-Enabled Network Adapter in Windows

NOTE 802.1X can be enabled in Windows by accessing the Local Area Connection Properties page.

Following are three components to an 802.1X connection:

- **Supplicant:** A software client running on a workstation. This is also known as an authentication agent.
- **Authenticator:** A wireless access point or switch.
- **Authentication server:** An authentication database, most likely a RADIUS server.

The typical 802.1X authentication procedure has four steps. The components used in these steps are illustrated in Figure 9-3.

Key Topic

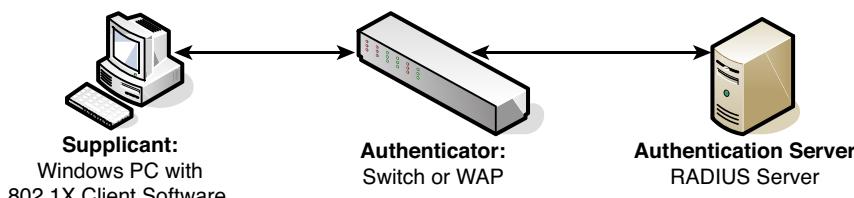


Figure 9-3 Components of a Typical 802.1X Authentication Procedure

NOTE 802.1X authentication components include a supplicant, authenticator, and authentication server.

- Step 1. Initialization**—If a switch or wireless access point detects a new supplicant, the port connection enables port 802.1X traffic; other types of traffic are dropped.
- Step 2. Initiation**—The authenticator (switch or wireless access point) periodically sends EAP requests to a MAC address on the network. The supplicant listens for this address and sends an EAP response that might include a user ID or other similar information. The authenticator encapsulates this response and sends it to the authentication server.
- Step 3. Negotiation**—The authentication server then sends a reply to the authenticator. The authentication server specifies which EAP method to use. (These are listed next.) Then the authenticator transmits that request to the supplicant.
- Step 4. Authentication**—If the supplicant and the authentication server agree on an EAP method, the two transmit until there is either success or failure to authenticate the supplicant computer.

Following are several types of EAP authentication:

- **EAP-MD5:** This is a challenge-based authentication providing basic EAP support. It enables only one-way authentication and not mutual authentication.
- **EAP-TLS:** This version uses Transport Layer Security, which is a certificate-based system that does enable mutual authentication. This does not work well in enterprise scenarios because certificates must be configured or managed on the client side and server side.
- **EAP-TTLS:** This version is Tunneled Transport Layer Security and is basically the same as TLS except that it is done through an encrypted channel, and it requires only server-side certificates.
- **EAP-FAST:** This uses a protected access credential instead of a certificate to achieve mutual authentication. FAST stands for flexible authentication via secure tunneling.
- **PEAP:** This is the **Protected Extensible Authentication Protocol** (also known as Protected EAP). This uses MSCHAPv2, which supports authentication via Microsoft Active Directory databases. It competes with EAP-TTLS and includes legacy password-based protocols. It creates a TLS tunnel by acquiring a public key infrastructure (PKI) certificate from a server known as a certificate authority (CA). The TLS tunnel protects user

authentication much like EAP-TTLS. More information on PKI and CAs can be found in Chapter 14.

Cisco also created a proprietary protocol called LEAP (Lightweight EAP), and it is just that—proprietary. To use LEAP, you must have a Cisco device such as an Aironet WAP or Catalyst switch, or another vendor’s device that complies with the Cisco Compatible Extensions program. Then you must download a third-party client on Windows computers to connect to the Cisco device. Most WLAN vendors offer an 802.1X LEAP download for their wireless network adapters.

Although 802.1X is often used for port-based network access control on the LAN, especially VLANs, it can also be used with VPNs as a way of remote authentication. Central connecting devices such as switches and wireless access points remain the same, but on the client side 802.1X would need to be configured on a VPN adapter, instead of a network adapter.

Many vendors, such as Intel and Cisco, refer to 802.1X with a lowercase x; however, the IEEE displays this on its website with an uppercase X. The protocol was originally defined in 2001 (802.1X-2001) and has been redefined in 2004 and 2010 (802.1X-2004 and 802.1X-2010, respectively). There are several links to more information about 802.1X in the “View Recommended Resources” appendix on this book’s disc.

LDAP

The **Lightweight Directory Access Protocol (LDAP)** is an application layer protocol used for accessing and modifying directory services data. It is part of the TCP/IP suite. Originally used in WAN connections, it has developed over time into a protocol commonly used by services such as Microsoft Active Directory on Windows Server domain controllers. LDAP acts as the protocol that controls the directory service. This is the service that organizes the users, computers, and other objects within the Active Directory. An example of the Active Directory is shown in Figure 9-4. Take note of the list of users (known as objects of the Active Directory) from the Users folder that is highlighted. Also observe other folders such as Computers that house other objects (such as Windows client computers).

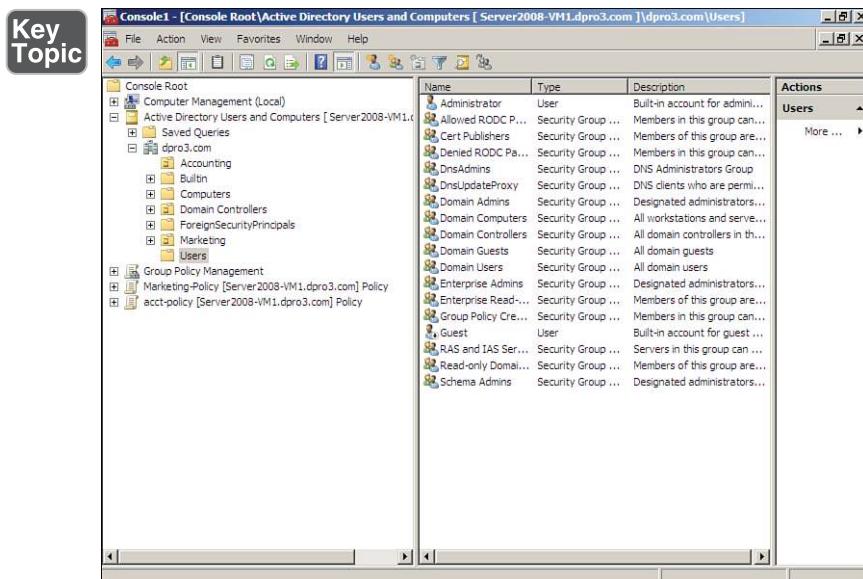


Figure 9-4 Example of Active Directory Showing User Objects

A Microsoft server that has Active Directory and LDAP running will have inbound port 389 open by default. To protect Active Directory from being tampered with, Secure LDAP can be used, which brings into play SSL (Secure Sockets Layer) on top of LDAP and uses inbound port 636 by default. Other implementations of LDAP use TLS (Transport Layer Security) over LDAP.

Kerberos and Mutual Authentication

Kerberos is an authentication protocol designed at MIT that enables computers to prove their identity to each other in a secure manner. It is used most often in a client-server environment; the client and the server both verify each other's identity. This is known as two-way authentication or **mutual authentication**. Often, Kerberos protects a network server from illegitimate login attempts, just as the mythological three-headed guard dog of the same name (also known as Cerberus) guards Hades.

A common implementation of Kerberos occurs when a user logs on to a Microsoft domain. (Of course, I am not saying that Microsoft domains are analogous to Hades!) The domain controller in the Microsoft domain is known as the key distribution center (KDC). This server works with **tickets** that prove the identity of users. The KDC is composed of two logical parts: the authentication server and the ticket-granting server. Basically, a client computer attempts to authenticate itself to the authentication server portion of the KDC. When it does so successfully, the client receives a

ticket. This is actually a ticket to get other tickets. The client uses this preliminary ticket to demonstrate its identity to a ticket-granting server in the hopes of ultimately getting access to a service—for example, making a connection to the Active Directory of a domain controller.

The domain controller running Kerberos will have inbound port 88 open to the service logon requests from clients. Figure 9-5 shows a `netstat -an` command run on a Windows Server that has been promoted to a domain controller. It points out port 88 (used by Kerberos) and port 389 (used by LDAP) on the same domain controller.

Key Topic

```

c:\> C:\WINDOWS\system32\cmd.exe
c:\> netstat -an | more
...
TCP 10.254.254.252:1025 10.254.254.252:1279 ESTABLISHED
TCP 10.254.254.252:1039 10.254.254.252:389 ESTABLISHED
TCP 10.254.254.252:1141 10.254.254.252:389 ESTABLISHED
TCP 10.254.254.252:1183 10.254.254.252:389 CLOSE_WAIT
TCP 10.254.254.252:1229 10.254.254.252:1025 ESTABLISHED
TCP 10.254.254.252:1927 10.254.254.252:1025 TIME_WAIT
TCP 127.0.0.1:389 127.0.0.1:1032 ESTABLISHED
TCP 127.0.0.1:389 127.0.0.1:1033 ESTABLISHED
TCP 127.0.0.1:389 127.0.0.1:1044 ESTABLISHED
TCP 127.0.0.1:389 127.0.0.1:1041 ESTABLISHED
TCP 127.0.0.1:1032 127.0.0.1:389 ESTABLISHED
TCP 127.0.0.1:1033 127.0.0.1:389 ESTABLISHED
TCP 127.0.0.1:1034 127.0.0.1:389 ESTABLISHED
TCP 127.0.0.1:1041 127.0.0.1:389 ESTABLISHED
TCP 127.0.0.1:1929 127.0.0.1:445 TIME_WAIT
UDP 0.0.0.0:445 **:**
UDP 0.0.0.0:500 **:**
UDP 0.0.0.0:1029 **:**
UDP 0.0.0.0:1036 **:**
UDP 0.0.0.0:14500 **:**
UDP 10.254.254.252:53 **:**
UDP 10.254.254.252:88 ← Kerberos Port 88
UDP 10.254.254.252:123 **:**
UDP 10.254.254.252:137 **:**
UDP 10.254.254.252:138 **:**
UDP 10.254.254.252:389 ← LDAP Port 389
UDP 10.254.254.252:464 **:**
UDP 127.0.0.1:53 **:**
UDP 127.0.0.1:123 **:**
UDP 127.0.0.1:1031 **:**
UDP 127.0.0.1:1035 **:**
UDP 127.0.0.1:1036 **:**
UDP 127.0.0.1:1040 **:**
UDP 127.0.0.1:1126 **:**
UDP 127.0.0.1:1146 **:**
UDP 127.0.0.1:1179 **:**
UDP 127.0.0.1:1182 **:**
UDP 127.0.0.1:1805 **:**

c:\>

```

Figure 9-5 Results of the `netstat -an` Command on a Windows Server

Kerberos is designed to protect against replay attacks and eavesdropping. One of the drawbacks of Kerberos is that it relies on a centralized server such as a domain controller. This can be a single point of failure. To alleviate this problem, secondary and tertiary domain controllers can be installed that keep a copy of the Active Directory and are available with no downtime in case the first domain controller fails. Another possible issue is one of synchronicity. Time between the clients and the domain controller must be synchronized for Kerberos to work properly. If for some reason a client attempting to connect to a domain controller becomes desynchronized, it cannot complete the Kerberos authentication, and as an end result the user cannot log on to the domain. This can be fixed by logging on to the affected client locally and synchronizing the client's time to the domain controller by using the `net time` command. For example, to synchronize to the domain controller in Figure 9-5, the command would be

```
net time \\10.254.254.252 /set
```

Afterward, the client should be able to connect to the domain. We revisit Kerberos and how it makes use of encryption keys in Chapter 13.

Kerberos—like any authentication system—is vulnerable to attack. Older Windows operating systems that run, or connect to, Kerberos are vulnerable to privilege escalation attacks; and newer Windows operating systems are vulnerable to spoofing. Of course, Microsoft will quickly release updates for these kinds of vulnerabilities (as they are found), but for the security administrator that does not allow Windows Update to automatically update, it's important to review the CVEs for the Microsoft systems often.

Remote Desktop Services

Remote Desktop Services (also referred to as Terminal Services) enables the remote control of Windows computers (most importantly for this section, Windows servers) from a client computer. This client computer could be on the LAN or out on the Internet, so the term “remote” is used loosely. It can also be used to enable client access to specific applications.

In Windows Server 2008 it is configured within Remote Desktop Management Server, and in Windows Server 2012 R2 it is configured via the Remote Desktop Services server role. This application is in charge of authenticating terminal users and will do so if the user has been configured properly. For example, users in question must have Remote Access permissions enabled within the properties of their account. Remote Desktop Services/Terminal Services authentication integrates directly with standard Windows Server authentication. The remote desktop/terminal server will have inbound port 3389 open to accept connections from remote clients. Client sessions are stored at the terminal server, which allows for disconnections and later reuse.

NOTE Remote Desktop Services is still often referred to as its original name, Terminal Services. In fact, the underlying service name is actually still called “TermService.”

Some of the vulnerabilities to Remote Desktop Services—and the Remote Desktop Protocol in general, otherwise known as RDP—include an extremely well-known port, comparatively weak encryption, and a lack of multifactor authentication. Because of this, you might choose to utilize another remote control application. At this point, security is relative, and your decision on what tool to use will be based on the type of data you are protecting.

As mentioned, the port is 3389 by default, and is extremely well known. But it can be modified within the inbound computer's Registry at the following path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
```

Third-party applications such as VNC, TeamViewer, and so on can be more secure in this respect because they can use web-based connections via HTTPS on port 443. Out-of-the-box, RDP is generally limited to SSL (TLS 1.0) with a 128-bit key based on the RC4 algorithm (which is considered crackable, though difficult to do so). However, RDP can also comply with Federal Information Processing Standard (FIPS) 140 encryption methods, but additional hardware and software modules are required, which might incur an unacceptable expense. On the other hand, third-party remote control applications such as the ones mentioned earlier will often use RSA encryption for the HTTPS connection, and the Advanced Encryption Standard (AES) with up to 256-bit keys for session security. Some third-party applications also offer multifactor authentication; for example, a passcode in combination with the standard username/password login. However, multifactor authentication could always be added to RDP as a separate module (at a price). Your final decision of what application to use will be based on cost, the number of remote connections required, the platforms you need to support, and, of course, the level of security you desire.

Captive Portals

Have you ever stayed at a hotel or gone to a coffee shop that had free Wi-Fi? What happens when you use that wireless network? Chances are you are redirected to a web page that asks for authentication prior to normal Internet use. Quite often you will have to create an account with a username (usually an e-mail address) and password, which is authenticated through e-mail. This is an example of a captive portal. So, the captive portal method forces the HTTP client (for instance, a web browser) of the wireless device to authenticate itself via a web page. The redirection could occur as HTTP or as DNS. Quite often, it is done through basic SSL-secured HTTPS web pages. This can often be circumvented with the use of a packet sniffer such as Wireshark. To avoid this potential hazard, an organization can opt for extended or multifactor authentication. There are many free, one-time charge, and subscription-based applications that an organization can use for Windows and Linux-based platforms. The whole point of the technology is to be able to track users that access the free wireless network. If the user performs any suspect actions, the user can be traced by way of e-mail address, IP address, and MAC address, in addition to other means if multifactor authentication is used.

Remote Authentication Technologies

Even more important than authenticating local users is authenticating *remote* users. The chances of illegitimate connections increase when you allow remote users to connect to your network. Examples of remote authentication technologies include RAS, VPN, RADIUS, TACACS+, and CHAP. Let's discuss these now.

Remote Access Service

Remote Access Service (RAS) began as a service that enabled dial-up connections from remote clients. Nowadays, more and more remote connections are made with high-speed Internet technologies such as cable Internet, DSL, and fiber-optic connections. But we can't discount the dial-up connection. It is used in certain areas where other Internet connections are not available, and is still used as a fail-safe in many network operation centers and server rooms to take control of networking equipment.

One of the best things you can do to secure a RAS server is to deny access to individuals who don't require it. Even if the user or user group is set to "not configured," it is wise to specifically deny them access. Allow access to only those users who need it; and monitor on a daily basis the logs that list who connected. If there are any unknowns, investigate immediately. Be sure to update the permissions list often in the case that a remote user is terminated or otherwise leaves the organization.

The next most important security precaution is to set up RAS authentication. One secure way is to use the **Challenge-Handshake Authentication Protocol (CHAP)**, which is an authentication scheme used by the Point-to-Point Protocol (PPP), which in turn is the standard for dial-up connections. It uses a challenge-response mechanism with one-way encryption. Due to this, it is not capable of mutual authentication in the way that Kerberos is, for example. CHAP uses DES and MD5 encryption types, which we cover in Chapter 13. Microsoft developed its own version of CHAP known as MS-CHAP; an example of this is shown in Figure 9-6. The figure shows the Advanced Security Settings dialog box of a dial-up connection. Notice that this particular configuration shows that encryption is required, and that the only protocol allowed is MS-CHAP V2. Of course, the RAS server has to be configured to accept MS-CHAP connections as well. You also have the option to enable EAP for the dial-up connection. Other RAS authentication protocols include SPAP, which is of lesser security, and PAP, which sends usernames and passwords in clear text—obviously insecure and to be avoided.

Key Topic

Figure 9-6 MS-CHAP Enabled on a Dial-Up Connection

NOTE Use CHAP, MS-CHAP, or EAP for dial-up connections. Verify that it is configured properly on the RAS server and dial-up client to ensure a proper handshake.

The CHAP authentication scheme consists of several steps. It authenticates a user or a network host to entities such as Internet access providers. CHAP periodically verifies the identity of the client by using a three-way handshake. The verification is based on a shared secret. After the link has been established, the authenticator sends a challenge message to the peer. The encrypted results are compared, and finally the client is either authorized or denied access.

The actual data transmitted in these RAS connections is encrypted as well. By default Microsoft RAS connections are encrypted by the RSA RC4 algorithm. More information on this can also be found in Chapter 13.

Now you might say, “But Dave, who cares about dial-up connections?” Well, there are two reasons that they are important. First, the supporting protocols, authentication types, and encryption types are used in other technologies; this is the basis for those systems. Second, as I mentioned before, some organizations still use the dial-up connection—for remote users or for administrative purposes. And hey, don’t downplay the dial-up connection. Old-school dial-up guys used to tweak the connection to the point where it was as fast as some DSL versions and as reliable. So there are going to be die-hards out there as well. Plus, there are some areas of the United States, and the rest of the world, that have no other option than dial-up.

However, RAS now has morphed into something that goes beyond just dial-up. VPN connections that use dial-up, cable Internet, DSL, and so on are all considered remote access.

Virtual Private Networks

A **virtual private network (VPN)** is a connection between two or more computers or devices not on the same private network. Generally, VPNs use the Internet to connect one host to another. It is desirable that only proper users and data sessions make their way to a VPN device; because of this, data encapsulation and encryption are used. A “tunnel” is created through any LANs and WANs that might intervene; this tunnel connects the two VPN devices together. Every time a new session is initiated, a new tunnel is created, which makes the connection secure.

VPNs normally use one of two tunneling protocols, as shown in Table 9-1.



Table 9-1 VPN Tunneling Protocols

Tunneling Protocol	Description	Port Used
Point-to-Point Tunneling Protocol (PPTP)	This is the more commonly used tunneling protocol (although that is quickly changing) but the less secure solution of the two listed here. PPTP generally includes security mechanisms, and no additional software or protocols need to be loaded. A VPN device or server must have inbound port 1723 open to enable incoming PPTP connections. PPTP works within the Point-to-Point Protocol (PPP), which is also used for dial-up connections, as mentioned earlier.	Port 1723
Layer 2 Tunneling Protocol (L2TP)	This is quickly gaining popularity due to the inclusion of IPsec as its security protocol. Although this is a separate protocol and L2TP doesn't have any inherent security, L2TP will be considered the more secure solution because IPsec is required in most L2TP implementations. A VPN device or server must have inbound port 1701 open to enable incoming L2TP connections.	Port 1701

PPTP and L2TP can cause a lot of havoc if the security settings are not configured properly on the client side and the server side. This can cause errors; you can find a link to the list of these error codes in the “View Recommended Resources” appendix on this book’s disc. We cover PPTP and L2TP encryption methods in Chapter 14.

Figure 9-7 shows an illustration of a VPN. Note that the VPN server is on one side of the cloud, and the VPN client is on the other. It should be known that the VPN client will have a standard IP address to connect to its own LAN. However, it will receive a second IP address from the VPN server or a DHCP device. This second IP address works “inside” the original IP address. So, the client computer will have two IP addresses; in essence, the VPN address is encapsulated within the logical IP address. As previously mentioned, dial-up authentication protocols such as CHAP are also used in other technologies; this is one of those examples. VPN adapters, regardless of the Internet connection used, can use MS-CHAP, as shown in Figure 9-7. To further increase authentication security, a separate RADIUS server can be used with the VPN server—we talk more about RADIUS in the next section.

NOTE VPNs use either PPTP (port 1723) or L2TP (port 1701) and can also incorporate CHAP on the client side and RADIUS servers for authentication.

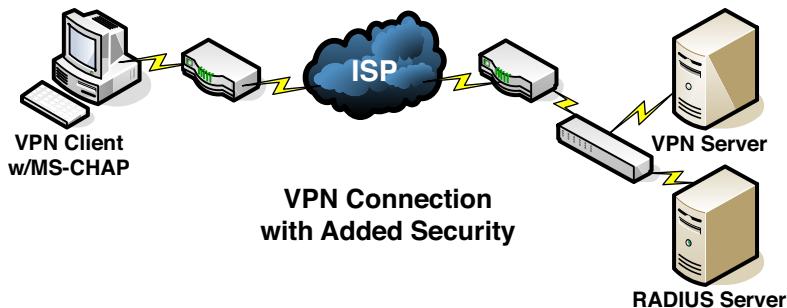


Figure 9-7 Illustration of a VPN

A Microsoft VPN can be set up on a standard Windows Server by configuring Routing and Remote Access Service (RRAS). Remote access policies can be created from here that permit or deny access to groups of users for dial-in or VPN connections. In Windows Server 2012/2008, you would need to set up RRAS as part of the Network Policy and Access Services role. Then you would right-click the Remote Access Logging & Policies node and access the Network Policy Server (NPS) window to create a new RRAS policy. Figure 9-8 displays the initiation of a RRAS VPN policy.

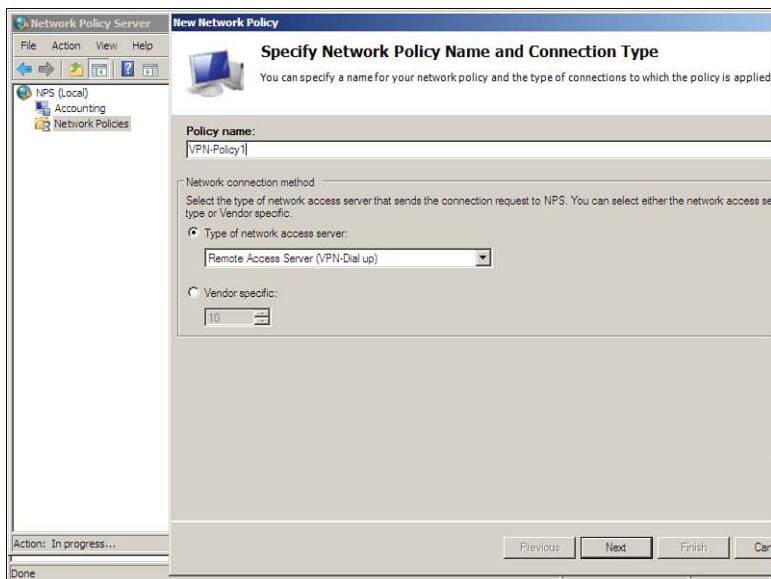


Figure 9-8 RRAS VPN Policy on a Windows Server

NOTE You could also configure DirectAccess if you have Windows Server 2008 R2 (or higher) and Windows 7 clients (or higher) to implement a Microsoft-based VPN.

Of course, you can run a VPN locally as well, and some companies do. We do just that in the video solution to Case Study 9-4 at the end of the chapter to demonstrate the setup of a working VPN.

You don't have to use a server for incoming VPN sessions. Hardware appliances are offered by several vendors. Larger organizations that need hundreds of simultaneous connections should opt for a **VPN concentrator** as their solution. Or, it might be part of your unified threat management (UTM) solution.

RADIUS Versus TACACS

We mentioned RADIUS previously in this chapter and in Chapter 8, and said that it could be used in combination with a SOHO router in order to provide strong authentication. Let's define it further: The **Remote Authentication Dial-In User Service (RADIUS)** provides centralized administration of dial-up, VPN, and wireless authentication and can be used with EAP and 802.1X. To set this up on a Windows Server, the Internet Authentication Service must be loaded; it is usually set up

on a separate physical server. RADIUS is a client-server protocol that runs on the application layer of the OSI model.

RADIUS works within the AAA concept: It is used to authenticate users, authorize them to services, and account for the usage of those services. RADIUS checks whether the correct authentication scheme such as CHAP or EAP is used when clients attempt to connect. It commonly uses port 1812 for authentication messages and port 1813 for accounting messages (both of which use UDP as the transport mechanism). In some proprietary cases, it uses ports 1645 and 1646 for these messages, respectively. Memorize these four ports for the exam!

The Terminal Access Controller Access-Control System (TACACS) is one of the most confusing-sounding acronyms ever. Now that we have reached the pinnacle of computer acronyms, let's really discuss what it is. TACACS is another remote authentication protocol that was used more often in Unix networks. In Unix, the TACACS service is known as the TACACS daemon. The newer and more commonly used implementation of TACACS is called **Terminal Access Controller Access-Control System Plus (TACACS+)**. It is not backward compatible with TACACS. TACACS+, and its predecessor XTACACS, were developed by Cisco. TACACS+ uses inbound port 49 like its forerunners; however, it uses TCP as the transport mechanism instead of UDP. Let's clarify: the older TACACS and XTACACS technologies are not commonly seen anymore. The two common protocols for remote authentication used today are RADIUS and TACACS+.

There are a few differences between RADIUS and TACACS+. Whereas RADIUS uses UDP as its transport layer protocol, TACACS+ uses TCP as its transport layer protocol, which is usually seen as a more reliable transport protocol (though each will have its own unique set of advantages). Also, RADIUS combines the authentication and authorization functions when dealing with users; however, TACACS+ separates these two functions into two separate operations that introduce another layer of security. It also separates the accounting portion of AAA into its own operation.

RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information such as the username can be easily captured, without need of decryption, by a third party. However, TACACS+ encrypts the entire body of the access-request packet. So, effectively TACACS+ encrypts entire client-server dialogues, whereas RADIUS does not. Finally, TACACS+ provides for more types of authentication requests than RADIUS.

Table 9-2 summarizes the local and remote authentication technologies we have covered thus far.

**Table 9-2** Summary of Authentication Technologies

Authentication Type	Description
802.1X	An IEEE standard that defines Port-based Network Access Control (PNAC). 802.1X is a data link layer authentication technology used to connect devices to a LAN or WLAN.
LDAP	An application layer protocol used for accessing and modifying directory services data. It is part of the TCP/IP suite. Originally used in WAN connections, it has morphed into a protocol commonly used by services such as Microsoft Active Directory.
Kerberos	An authentication protocol designed at MIT that enables computers to prove their identity to each other in a secure manner. It is used most often in a client-server environment; the client and the server both verify each other's identity.
RAS	A service that enables dial-up and various types of VPN connections from remote clients.
CHAP	An authentication scheme used by the Point-to-Point Protocol (PPP) that is the standard for dial-up connections. It utilizes a challenge-response mechanism with one-way encryption.
RADIUS	Used to provide centralized administration of dial-up, VPN, and wireless authentication. It can be used with EAP and 802.1X. Uses ports 1812 and 1813, or 1645 and 1646, over a UDP transport.
TACACS	Another remote authentication protocol, similar to RADIUS, and used more often in Unix networks, though it is deprecated.
TACACS+	Remote authentication developed by Cisco, similar to RADIUS but separates authentication and authorization into two separate processes. Uses port 49 over a TCP transport.

Chapter Summary

Users must constantly prove themselves to the world of technology. It's amazing how many times a person can be authenticated during a typical day. An authentication method could be as simple as typing an e-mail address and password; for example, when logging into a web-based e-mail system. Or, it could be as complex as a multifactor authentication system; where a user is required to enter a password, then a PIN, then swipe a smart card, and finally scan a thumb!

The complexity of the authentication system will be based on the confidentiality level of an organization's data and resources. If a person can supply the necessary identification and credentials, and the system is configured properly, that person

should be authenticated to the system, and finally authorized to access data, or enter a server room, or whatever the case may be. The authentication system can include methods such as: something the user knows, something the user has, something the user does, something the user is, and somewhere the user is. These systems span from the physical (door access systems and biometrics) to the logical (localized and remote authentication software/hardware). In some cases, to make things easier for the end user, a single sign-on (SSO) is utilized where the user need only remember one password. Sometimes it's not even the user that is authenticated, but the computer itself; for example, when a network adapter adheres to the 802.1X protocol.

Authentication systems can fail. The most common failures are the *false positive*—when a system authenticates a user who should not be allowed access to the system, and the *false negative*—when a system denies a user who actually should be allowed access to the system. A system that has too many failures will cause user distress, and should be reconfigured and tested carefully.

Examples of localized authentication systems include 802.1X, LDAP, Kerberos, and RDP. Examples of remote authentication systems include RAS, VPNs, and RADIUS. However, there is a gray area here. Some local systems can be used for remote access as well, and vice versa. Remember: This is not a cut-and-dried technology in general; for example, RDP could be used locally or over the Internet. It all hinges on what your organization needs for its end users. Nowadays, more and more people work from home or on the road, making remote authentication vital to the organization's efficiency and overall production.

One thing to keep in mind is that attackers (and con artists) are very smart. In fact, the sad truth is that they are often smarter than some IT people. A poorly designed authentication system is tantamount to leaving the physical key in the door. However, a well-planned authentication system can save an organization millions of dollars and untold man hours in the long run.

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 9-3 lists a reference of these key topics and the page number on which each is found.

Table 9-3 Key Topics for Chapter 9

Key Topic Element	Description	Page Number
Bulleted list	Authentication methods	340
Figure 9-2	Example of an 802.1X-enabled network adapter in Windows	349
Figure 9-3	Components of a typical 802.1X authentication procedure	349
Figure 9-4	Example of Active Directory showing user objects	352
Figure 9-5	Results of the netstat -an command on a Windows Server	353
Figure 9-6	MS-CHAP enabled on a dial-up connection	357
Table 9-1	VPN tunneling protocols	358
Table 9-2	Summary of authentication technologies	362

Define Key Terms

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

identification, authentication, authorization, identity proofing, closed-circuit television (CCTV), security tokens, mantrap, biometrics, multifactor authentication, single sign-on (SSO), federated identity management, false positive, false negative, 802.1X, Extensible Authentication Protocol (EAP), Protected Extensible Authentication Protocol (PEAP), Lightweight Directory Access Protocol (LDAP), Kerberos, mutual authentication, tickets, Remote Access Service (RAS), Challenge-Handshake Authentication Protocol (CHAP), virtual private network (VPN), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), VPN concentrator, Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+)

Review Questions

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

1. Which of the following is the verification of a person's identity?
 - A. Authorization
 - B. Accountability
 - C. Authentication
 - D. Password
2. Which of the following would fall into the category of "something a person is"?
 - A. Passwords
 - B. Passphrases
 - C. Fingerprints
 - D. Smart cards
3. Which of the following are good practices for tracking user identities? (Select the two best answers.)
 - A. Video cameras
 - B. Key card door access systems
 - C. Sign-in sheets
 - D. Security guards
4. What are two examples of common single sign-on authentication configurations? (Select the two best answers.)
 - A. Biometrics-based
 - B. Multifactor authentication
 - C. Kerberos-based
 - D. Smart card-based
5. Which of the following is an example of two-factor authentication?
 - A. L2TP and IPsec
 - B. Username and password
 - C. Thumbprint and key card
 - D. Client and server

6. What is the main purpose of a physical access log?
 - A. To enable authorized employee access
 - B. To show who exited the facility
 - C. To show who entered the facility
 - D. To prevent unauthorized employee access
7. Which of the following is not a common criteria when authenticating users?
 - A. Something you do
 - B. Something you are
 - C. Something you know
 - D. Something you like
8. Of the following, what two authentication mechanisms require something you physically possess? (Select the two best answers.)
 - A. Smart card
 - B. Certificate
 - C. USB flash drive
 - D. Username and password
9. Which of the following is the final step a user needs to take before that user can access domain resources?
 - A. Verification
 - B. Validation
 - C. Authorization
 - D. Authentication
10. To gain access to your network, users must provide a thumbprint and a user-name and password. What type of authentication model is this?
 - A. Biometrics
 - B. Domain logon
 - C. Multifactor
 - D. Single sign-on

- 11.** The IT director has asked you to set up an authentication model in which users can enter their credentials one time, yet still access multiple server resources. What type of authentication model should you implement?
- A.** Smart card and biometrics
 - B.** Three-factor authentication
 - C.** SSO
 - D.** VPN
- 12.** Which of the following about authentication is false?
- A.** RADIUS is a client-server system that provides authentication, authorization, and accounting services.
 - B.** PAP is insecure because usernames and passwords are sent as clear text.
 - C.** MS-CHAPv1 is capable of mutual authentication of the client and server.
 - D.** CHAP is more secure than PAP because it encrypts usernames and passwords.
- 13.** What types of technologies are used by external motion detectors? (Select the two best answers.)
- A.** Infrared
 - B.** RFID
 - C.** Gamma rays
 - D.** Ultrasonic
- 14.** In a secure environment, which authentication mechanism performs better?
- A.** RADIUS because it is a remote access authentication service.
 - B.** RADIUS because it encrypts client-server passwords.
 - C.** TACACS+ because it is a remote access authentication service.
 - D.** TACACS+ because it encrypts client-server negotiation dialogues.
- 15.** Which port number does the protocol LDAP use when it is secured?
- A.** 389
 - B.** 443
 - C.** 636
 - D.** 3389

- 16.** Which of the following results occurs when a biometric system identifies a legitimate user as unauthorized?
- A.** False rejection
 - B.** False positive
 - C.** False acceptance
 - D.** False exception
- 17.** Of the following, which is not a logical method of access control?
- A.** Username/password
 - B.** Access control lists
 - C.** Biometrics
 - D.** Software-based policy
- 18.** Which of the following permits or denies access to resources through the use of ports?
- A.** Hub
 - B.** 802.11n
 - C.** 802.11x
 - D.** 802.1X
- 19.** Your data center has highly critical information. Because of this you want to improve upon physical security. The data center already has a video surveillance system. What else can you add to increase physical security? (Select the two best answers.)
- A.** A software-based token system
 - B.** Access control lists
 - C.** A mantrap
 - D.** Biometrics
- 20.** Which authentication method completes the following in order: logon request, encrypts value response, server, challenge, compare encrypts results, and authorize or fail referred to?
- A.** Security tokens
 - B.** Certificates
 - C.** Kerberos
 - D.** CHAP

- 21.** What does a virtual private network use to connect one remote host to another? (Select the best answer.)
- A.** Modem
 - B.** Network adapter
 - C.** Internet
 - D.** Cell phone
- 22.** Two items are needed before a user can be given access to the network. What are these two items?
- A.** Authentication and authorization
 - B.** Authorization and identification
 - C.** Identification and authentication
 - D.** Password and authentication
- 23.** Kerberos uses which of the following? (Select the two best answers.)
- A.** Ticket distribution service
 - B.** The Faraday cage
 - C.** Port 389
 - D.** Authentication service
- 24.** Which of the following authentication systems makes use of a Key Distribution Center?
- A.** Security tokens
 - B.** CHAP
 - C.** Kerberos
 - D.** Certificates
- 25.** Of the following, which best describes the difference between RADIUS and TACACS+?
- A.** RADIUS is a remote access authentication service.
 - B.** RADIUS separates authentication, authorization, and auditing capabilities.
 - C.** TACACS+ is a remote access authentication service.
 - D.** TACACS+ separates authentication, authorization, and auditing capabilities.

- 26.** Which of the following best describes the proper method and reason to implement port security?
- A.** Apply a security control that ties specific ports to end-device MAC addresses, and prevents additional devices from being connected to the network.
 - B.** Apply a security control that ties specific ports to end-device IP addresses, and prevents additional devices from being connected to the network.
 - C.** Apply a security control that ties specific ports to end-device MAC addresses, and prevents all devices from being connected to the network.
 - D.** Apply a security control that ties specific ports to end-device IP addresses, and prevents all devices from being connected to the network.
- 27.** You are tasked with setting up a wireless network that uses 802.1X for authentication. You set up the wireless network using WPA2 and CCMP; however, you don't want to use a PSK for authentication. Which of the following options would support 802.1X authentication?
- A.** Kerberos
 - B.** CAC card
 - C.** Preshared key
 - D.** RADIUS
- 28.** Which two options can prevent unauthorized employees from entering a server room? (Select the two best answers.)
- A.** Bollards
 - B.** CCTV
 - C.** Security guard
 - D.** 802.1X
 - E.** Proximity reader
- 29.** What is the most secure method of authentication and authorization in its default form?
- A.** TACACS
 - B.** Kerberos
 - C.** RADIUS
 - D.** LDAP

- 30.** When attempting to grant access to remote users, which protocol uses separate, multiple-challenge responses for each of the authentication, authorization, and audit processes?
- A.** RADIUS
 - B.** TACACS
 - C.** TACACS+
 - D.** LDAP
- 31.** Before gaining access to the data center, you must swipe your finger on a device. What type of authentication is this?
- A.** Biometrics
 - B.** Single sign-on
 - C.** Multifactor
 - D.** Tokens
- 32.** Which of the following is an authentication system that uses UDP as the transport mechanism?
- A.** LDAP
 - B.** Kerberos
 - C.** RADIUS
 - D.** TACACS+
- 33.** Your organization provides to its employees badges that are encoded with a private encryption key and specific personal information. The encoding is used to provide access to the organization's network. What type of authentication method is being used?
- A.** Token
 - B.** Biometrics
 - C.** Kerberos
 - D.** Smart card
- 34.** You are in charge of training a group of technicians on the authentication method their organization uses. The organization currently runs an Active Directory infrastructure. Which of the following best correlates to the host authentication protocol used within that organization's IT environment?
- A.** TACACS+
 - B.** Kerberos

- C. LDAP
 - D. 802.1X
35. Which of the following is an authentication and accounting service that uses TCP as its transport mechanism when connecting to routers and switches?
- A. Kerberos
 - B. RADIUS
 - C. Captive portal
 - D. TACACS+

Answers and Explanations

1. C. Authentication is the verification of a person's identity. Authorization to specific resources cannot be accomplished without previous authentication of the user.
2. C. Fingerprints are an example of something a person is. The process of measuring that characteristic is known as biometrics.
3. A. and B. Video cameras enable a person to view and visually identify users as they enter and traverse a building. Key card access systems can be configured to identify a person as well, as long as the right person is carrying the key card!
4. C. and D. Kerberos and smart card setups are common single sign-on configurations.
5. C. Two-factor authentication (or dual-factor) means that two pieces of identity are needed prior to authentication. A thumbprint and key card would fall into this category. L2TP and IPsec are protocols used to connect through a VPN, which by default require only a username and password. Username and password is considered one-factor authentication. There is no client and server authentication model.
6. C. A physical access log's main purpose is to show who entered the facility and when. Different access control and authentication models will be used to permit or prevent employee access.
7. D. Common criteria when authenticating users includes something you do, something you are, something you know, something you have, and somewhere you are. A person's likes and dislikes are not common criteria; although, they may be asked as secondary questions when logging in to a system.

8. **A.** and **C.** Two of the authentication mechanisms that require something you physically possess include smart cards and USB flash drives. Key fobs and cardkeys would also be part of this category. Certificates are granted from a server and are stored on a computer as software. The username/password mechanism is a common authentication scheme, but it is something that you type and not something that you physically possess.
9. **C.** Before a user can gain access to domain resources, the final step is to be authorized to those resources. Previously the user should have provided identification to be authenticated.
10. **C.** Multifactor authentication means that the user must provide two different types of identification. The thumbprint is an example of biometrics. Username and password are examples of a domain logon. Single sign-on would only be one type of authentication that enables the user access to multiple resources.
11. **C.** SSO (single sign-on) enables users to access multiple servers and multiple resources while entering their credentials only once. The type of authentication can vary but will generally be a username and password. Smart cards and biometrics is an example of two-factor authentication. VPN is short for virtual private network.
12. **C.** MS-CHAPv1 is not capable of mutual authentication of the client and server. Mutual authentication is accomplished with Kerberos. All the other statements are true.
13. **A.** and **D.** Motion detectors often use infrared technology; heat would set them off. They also use ultrasonic technology; sounds in higher spectrums that humans cannot hear would set these detectors off.
14. **D.** Unlike RADIUS, TACACS+ (Terminal Access Controller Access-Control System Plus) encrypts client-server negotiation dialogues. Both protocols are remote authentication protocols.
15. **C.** Port 636 is the port used to secure LDAP. Port 389 is the standard LDAP port number. Port 443 is used by HTTPS (SSL/TLS), and port 3389 is used by RDP.
16. **A.** If a biometric system identifies a legitimate user as unauthorized, it is known as a false rejection or a false negative. A false positive is when a system authenticates a user who should not be allowed access. False acceptance is similar to a false positive in biometric systems. False exceptions have to do with software that has failed and needs to be debugged.
17. **C.** The only answer that is not a logical method of access control is biometrics. Biometrics deals with the physical attributes of a person and is the most tangible of the answers. All the rest deal with software, so they are logical methods.

- 18. D.** 802.1X permits or denies access to resources through the use of ports. It implements Port-based Network Access Control or PNAC. This is part of the 802.1 group of IEEE protocols. 802.1X should not be confused with 802.11x, which is an informal term used to denote any of the 802.11 standards including 802.11b, 802.11g, 802.11n, and 802.11ac. A hub connects computers by way of physical ports but does not permit or deny access to any particular resources; it is a simple physical connector of computers.
- 19. C. and D.** A mantrap is a device made to capture a person. It is usually an area with two doorways, the first of which leads to the outside and locks when the person enters, the second of which leads to the secure area and is locked until the person is granted access. Biometrics can help in the granting of this access by authenticating the user in a secure way, such as thumbprint, retina scan, and so on. Software-based token systems and access control lists are both logical and do not play into physical security.
- 20. D.** CHAP, the Challenge Handshake Authentication Protocol, authenticates a user or a network host to entities like Internet access providers. CHAP periodically verifies the identity of the client by using a three-way handshake; the verification is based on a shared secret. After a link has been established, the authenticator sends a challenge message to the peer; this does not happen in the other three authentication methods listed.
- 21. C.** The Internet is used to connect hosts to each other in virtual private networks. A particular computer will probably also use a VPN adapter and/or a network adapter. Modems generally are used in dial-up connections and are not used in VPNs.
- 22. C.** Before users can be given access to the network, the network needs to identify them and authenticate them. Later, users may be authorized to use particular resources on the network. Part of the authentication scheme may include a username and password. This would be known as an access control method.
- 23. A. and D.** Kerberos uses a ticket distribution service and an authentication service. This is provided by the Key Distribution Center. A Faraday cage is used to block data emanations. Port 389 is used by LDAP. One of the more common ports that Kerberos uses is port 88.
- 24. C.** Kerberos uses a KDC (Key Distribution Center) to centralize the distribution of certificate keys and keep a list of revoked keys.
- 25. D.** Unlike RADIUS, TACACS+ separates authentication, authorization, and auditing capabilities. The other three answers are incorrect and are not differences between RADIUS and TACACS+.

- 26.** A. You can achieve port security by applying a security control (such as 802.1X), which ties specific physical ports to end-device MAC addresses and prevents additional devices from being connected to the network. Note that port security solutions such as 802.1X are data link layer technologies (layer 2) so they deal with MAC addresses, not IP addresses. You wouldn't want to exclude all devices from being connected to the network as this would cause a severe problem with connectivity.
- 27.** D. RADIUS is a common back-end authenticator for 802.1X. When setting up a wireless access point, the two security mode options are usually PSK (pre-shared key), which is stored on the WAP, and Enterprise, which usually refers authentication to an external RADIUS server. Kerberos deals with authentication to Microsoft domains. CAC cards are smart cards that are used for ID and authentication to systems.
- 28.** C. and E. If a person doesn't have the proper proximity card, that person will be prevented from entering a server room or other protected room. Security guards can also prevent people from accessing unauthorized areas. However, bollards (short vertical posts) probably wouldn't stop a person, besides they aren't normally installed in front of a server room entrance. CCTV video surveillance is a detective control, but not a preventive control. 802.1X deals with authentication, not with physical security.
- 29.** B. Kerberos is the most secure method of authentication listed. It has a more complicated system of authentication than TACACS (which is outdated) and RADIUS (which is used in different scenarios than Kerberos). LDAP deals with directories (for example, the ones on a Microsoft domain controller), which Kerberos first needs to give access to.
- 30.** C. TACACS+ is the only answer listed that uses separate processes for authentication, authorization, and auditing. That is one of the main differences between it and RADIUS. TACACS is deprecated and is not often seen in the field. LDAP deals with managing directories of information.
- 31.** A. Fingerprint technology is part of the realm of biometrics. Single sign-on means that you can use one type of authentication to get access to more than one system. While that could be going on in this scenario, it is not explicit, so biometrics is the more accurate answer. Multifactor means that more than one type of authentication is needed; for example, a fingerprint and a PIN. Let's say that users were expected to type a PIN into a keypad to gain access to the data center. You might find over time that some persons who enter don't match the owner of the PIN. That uncertainty can be avoided by incorporating biometrics. Tokens are used to gain access to systems and networks, and might include rolling one-time passwords, but do not incorporate a person's physical characteristics such as a fingerprint.

- 32. C.** RADIUS is the authentication system that uses UDP as the transport mechanism. The others all use TCP. Remember, RADIUS uses ports 1812 and 1813 (or 1645 and 1646), LDAP uses 389 (or 636 for secure LDAP), Kerberos uses port 88, and TACACS+ uses port 49.
- 33. D.** A badge encoded with a private encryption key would be an example of a smart card. Tokens are software-based and could be used with a USB flash drive or could be stored on a mobile device. An example of biometrics is a thumbprint scan or retina scan. Kerberos is an authentication technology used by operating systems such as Windows (often in domain scenarios).
- 34. B.** If the organization runs Active Directory, that means they have a Windows Server that is acting as a domain controller. These use the Kerberos authentication system by default. TACACS+ is an example of a remote authentication system, but is owned by Cisco, and is not a part of Active Directory. LDAP is the protocol in Windows that controls Active Directory objects, and works in conjunction with Kerberos, but is not the actual authentication method used. 802.1X is an authentication method used by network adapters on the data link layer.
- 35. D.** TACACS+ is an authentication, accounting, and authorization service. It uses TCP as its transport mechanism. Kerberos authenticates only, and can use TCP and UDP. RADIUS performs authentication and accounting but uses UDP as the transport mechanism. A captive portal redirects people in an effort to authenticate them. It will often do this within a web browser, and might use TCP (HTTPS), but does not perform accounting services.

Case Studies for Chapter 9

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

Case Study 9-1: Choosing Physical Security Methods

Scenario: You are the security administrator for Prowse Inc., a technology research firm that has 20 users in the main office, several offsite computers, a data center, and an unsecured computer lab. Your task is to use physical methods to secure these computers.

Name eight types of physical security methods and define them in Table 9-4. The solution to Case Study 9-1 may have different answers than yours.

Table 9-4 Types of Physical Security Methods

Case Study 9-2: Selecting the Correct Authentication Technology

Scenario: There are many types of authentication technologies. Your organization employs two localized authentication technologies and two remote authentication technologies. Your organization uses a Microsoft Windows Server that runs Active Directory. Also, your organization uses the PPTP protocol. Finally, the remote authentication technology uses UDP as the transport mechanism.

Your task is to identify the four types of authentication technologies your organization uses, describe each one briefly, and specify the inbound port for each. Enter that information in Table 9-5.

Table 9-5 Authentication Technologies Your Organization Uses

Authentication Technology	Brief Description	Port Number Used

Case Study 9-3: Understanding 802.1X

Scenario: You are in charge of implementing an 802.1X solution. Your job is to first define the three main elements of an 802.1X authentication scheme. Next, you must specify the exact technologies you will use for each of those three main elements.

In Table 9-6, describe the three main elements of 802.1X. Then, use the Internet to research actual types of 802.1X-compliant network adapters and components that you can use to create an actual working 802.1X authentication scheme.

Table 9-6 802.1X Authentication Elements

802.1X Element	Description	Actual Component

Case Study 9-4: Setting Up a Secure VPN

Scenario: Your boss wants to enable remote access for several people who will be working from home. You are now in charge of implementing a secure VPN solution for the data commuters.

Name a couple of vendors that offer secure VPN solutions. Describe the two main protocols that are used with VPN connections and specify their port numbers.

Case Study Solutions

Case Study 9-1 Solution

There are many types of physical security methods. Table 9-7 gives eight examples and basic descriptions for them based on the scenario in Case Study 9-1.

Table 9-7 Types of Physical Security Methods—Solution

Physical Security Method	Description
CCTV	Closed-circuit television, used to monitor and record images from server rooms and data centers.
Cable locks	Used to physically lock down computers and monitors; for example, computers in an otherwise unsecured computer lab.
Cipher lock	A type of door lock that uses a basic cipher mechanism where the numbers of the code have to be entered sequentially—often push button operated. Used in server rooms, data centers, and even for entrances to offices.
Proximity badges	Basic swiping cards used to allow access to an office or to a server room. The card (or badge) need only be in close proximity to the sensor for the door in question.
Safe	A wonderful way to protect items such as optical discs, backup tapes, USB flash drives, application and development discs, and so on.
Mantrap	A secure area that can be used to hold a person until that person is authenticated to the area ahead. Often used as entrances to server rooms and data centers (and even offices), while still allowing a means of egress in the case of an emergency.
Biometric scanner	Often a type of scanner that can be used on laptops and other mobile devices. It connects via USB and will usually scan a thumbprint. This type of physical security works great for computers that are located outside the office; for example, computers used by salespersons or data commuters.

Physical Security Description**Method**

Smart cards	Like proximity badges, something a person <i>has!</i> For example, a Common Access Card, which has an embedded chip that can authenticate a user. Excellent choice for highly secure areas such as server rooms and data centers.
-------------	---

Your organization's physical security methods will vary. They will be based on the IT security budget as well as the level of confidentiality of your data. Consider researching additional methods of physical security on the Internet.

Simulation: Complete the simulation “9-1: Choosing Physical Security Methods.”

Case Study 9-2 Solution

This chapter contains many types of authentication technologies, but this particular Case Study scenario was asking for four: Kerberos and LDAP, which are used by Active Directory on Microsoft Windows Server domain controllers; a Remote Access Service—namely VPN—in this case utilizing PPTP; and RADIUS server, which uses UDP as its transport mechanism. See Table 9-8 for the rest of the solution.

Table 9-8 Authentication Technologies Your Organization Uses—Solution

Authentication Technology	Brief Description	Port Number Used
Kerberos	Authenticates users in an Active Directory environment.	88
LDAP	Controls access for users and computers in an Active Directory environment.	389
Remote Access Service (VPN using PPTP)	Allows remote access for computers outside the LAN.	1723
RADIUS	A powerful remote authentication technology used in conjunction with VPN. It utilizes the UDP transport mechanism.	1812 and 1813 (sometimes port 1645 and 1646)

Simulation: Complete the simulation “9-2: Selecting the Correct Authentication Technology.”

Case Study 9-3 Solution

The three main elements of an 802.1X authentication scheme include the supplicant, the authenticator, and the authentication server. There are several companies that offer products that comply with 802.1X secure authentication. See Table 9-9 for descriptions and examples of companies that offer solutions.

Table 9-9 802.1X Authentication Elements—Solution

802.1X Element	Description	Actual Component
Supplicant	A software client running on a workstation. This is also known as an authentication agent.	Many network adapters (wired and wireless) from Intel and Cisco are 802.1X compliant.
Authenticator	A wireless access point or switch.	Cisco and D-Link have options for 802.1X-compliant WAPs and switches.
Authentication server	An authentication database.	Microsoft Windows RADIUS Server.

Video Solution: Watch the video solution “9-3: Understanding 802.1X” on the accompanying disc.

Simulation: Complete the simulation “9-3: Understanding 802.1X.”

Case Study 9-4 Solution

A couple of vendors that offer secure VPN solutions for small offices include D-Link and Cisco (through its subsidiary Linksys), among other manufacturers of SOHO routers. For larger environments you would look to companies such as Cisco, Microsoft, Juniper, and so on. The two main protocols that can be used in a secure VPN solution include PPTP (port 1723) and L2TP (port 1701). L2TP requires specialized certificate services, whereas PPTP does not.

Use the Internet to further research the variety of VPN solutions available.

Video Solution: Watch the video solution “9-4: Setting Up a Secure VPN” on the accompanying disc.



This chapter covers the following subjects:

- **Access Control Models Defined:** This section gets into access control models, such as MAC, DAC, and RBAC, plus methodologies such as implicit deny and job rotation. Before creating and enforcing policies, a plan of action has to be developed, and the access control model to be used should be at the core of that plan.
- **Rights, Permissions, and Policies:** Here, we delve into users, groups, permissions, rights, and policies that can be created on a computer network. By configuring users, templates, and groups in a smart fashion, you can ease administration and increase security at the same time. Policies can control just about anything a user does on the network or on an individual computer. And security templates make it easier than ever to implement a secure set of policies.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 4.4, 5.2, and 5.3.

Access Control Methods and Models

Controlling user access is of paramount importance. You don't want just any Tom, Dick, or Harry to gain admittance to your computer network! The first step in controlling user access is to define who needs to have access and what they need to have access to. After this is done, an access control plan must be developed. This primarily consists of choosing an access control model. Which model you should choose depends on your organization's procedures and written policies, the level of security you need, and the amount of IT resources at your disposal. After a model has been selected, you should implement as many safe practices as possible to bolster the model's effectiveness. Then, you can actually implement security on the computers and network. This includes creating and organizing secure users, groups, and other network objects such as organizational units. More important, it incorporates the use of policies and Group Policy objects. By configuring computer-based policies for your users, groups, and computers, you are forcing them to abide by your organization's rules.

Foundation Topics

Access Control Models Defined

Access control models are methodologies in which admission to physical areas, and more important, computer systems, is managed and organized. Access control, also known as an access policy, is extremely important when it comes to users accessing secure or confidential data. Some organizations also practice concepts such as separation of duties, job rotation, and least privilege. By combining these best practices along with an access control model, a robust plan can be developed concerning how users access confidential data and secure areas of a building.

There are several models for access control, each with its own special characteristics that you should know for the exam. The three most commonly recognized models are discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC). Let's discuss these now.

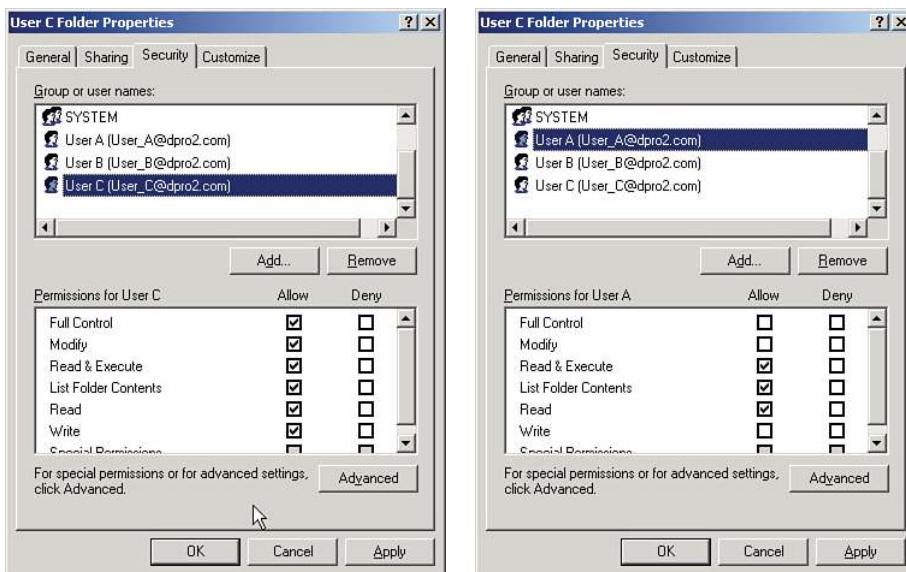
Discretionary Access Control

Discretionary access control (DAC) is an access control policy generally determined by the owner. Objects such as files and printers can be created and accessed by the owner. Also, the owner decides which users are allowed to have access to the objects, and what level of access they may have. The levels of access, or permissions, are stored in access control lists (ACLs).

Originally, DAC was described in The Orange Book as the Discretionary Security Policy and was meant to enforce a consistent set of rules governing limited access to identified individuals. The Orange Book's proper name is the **Trusted Computer System Evaluation Criteria**, or TCSEC, and was developed by the DoD; however, The Orange Book is old (they refer to it in the movie *Hackers* in the 1990s!), and the standard was superseded in 2005 by an international standard called the Common Criteria for Information Technology Security Evaluation (or simply Common Criteria). But the DAC methodology lives on in most of today's personal computers and client/server networks.

NOTE An entire set of security standards was published by the DoD in the 1980s and 1990s known as the “Rainbow Series.” Although The Orange Book is the centerpiece of the series (maybe not in the color spectrum, but as far as security content), there are other ones you might come into contact with, such as The Red Book, which is the Trusted Network Interpretation standard. Some of the standards have been superseded, but they contain the basis for many of today’s security procedures.

An example of DAC would be a typical Windows computer with two users. User A can log on to the computer, create a folder, stock it with data, and then finally configure permissions so that only she can access the folder. User B can log on to the computer, but cannot access User A’s folder by default, unless User A says so, and configures it as so! However, User B can create his own folder and lock down permissions in the same way. Let’s say that there was a third user, User C, who wanted both User A and User B to have limited access to a folder that he created. That is also possible by setting specific permission levels, as shown in Figure 10-1. The first Properties window shows that User C (the owner) has Full Control permissions. This is normal because User C created the folder. But in the second Properties window, you see that User A has limited permissions, which were set by User C.



Key Topic

Figure 10-1 Example of Discretionary Access in Windows

NOTE The owner of a resource controls the permissions to that resource! This is the core of the DAC model.

Windows networks/domains work in the same fashion. Access to objects is based on which user created them and what permissions they assign to those objects. However, in Windows networks we can group users together and assign permissions by way of roles as well. More on that in the role-based access control (RBAC) section.

In a way, DAC, when implemented in client-server networks, is sort of a decentralized administration model. Even though an administrator still has control over most, or all, resources (depending on company policy), the owners retain a certain amount of power over their own resources. But, many companies take away the ability for users to configure permissions. They may create folders and save data to them, but the permissions list is often generated on a parent folder by someone else and is inherited by the subfolder.

There are two important points to remember when talking about the DAC model: First, every object in the system has an owner, and the owner has control over its access policy; and second, access rights, or permissions, can be assigned by the owner to users to specifically control object access.

Mandatory Access Control

Mandatory access control (MAC) is an access control policy determined by a computer system, not by a user or owner, as it is in DAC. Permissions are pre-defined in the MAC model. Historically, it has been used in highly classified government and military multilevel systems, but you will find lesser implementations of it in today's more common operating systems as well. The MAC model defines sensitivity labels that are assigned to *subjects* (users) and *objects* (files, folders, hardware devices, network connections, and so on). A subject's label dictates its security level, or level of trust. An object's label dictates what level of clearance is needed to access it, also known as a trust level (this is also known as *data labeling*). The access controls in a MAC system are based on the security classification of the data and “need-to-know” information—where a user can access only what the system considers absolutely necessary. Also, in the MAC model, data import and export are controlled. MAC is the strictest of the access control models.

An example of MAC can be seen in FreeBSD version 5.0 and higher. In this OS, access control modules can be installed that allow for security policies that label subjects and objects. The enforcement of the policies is done by administrators or by the OS; this is what makes it mandatory and sets it apart from DAC. Another example is Security-Enhanced Linux (SELinux), a set of kernel modifications to Linux that supports DoD-style mandatory access controls such as the requirement for trusted computing base (TCB). Though often interpreted differently, TCB can be described as the set of all hardware and software components critical to a system's security and all associated protection mechanisms. The mechanisms must meet a certain standard, and SELinux helps accomplish this by modifying the kernel of the Linux OS in a secure manner. Like DAC, MAC was also originally defined in The Orange Book, but as the Mandatory Security Policy—a policy that enforces access control based on a user's clearance and by the confidentiality levels of the data. Even though The Orange Book is deprecated, the concept of MAC lives on in today's systems and is implemented in two ways:

- **Rule-based access control:** Also known as label-based access control, this defines whether access should be granted or denied to objects by comparing the object label and the subject label.
- **Lattice-based access control:** Used for more complex determinations of object access by subjects. Somewhat advanced mathematics are used to create sets of objects and subjects and define how the two interact.

NOTE Rule-based access control uses labels, is part of mandatory access control, and should not be confused with *role-based* access control.

NOTE Other related access control models include Bell-LaPadula, Biba, and Clark-Wilson. Bell-LaPadula is a state machine model used for enforcing access control in government applications. It is a less common multilevel security derivative of mandatory access control. This model focuses on data confidentiality and controlled access to classified information. The Biba Integrity Model describes rules for the protection of data integrity. Clark-Wilson is another integrity model that provides a foundation for specifying and analyzing an integrity policy for a computing system.

Role-Based Access Control (RBAC)

Role-based access control (RBAC) is an access model that, like MAC, is controlled by the system, and, unlike DAC, not by the owner of a resource. However, RBAC is different from MAC in the way that permissions are configured. RBAC works with sets of permissions, instead of individual permissions that are label-based. A set of permissions constitutes a role. When users are assigned to roles, they can then gain access to resources. A role might be the ability to complete a specific operation in an organization as opposed to accessing a single data file. For example, a person in a bank who wants to check a prospective client's credit score would be attempting to perform a transaction that is allowed only if that person holds the proper role. So roles are created for various job functions in an organization. Roles might have overlapping privileges and responsibilities. Also, some general operations can be completed by all the employees of an organization. Because there is overlap, an administrator can develop role hierarchies; these define roles that can contain other roles, or have exclusive attributes.

Think about it. Did you ever notice that an administrator or root user is extremely powerful? Perhaps too powerful? And standard users are often not powerful enough to respond to their own needs or fix their own problems. Some operating systems counter this problem by creating mid-level accounts such as Power Users (Microsoft) or Operators (Solaris), but for large organizations, this is not flexible enough. Currently, more levels of roles and special groups of users are implemented in newer operating systems. RBAC is used in database access as well and is becoming more common in the healthcare industry and government.

Table 10-1 summarizes the access control models we discussed in the last three sections: DAC, MAC, and RBAC.

**Table 10-1** Summary of Access Control Models

Access Control Model	Key Points
DAC	Every object in the system has an owner. Permissions are determined by the owner.
MAC	Permissions are determined by the system. Can be rule-based or lattice-based. Labels are used to identify security levels of subjects and objects.
RBAC	Based on roles, or sets of permissions involved in an operation. Controlled by the system.

NOTE Another type of access control method is known as anonymous access control—for example, access to an FTP server. This method uses attributes before access is granted to an object. Authentication is usually not required.

NOTE In general, access control can be centralized or decentralized. *Centralized* access control means that one entity is responsible for administering access to resources. *Decentralized* access control means that more than one entity is responsible, and those entities are closer to the actual resources than the entity would be in a centralized access control scenario.

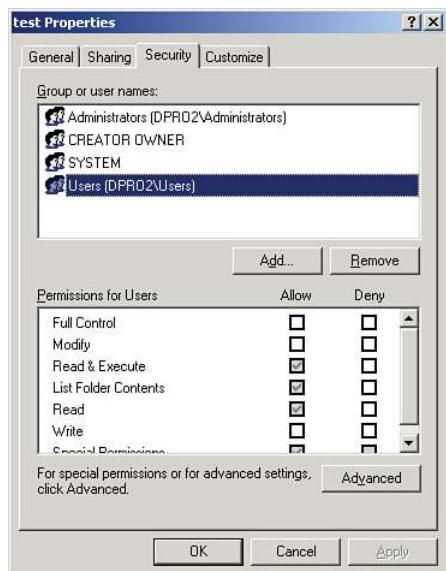
Access Control Wise Practices

After you decide on an access control model that fits your needs, you should consider employing some other concepts. Some of these are used in operating systems automatically to some extent:

- **Implicit deny:** This concept denies all traffic to a resource unless the users generating that traffic are specifically granted access to the resource. Even if permissions haven't been configured for the user in question, that person will still be denied access. This is a default setting for access control lists on a Cisco router. It is also used by default on Microsoft computers to a certain extent. Figure 10-2 shows an example of this. In the folder's permissions, you can see that the Users group has the Read & Execute, List Folder Contents, and Read permissions set to Allow. But other permissions such as Modify are not configured at all—not set to Allow or Deny. Therefore, the users in the Users group

cannot modify data inside the folder because that permission is implicitly denied. Likewise, they can't take full control of the folder.

NOTE Implicit deny will deny users access to a resource unless they are specifically allowed access.



Key Topic

Figure 10-2 Example of Implicit Deny on a Windows Folder

- **Least privilege:** This is when users are given only the amount of privileges needed to do their job and not one iota more. A basic example of this would be the Guest account in a Windows computer. This account (when enabled) can surf the Web and use other basic applications but cannot make any modifications to the computer system. However, least privilege as a principle goes much further. One of the ideas behind the principle is to run the user session with only the processes necessary, thus reducing the amount of CPU power needed. This hopefully leads to better system stability and system security. Have you ever noticed that many crashed systems are due to users trying to do more than they really should be allowed? Or more than the computer can handle? The concept of *least* privilege tends to be absolute, whereas an absolute solution isn't quite possible in the real world. It is difficult to gauge exactly what the "least" amount of privileges and processes would be. Instead,

a security administrator should practice the implementation of minimal privilege, reducing what a user has access to as much as possible. Programmers also practice this when developing applications and operating systems, making sure that the app has only the least privilege necessary to accomplish what it needs to do. This concept is also known as “the principle of least privilege.”

- **Separation of duties:** This is when more than one person is required to complete a particular task or operation. If one person has too much control and completes too many portions of a task, it can become a security risk. The more people involved, the less the chance that a job can be compromised. Checks and balances are employed to make sure that the proper equilibrium of users is maintained. One example of this would be the securing of a new network. There might be one or more security administrators in charge of doing the actual planning, and a couple more doing the actual implementation, and finally another group for testing; or perhaps, a third-party company will do the testing, keeping everything on the up and up. It all depends on the size of the organization and the internal trust level (and the IT budget!).

Separation of duties can also be applied to a single user. For example, if a user on a typical Windows computer (Vista or newer) has a specific set of privileges, but the user wants to do something on the system that requires administrative access, User Account Control (UAC) kicks in and asks for the proper credentials to perform the actions of that role. If the credentials cannot be supplied, UAC blocks the action, keeping the various duties separate.

- **Job rotation:** This is one of the checks and balances that might be employed to enforce the proper separation of duties. Job rotation is when users are cycled through various assignments to
 - Increase user insight as to overall operations
 - Reduce employee boredom
 - Enhance employee skill level
 - Increase operation security

Job rotation creates a pool of people that can do an individual job and discourages hoarding of information. It also helps to protect the purity of an operation. By cross-training people in each department, you defend against fraud and increase awareness, making it easier to detect if it does happen.

By incorporating the implicit deny, least privilege, separation of duties, and job rotation concepts, your total access control plan can be improved greatly. These access control principles can be applied both to desktop computers and to mobile devices. However, the specific way they are applied will depend on the particular operating

systems and the policies—both written and computerized—of the organization you work for.

Rights, Permissions, and Policies

Now that we have a plan for access control, we need to implement it in a tangible way. By strategically setting up organizational units, users, and groups, and by assigning permissions according to our chosen access control model, we can create a safe, guarded working area for all employees. In so doing, we can protect the data on the network.

Users, Groups, and Permissions

User accounts can be added to individual computers or to networks. For example, a Windows client, Linux computer, or Mac can have multiple users. And larger networks that have a controlling server, for example, a Windows domain controller, enable user accounts that can access one or more computers on the domain. In a Microsoft domain, users are added in Active Directory Users and Computers (ADUC), as shown in Figure 10-3.

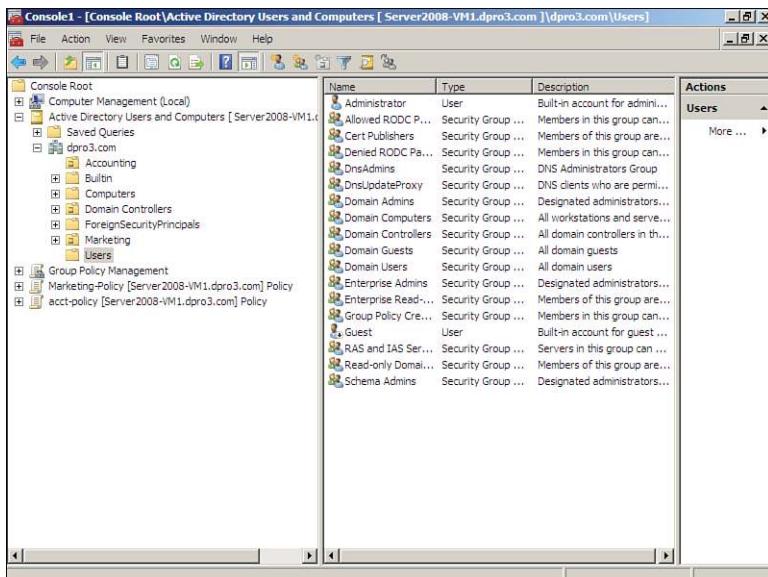


Figure 10-3 The Users Folder Within ADUC on a Windows Server

ADUC can be accessed from Administrative Tools or added as a snap-in to an MMC. Users can be added in one of two places:

- **In the Users folder:** This is located inside the domain name within ADUC.
- **In an OU:** Organizational units can be created within the domain. These are often made to mimic the departments of a company. In Figure 10-3, there are Accounting and Marketing OUs; users can be created within these OUs.

User rights can be modified within the particular user's Properties window. There are many more rights associated with a user account that is stored on a Windows Server domain controller than there are on an individual Windows client computer. For example, the Account tab can be configured so that the user account has an expiration date. You can see this in Figure 10-4, where at the bottom of the Properties window, we had configured Megan's account to expire on April 1, 2013—and that was no April Fools' prank! Immediately after that expiration date, the user couldn't log on to the domain unless her account was reconfigured or she logged on as someone else.

Key Topic

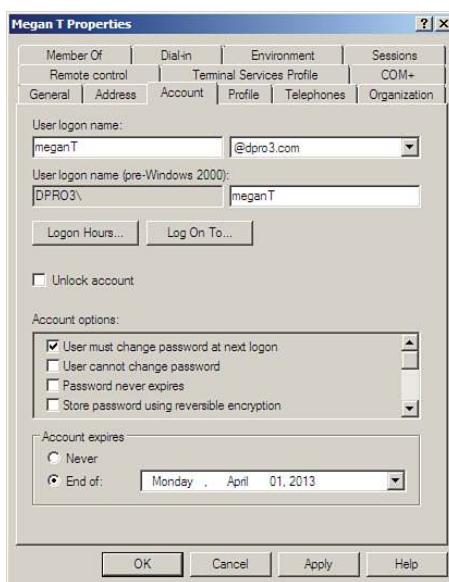
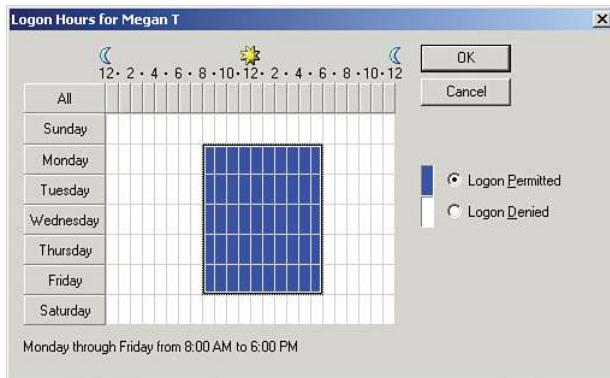


Figure 10-4 User Account Expiration Date

NOTE Users cannot log on to a network after their account has expired. The Account Expiration date in Windows controls this.

By clicking the Logon Hours button, time-of-day restrictions can be configured so that a user can log on only at certain times throughout the week. An example of this is shown in Figure 10-5. In the figure, Megan's user account has been configured in such a way that she can log on to the domain only between 8 a.m. and 6 p.m. Monday–Friday. If she attempts to log on at any other time, the system will deny access. These kinds of access rights are available on domain controllers.



Key Topic

Figure 10-5 Time-of-Day Restrictions for a Standard User

NOTE Users can log on to the network only during their configured logon hours.

Sometimes users have more than one account. This might have been done to allow access to multiple systems or resources. There are plenty of different issues that can occur because of this. To mitigate problems that can develop from a user having two accounts, consider the consolidation of accounts, for example utilizing a federated identity management (FIM) system, one that will incorporate single sign-on. User administration can also benefit from credential management, where passwords, certificates, and other logon credentials are stored in a special folder called a vault. A security administrator should also consider the use of roles (RBAC) and user groups.

Groups can be created to classify users and to ease administration when assigning permissions. If you refer to Figure 10-3, you see that a group is displayed with a two-headed icon (for example, the Domain Admins group). Single users are displayed with a single head, as is the case with the Administrator. By grouping users together, you can save a lot of time when assigning permissions to files and other resources; instead of assigning permissions to one user at a time, it can be done to the entire group in one shot.

Permissions such as file and printer access can be assigned to individual users or to groups. These permissions (also known as access modes) are examples of **access**

control lists (ACLs). An ACL is a list of permissions attached to an object. ACLs reside on firewalls, routers, and computers. Permissions in an ACL might allow access or deny access. It all depends on who is required to have access; then, the configuration is up to you.

In Windows there are two types of permissions. Sharing permissions are basic permissions including Full Control, Change, and Read, which are applied to folders only. These are often ignored in favor of the more powerful (and superseding) NTFS permissions, also called security permissions, which can secure folders and individual files. In a standard Windows folder on a domain, the types of NTFS permissions include the following:

- Full Control
- Modify
- Read & Execute
- List Folder Contents
- Read
- Write

These are shown in Figure 10-6 on a Windows Server in the Properties window of a folder named “test folder.” Note that the Administrators group has full control of the folder. Also note that you can allow particular permissions, or specifically deny those permissions. If a permission is not set to Allow, it will be implicitly denied.

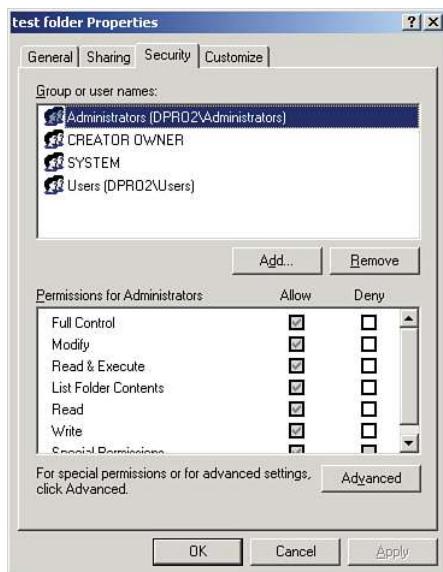


Figure 10-6 NTFS Permissions

In Linux, file permissions are broken down into three types: read, write, and execute (R, W, and X). They can be assigned to three different permission groups: owner, group, and all users (U, G, and O or A). These can be assigned and configured in the command-line with the `chmod` command (change mode), either by group letter or by using a designated numbering system. For example, in the latter case:

- R (Read) = 4
- W (Write) = 2
- X (Execute) = 1

These are added together to form each permission. For example, if a user was given read and write access, the number would be 6. If, however, the person was given read, write, and execute access, the number would be 7. Here's an example of the `chmod` command:

```
chmod 760 testfile
```

In the example we have the `chmod` command followed by the numbers 7, 6, and 0, and the name of the file, "testfile" (of course, the path to that file can be more complex). The first number, 7, represents the owner permission (which in this case is equal to full access). The second number, 6, represents the group permission (in this case read and write access). The final number, 0, represents the all users (or all *other* users) permission, which has no access. This is just an example; the numbers could be whatever you select for the three groups. You might see 777 when all groups have all permissions, though it is not normally recommended. It is common on a web server or file server to see 755, which means that the owner has all permissions, and the group and all users have read and execute permissions. You don't want a typical user to have write permissions on a web server! In summary, the `chmod` command is a great way to assign permissions to all three groups using a single command.

When working with permissions, the "least privilege" or "minimal privilege" concept should be implemented. Give the users only the amount of access that they absolutely need. Note that permissions for long-term employees could suffer from *privilege creep* over time. To mitigate this, consider periodic user permission reviews and evaluation of ACLs. This procedure will ensure that users have the access to the correct data. Also consider this procedure if a company has a particularly high attrition rate (hiring and terminating of employees). This will verify that users no longer with the company cannot log on to the network and cannot gain access to resources. It also ensures that new users can gain access to necessary resources.

Permission Inheritance and Propagation

If you create a folder, the default action it takes is to inherit permissions from the parent folder, which ultimately come from the root folder. So any permissions set in the parent are inherited by the subfolder. To view an example of this, locate any folder within an NTFS volume (besides the root folder), right-click it, and select Properties, access the Security tab, and click the Advanced button. Here, you see an enabled checkbox named Allow Inheritable Permissions from the Parent to Propagate... toward the bottom of the window, as shown in Figure 10-7. This means that any permissions added or removed in the parent folder will also be added or removed in the current folder. In addition, those permissions inherited cannot be modified in the current folder. To make modifications, you would have to deselect the Allow Inheritable Permissions from the Parent to Propagate... checkbox. When you do so, you have the option to copy the permissions from the parent to the current folder or remove them entirely. To summarize, by default the parent is automatically propagating permissions to the subfolder, and the subfolder is inheriting its permissions from the parent.

You can also propagate permission changes to subfolders not inheriting from the current folder. To do so, select the Replace Permission Entries on All Child Objects... checkbox. This might all seem a bit confusing, and you will probably not be asked many questions on the subject. Just remember that folders automatically inherit from the parent unless you turn off inheriting—and you can propagate permission entries to subfolders at any time by selecting the Replace option.

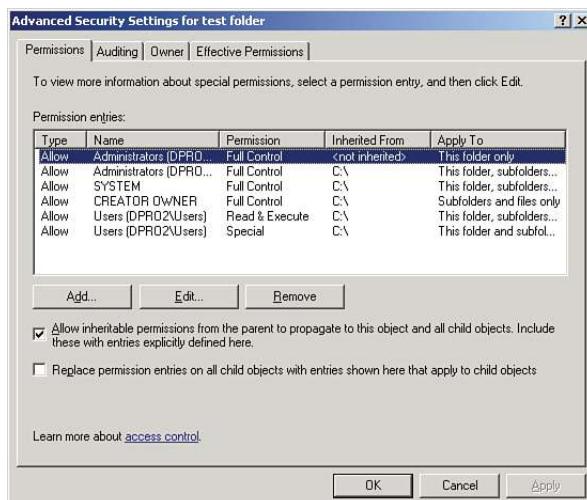


Figure 10-7 Inheritable Permissions

Moving and Copying Folders and Files

This subject and the previous one are actually more advanced Microsoft concepts, the type you would be asked on a Microsoft exam, and less likely to be asked on a CompTIA exam, so we'll try to keep this simple. Moving and copying folders have different results when it comes to permissions. Basically, it breaks down like this:

- If you *copy* a folder (or file) on the same volume or to a different volume, the folder inherits the permissions of the parent folder it was copied to (target directory).
- If you *move* a folder (or file) to a different location on the same volume, the folder retains its original permissions. (You cannot move a folder to a separate volume; if you attempt to do so it will automatically be copied to the other volume.)

NOTE Keep in mind that when you move data within a volume, the data isn't actually relocated; instead the pointer to the file or folder is modified. Accordingly, permissions are not really moved either, so they remain the same.

Usernames and Passwords

The most common type of authentication is the username/password combination. Usernames are usually based on a person's real name. Large organizations often use the `firstname.lastname` convention (for example, `david.prowse@company.com`) or first initial and last name (`dprowse@company.com`). Smaller organizations might use the first name and last initial. The naming convention decided upon should be easy for you to implement without name confusion, and it should have the capability to be utilized for all systems on the network, including login, e-mail, database, file access, and so on.

The password is either set by the user or created automatically for the user by an administrator. Figure 10-8 shows an example of a password created by the administrator. However, in this case, the user is not blocked from changing the password (unless a policy was created for that purpose). Note that the second checkbox, `User Cannot Change Password`, is not selected. As an administrator, you also have the option to select `User Must Change Password at Next Logon`. A user would have to pick a password when he first logs on to the domain, one that meets whatever complexity requirements your network calls for. This with the self-service password resetting (when users reset their own passwords at regular intervals) is necessary in larger networks to ease administration and increase security. The only caveat to this

is account lockouts. Unlocking accounts that were locked by the system should be done only by an administrator or system operator.



Figure 10-8 Password Phase of User Account Creation

At this point, it is common knowledge that a strong password is important for protecting a user account. Nowadays, many user accounts are compromised because of laziness; laziness on the part of the user for not configuring a strong password, or lethargic complacency on the part of the administrator for not enforcing the use of strong passwords.

But what is a strong password? That depends on the organization you deal with, but generally it is broken down into a few easy-to-remember points. Passwords should comply with the following:

- Contain uppercase letters
- Contain lowercase letters
- Contain numbers
- Contain special characters (symbols)
- Should be 8 to 10 characters or more. Some organizations that have extremely sensitive data will require 15 characters as a minimum.

Changing your password at regular intervals is important as well. The general rule of thumb is to change your password as often as you change your toothbrush. However, because this is a subjective concept (to put it nicely!), many organizations have policies concerning your password that we discuss in the next section. It might need to meet certain requirements, or be changed at regular intervals, and so forth.

Here are a few more tips when it comes to user accounts, passwords, and logons:

- **Rename and password protect the Administrator account:** It's nice that Windows has incorporated a separate Administrator account; the problem is that by default the account has no password. To configure this account, navigate to Computer Management > System Tools > Local Users and Groups > Users and locate the Administrator account. In a domain, this would be in ADUC > Domain name > Users. By right-clicking the account, you see a drop-down menu in which you can rename it and/or give it a password. (Just remember the new username and password!) Now it's great to have this additional Administrator account on the shelf just in case the primary account fails; however, some operating systems such as Vista disable the account by default. To enable it, right-click the account and select Properties. In the General tab, deselect the Account Is Disabled checkbox. Alternatively, open the command-line and type the following:

```
net user administrator /active:yes
```

The way that the Administrator account behaves by default depends on the version of Windows. The Linux/UNIX counterpart is the root account. The same types of measures should be employed when dealing with this account.

- **Verify that the Guest account (and other unnecessary accounts) is disabled:** This can be done by right-clicking the account in question, selecting Properties, and then selecting the checkbox named Account Is Disabled. It is also possible to delete accounts (aside from built-in accounts such as the Guest account); however, companies usually opt to have them disabled instead so that the company can retain information linking to the account. So, if an employee is terminated, the system administrator should generally implement the policy of account disablement. By disabling the account, the employee in question can no longer log in to the network, but the system administrator still has access to the history of that account.
- **Use Ctrl+Alt+Del:** Pressing Ctrl+Alt+Del before the logon adds a layer of security to the logon process. This can be added as a policy on individual Windows computers. It is implemented by default with computers that are members of a domain.
- **Use policies:** Policies governing user accounts, passwords, and so on can help you to enforce your rules, as discussed in the next section. Large organizations with a lot of users usually implement a self-service password management system. This means that users reset their own passwords after a given amount of time (set in a Group Policy); the administrator does not create passwords for users.

Policies

Policies are rules or guidelines used to guide decisions and achieve outcomes. They can be written or configured on a computer. The former are more difficult to enforce, whereas the latter would have to be hacked to be bypassed. Local computer policies and network policies are what really make an access control model effective.

Password policies can be implemented to enforce the usage of complex passwords and regulate how long passwords last. They can be configured on local computers, such as Windows operating systems, by navigating to Administrative Tools > Local Security Policy. When in the Local Security Settings window, continue to Security Settings > Account Policies > Password Policy.

More important, policies can be configured for an entire network, for example, on a Microsoft domain. The policy can affect the entire domain or individual organizational units. This would be known as a Group Policy and would be configured on a domain controller. For example, a Windows Server domain controller can be configured by completing the following steps:

Step 1. Access the domain controller.

Step 2. Create an MMC.

Step 3. Add the Default Domain Policy to the MMC. (Done by adding a Group Policy Object Editor snap-in.)

Step 4. In the Default Domain Policy, navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy.

NOTE The Default Domain Policy affects all users. This is okay for small networks, but for larger networks, separate organizational units should be created, each with its own security policy. From there, group-based privileges and individual user-based privileges can be expertly defined.

When Password Policy is selected, you see the following policies:

Key Topic

- **Enforce password history:** When this is defined, users cannot use any of the passwords remembered in the history. If you set the history to 3, the last three passwords cannot be reused when it is time to change the password.
- **Maximum and minimum password age:** This defines exactly how long a password can be used. The maximum is initially set to 42 days but does not affect the default Administrator account. To enforce effective password history,

the minimum must be higher than zero. This is part of a category known as password expiration.

- **Minimum password length:** This requires that the password must be at least the specified number of characters. For a strong password policy, set this to 8 or more (as long as other complex requirements are also set; if not, the password should be longer).
- **Password must meet complexity requirements:** This means that passwords must meet three of these four criteria: uppercase characters, lowercase characters, digits between 0 and 9, and non-alphabetic characters (special characters).

To effectively stop users from reusing the same password, a security administrator should combine the Enforce Password History policy with the Minimum Password Age policy. The Minimum Password Age setting must be less than the Maximum Password Age setting and must be more than zero to enforce a password history policy. In addition, the security administrator might need to create a policy that states that passwords cannot be changed more than once a day: This would prevent users from changing their passwords X number of times in an attempt to bypass that password history policy.

Remember that all these policies, when enabled, affect all users to which the policy applies. If it is the Default Domain Policy (usually not recommended for configuration), it affects all users; if it is an OU policy, it affects all users in the OU.

Complexity and Length of a Password

You might see equations that represent the complexity and length of a password, for example, 26^n . In this case the 26 refers to the letters in the alphabet: “a” through “z” (lowercase), which comes to 26 characters in total. If we also allowed uppercase letters, this number would be 52. If we added numbers, it would come to 62, and so on. But for now, let’s stick with 26^n as the example. The superscript n is a variable that refers to the length of the password. When calculating a password, the number of characters should be raised to a particular power equal to the length of the password. So, if our policy dictates a password that is ten characters long, then it would be 26 to the power of 10, or 26^{10} . This would come to 141 trillion combinations. In this case $n = 10$, but it doesn’t have to; n could be 12, 14, or whatever the security administrator sets the password length to within the password policy.

NOTE For more information on password policies and password best practices, see the following links:

<http://technet.microsoft.com/en-us/library/hh994572.aspx>

<http://technet.microsoft.com/en-us/library/cc784090.aspx>

There are plenty of other policies that you can configure. You can pretty much configure any policy on a domain. You can't configure how a person should shave in the morning, but anything computer-related can be modified and policed. One example is how many attempts a person will be allowed when typing in a password. This is known as the Account Lockout Threshold, as shown in Figure 10-9. Many companies adjust this to 3; this is known as the “3 strikes and you're out rule.”

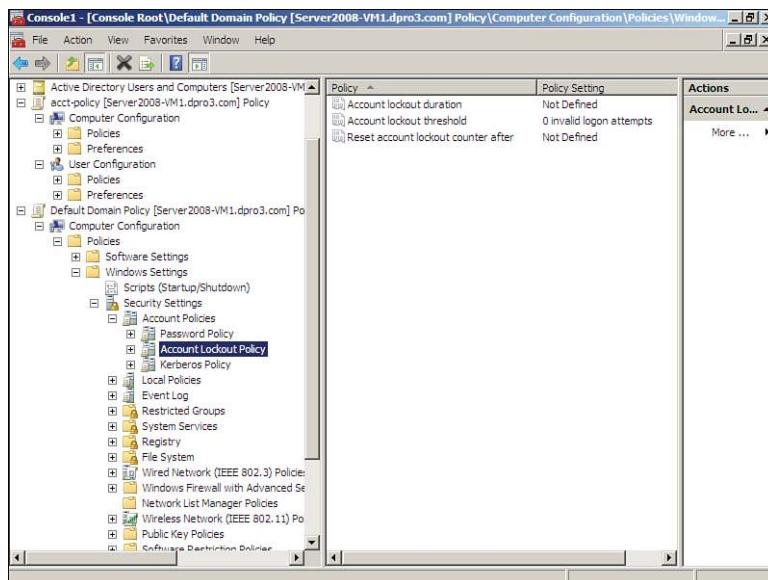


Figure 10-9 Account Lockout Threshold Policy

Another great tool is the previous logon notification. This can be configured in a policy and shows the user the last time the account logged in successfully—generally during the logon process. If users suspect that their account was compromised, they could check the previous logon notification and compare that with when they remember logging in.

It's important to note that when logging on to a Microsoft network, the logon process is secured by the Kerberos protocol, which is run by the domain controller.

This adds a layer of protection for the username and password as they are authenticated across the network. When users take a break or go to lunch, they should lock the computer. This can be done by pressing Windows+L. When doing so, the operating system goes into a locked state, and the only way to unlock the computer is to enter the username and password of the person who locked the computer. The difference between this and logging out is that a locked computer keeps all the session's applications and files open, whereas logging out closes all applications and open files. A policy can also be configured to force locking after a certain amount of time has elapsed. Literally hundreds of policies are configurable. You could spend weeks doing it! Microsoft understands this and offers various levels of security templates that can be imported into your OU policy, making your job as an administrator a bit easier. A particular template might be just what you are looking for, or it might need a bit of tweaking. But in most cases it beats starting from scratch!

Policies can be developed on all kinds of software and systems, not just operating systems. For example, many organizations have websites, and a good portion of those organizations now set up bulletin board systems where authorized users can post messages. Bulletin boards are also known as forums or portals. Bulletin boards are often the playground for malicious activity; for example, users or bots posting spam messages. Various policies can be implemented on an interactive bulletin board system to prevent these types of problems. For example, when people first register, they would need to answer a question that requires something they know such as $2+4 =$ blank. The user would enter the answer (6) and continue on their merry way. Another viable option is to use **CAPTCHA** (Completely Automated Public Turing test to tell Computers and Humans Apart), which can display an image that has letters and numbers in it. The user must type the letters and numbers that they see before they can register, or perhaps to post any messages at all. This is a good deterrent for bots!

User Account Control (UAC)

User Account Control (UAC) is a security component of Windows that keeps every user (besides the actual Administrator account) in standard user mode instead of as an administrator with full administrative rights—even if the person is a member of the administrators group. It is meant to prevent unauthorized access, as well as avoid user error in the form of accidental changes. With UAC enabled, users perform common tasks as non-administrators, and, when necessary, as administrators, without having to switch users, log off, or use Run As.

Basically, UAC was created with two goals in mind:

- To eliminate unnecessary requests for excessive administrative-level access to Windows resources

- To reduce the risk of malicious software using the administrator's access control to infect operating system files

When a standard end user requires administrator privileges to perform certain tasks such as installing an application, a small pop-up UAC window appears, notifying the user that an administrator credential is necessary. If the user has administrative rights and clicks Continue, the task is carried out, but if the user does not have sufficient rights, the attempt fails. Note that these pop-up UAC windows do not appear if the person is logged on with the actual Administrator account.

If necessary, UAC can be disabled in the Control Panel. If a change is made to UAC in Windows 7 and older, the system needs to be restarted.

There are other examples of generic account prohibition that work in the same manner as UAC. Third-party tools are available for Windows and Linux. An administrator might find that UAC does not have the configurability they desire. Regardless of the type of account prohibition used, it is important to conduct user access reviews—audits of what users have been able to access over time—and continuously monitor users' actions in this regard. We'll discuss this mindset in Chapter 12, "Monitoring and Auditing."

Chapter Summary

In order to have an efficient computer network, the security administrator needs to be *in control*. This is still feasible, even in today's complicated computer networks. An admin can choose from three basic access control models: discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC). Probably the most common is DAC; many Windows-controlled and Linux-controlled networks utilize this model. Whatever the model, remember that they are based on subjects (users) and objects (data files and other resources).

For access control to work well, it is wise to implement certain concepts such as: implicit deny, where all traffic is denied except for what a user specifically needs; least privilege, where a user is only given the permissions necessary to perform a task; separation of duties, where more than one person is required to complete a task; and job rotation, where a pool of people can work on the same individual job if necessary. Used together, an access control model can be very effective.

A lot of the concepts in the preceding two paragraphs are intangibles. To secure access to data in the technical sense, permissions and policies are your best friends. Both large and small networks can benefit from the use of permissions and groups of users: Using permissions enables a more secure system; using groups of users allows you to automate the distribution of permissions to multiple users at once.

Permissions are also known as rights, access modes, and, depending on the scenario, access control lists (ACLs). The common Windows system uses a set of six NTFS permissions spanning from the ability to read files only, all the way to having full control of those files. In Unix/Linux-based systems, three types of permissions—read, write, and execute—are assigned to users, groups, and owners by way of a three-digit number and the `chmod` command.

Access control also hinges on authentication, the most common form of which is the username/password combination. The importance of complex passwords cannot be stressed enough. An organization will often require eight to ten characters minimum, including uppercase letters, numbers, and special characters. And all of this is usually enforced by a computerized policy. Password policies such as password history, maximum password age, minimum password length, and password complexity requirements, if configured properly, can offer your users a decent level of protection. The user accounts themselves can also be secured with the use of account lockouts, time-of-day restrictions, and User Account Control.

We mentioned in the beginning of the chapter that you don't want any Tom, Dick, or Harry to get access to your data. If you don't control access to your data, it is the equivalent of allowing the three stooges into your servers. You'd be surprised how many companies disregard best practices for access control. But when it comes to this layer of security, a little bit of planning and a modest piece of automated configuration can go a long way.

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 10-2 lists a reference of these key topics and the page number on which each is found.

Table 10-2 Key Topics for Chapter 10

Key Topic Element	Description	Page Number
Figure 10-1	Example of discretionary access in Windows	385
Table 10-1	Summary of access control models	388
Figure 10-2	Example of implicit deny on a Windows folder	389

Key Topic Element	Description	Page Number
Figure 10-4	User account expiration date	392
Figure 10-5	Time-of-day restrictions for a standard user	393
Bulleted list	Password compliance	400

Define Key Terms

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

access control model, discretionary access control (DAC), Trusted Computer System Evaluation Criteria (TCSEC), mandatory access control (MAC), role-based access control (RBAC), implicit deny, least privilege, separation of duties, job rotation, access control list (ACL), permissions, CAPTCHA

Review Questions

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

1. Which of the following is the strongest password?
 - A. locrian#
 - B. Marqu1sD3S0d
 - C. This1sV#ryS3cure
 - D. Thisisverysecure

2. Which of these is a security component of Windows?
 - A. UAC
 - B. UPS
 - C. Gadgets
 - D. Control Panel

3. What key combination helps to secure the logon process?
 - A. Windows+R
 - B. Ctrl+Shift+Esc
 - C. Ctrl+Alt+Del
 - D. Alt+F4

4. Which of the following is the most common authentication model?
 - A. Username and password
 - B. Biometrics
 - C. Key cards
 - D. Tokens
5. Which of the following access control methods uses rules to govern whether object access will be allowed? (Select the best answer.)
 - A. Rule-based access control
 - B. Role-based access control
 - C. Discretionary access control
 - D. Mandatory access control
6. When using the mandatory access control model, what component is needed?
 - A. Labels
 - B. Certificates
 - C. Tokens
 - D. RBAC
7. Which of the following statements regarding the MAC model is true?
 - A. Mandatory access control is a dynamic model.
 - B. Mandatory access control enables an owner to establish access privileges to a resource.
 - C. Mandatory access control is not restrictive.
 - D. Mandatory access control users cannot share resources dynamically.
8. In the DAC model, how are permissions identified?
 - A. Role membership.
 - B. Access control lists.
 - C. They are predefined.
 - D. It is automatic.
9. Robert needs to access a resource. In the DAC model, what is used to identify him or other users?
 - A. Roles
 - B. ACLs

C. MAC

D. Rules

- 10.** A company has a high attrition rate. What should you ask the network administrator to do first? (Select the best answer.)
 - A.** Review user permissions and access control lists.
 - B.** Review group policies.
 - C.** Review Performance logs.
 - D.** Review the Application log.
- 11.** Your company has 1000 users. Which of the following password management systems will work best for your company?
 - A.** Multiple access methods
 - B.** Synchronize passwords
 - C.** Historical passwords
 - D.** Self-service password resetting
- 12.** In a discretionary access control model, who is in charge of setting permissions to a resource?
 - A.** The owner of the resource
 - B.** The administrator
 - C.** Any user of the computer
 - D.** The administrator and the owner
- 13.** Jason needs to add several users to a group. Which of the following will help him to get the job done faster?
 - A.** Propagation
 - B.** Inheritance
 - C.** Template
 - D.** Access control lists
- 14.** How are permissions defined in the mandatory access control model?
 - A.** Access control lists
 - B.** User roles
 - C.** Defined by the user
 - D.** Predefined access privileges

- 15.** Which of the following would lower the level of password security?
- A.** After a set number of failed attempts, the server will lock the user out, forcing her to call the administrator to re-enable her account.
 - B.** Passwords must be greater than eight characters and contain at least one special character.
 - C.** All passwords are set to expire after 30 days.
 - D.** Complex passwords that users cannot change are randomly generated by the administrator.
- 16.** Of the following access control models, which uses object labels? (Select the best answer.)
- A.** Discretionary access control
 - B.** Role-based access control
 - C.** Rule-based access control
 - D.** Mandatory access control
- 17.** Which of the following methods could identify when an unauthorized access has occurred?
- A.** Two-factor authentication
 - B.** Session termination
 - C.** Previous logon notification
 - D.** Session lock
- 18.** What would you use to control the traffic that is allowed in or out of a network? (Select the best answer.)
- A.** Access control lists
 - B.** Firewall
 - C.** Address Resolution Protocol
 - D.** Discretionary access control
- 19.** In an attempt to detect fraud and defend against it, your company cross-trains people in each department. What is this an example of?
- A.** Separation of duties
 - B.** Chain of custody
 - C.** Job rotation
 - D.** Least privilege

- 20.** What is a definition of implicit deny?
- A.** Everything is denied by default.
 - B.** All traffic from one network to another is denied.
 - C.** ACLs are used to secure the firewall.
 - D.** Resources that are not given access are denied by default.
- 21.** In an environment where administrators, the accounting department, and the marketing department all have different levels of access, which of the following access control models is being used?
- A.** Role-based access control (RBAC)
 - B.** Mandatory access control (MAC)
 - C.** Discretionary access control (DAC)
 - D.** Rule-based access control (RBAC)
- 22.** Which security measure should be included when implementing access control?
- A.** Disabling SSID broadcast
 - B.** Time-of-day restrictions
 - C.** Changing default passwords
 - D.** Password complexity requirements
- 23.** Which password management system best provides for a system with a large number of users?
- A.** Locally saved passwords management system
 - B.** Synchronized passwords management system
 - C.** Multiple access methods management system
 - D.** Self-service password reset management system
- 24.** You administer a bulletin board system for a rock and roll band. While reviewing logs for the board, you see one particular IP address posting spam multiple times per day. What is the best way to prevent this type of problem?
- A.** Block the IP address of the user.
 - B.** Ban the user.
 - C.** Disable ActiveX.
 - D.** Implement CAPTCHA.

- 25.** Your organization has enacted a policy where employees are required to create passwords with at least 15 characters. What type of policy does this define?
- A.** Password length
 - B.** Password expiration
 - C.** Minimum password age
 - D.** Password complexity
- 26.** Users are required to change their passwords every 30 days. Which policy should be configured?
- A.** Password length
 - B.** Password recovery
 - C.** Password expiration
 - D.** Account lockout
- 27.** You want to mitigate the possibility of privilege creep among your long-term users. What procedure should you employ?
- A.** Mandatory vacations
 - B.** Job rotation
 - C.** User permission reviews
 - D.** Separation of duties
- 28.** A security administrator implements access controls based on the security classification of the data and need-to-know information. Which of the following would best describe this level of access control?
- A.** Least privilege
 - B.** Mandatory access control
 - C.** Role-based access control
 - D.** Implicit deny
- 29.** Which of the following access control models would be found in a firewall?
- A.** Mandatory access control
 - B.** Discretionary access control
 - C.** Role-based access control
 - D.** Rule-based access control

- 30.** You are consulting for a small organization that relies on employees who work from home and on the road. A hacker has compromised the network by denying remote access to the company using a script. Which of the following security controls did the hacker exploit?
- A.** Password complexity
 - B.** DoS
 - C.** Account lockout
 - D.** Password length

Answers and Explanations

- 1. C.** The answer This1sV#ryS3cure incorporates case-sensitive letters, numbers, and special characters and is 16 characters long. The other answers do not have the complexity of This1sV#ryS3cure.
- 2. A.** User Account Control (UAC) adds a layer of security to Windows that protects against malware and user error and conserves resources. It enforces a type of separation of duties.
- 3. C.** Ctrl+Alt+Del is the key combination used to help secure the logon process. It can be added by configuring the Local Security policy.
- 4. A.** By far the username and password combination is the most common authentication model. Although biometrics, key cards, and tokens are also used, the username/password is still the most common.
- 5. A.** Rule-based access control uses rules to govern whether an object can be accessed. It is a type of mandatory access control.
- 6. A.** Labels are required in the mandatory access control (MAC) model.
- 7. D.** In the MAC (mandatory access control) model, users cannot share resources dynamically. MAC is not a dynamic model; it is a static model. Owners cannot establish access privileges to a resource; this would be done by the administrator. MAC is indeed very restrictive, as restrictive as the administrator wants it to be.
- 8. B.** In the discretionary access control model, permissions to files are identified by access control lists (ACLs). Role membership is used in RBAC. The mandatory access control model predefines permissions. Either way, it is not identified automatically.
- 9. B.** Access control lists (ACLs) are used in the discretionary access control model. This is different from role-based, rule-based, and MAC (mandatory access control) models.

10. **A.** The first thing administrators should do when they notice that the company has a high attrition rate (high turnover of employees) is to conduct a thorough review of user permissions, rights, and access control lists. A review of group policies might also be necessary but is not as imperative. Performance logs and the Application log will probably not pertain to the fact that the company has a lot of employees being hired and leaving the company.
11. **D.** It would be difficult for administrators to deal with thousands of users' passwords; therefore, the best management system for a company with 1000 users would be self-service password resetting.
12. **A.** In the discretionary access control (DAC) model, the owner of the resource is in charge of setting permissions. In a mandatory access control model, the administrator is in charge.
13. **C.** By using a template, you can add many users to a group at once simply by applying the template to the users. Propagation and inheritance deal with how permissions are exchanged between parent folders and subfolders. Access control lists show who was allowed access to a particular resource.
14. **D.** The mandatory access control model uses predefined access privileges to define which users have permission to resources.
15. **D.** To have a secure password scheme, passwords should be changed by the user. They should not be generated by the administrator. If an administrator were to generate the password for the user, it would have to be submitted in written (and unencrypted) form in some way to the user. This creates a security issue, especially if the user does not memorize the password and instead leaves a written version of it lying around. All the other answers would increase the level of password security.
16. **D.** The mandatory access control (MAC) model uses object and subject labels. DAC and RBAC (role-based access control) do not. Rule-based access control is a portion of MAC, and although it might use labels, MAC is the best answer.
17. **C.** Previous logon notification can identify whether unauthorized access has occurred. Two-factor authentication means that person will supply two forms of identification before being authenticated to a network or system. Session termination is a mechanism that can be implemented to end an unauthorized access. Session lock mechanisms can be employed to lock a particular user or IP address out of the system.
18. **A.** Access control lists can be used to control the traffic that is allowed in or out of a network. They are usually included as part of a firewall, and they are the better answer because they specifically will control the traffic. Address

Resolution Protocol (ARP) resolves IP addresses to MAC addresses. In the discretionary access control model, the owner controls permissions of resources.

19. **C.** When a company cross-trains people, it is known as job rotation. Separation of duties is in a way the opposite; this is when multiple people are needed to complete a single task. Chain of custody has to do with the legal paper trail of a particular occurrence. Least privilege is a mitigation technique to defend against privilege escalation attacks.
20. **D.** If a resource is not given specific access, it will be implicitly denied by default. Access control lists are used to permit or deny access from one network to another and are often implemented on a firewall.
21. **A.** Role-based access control is when different groups or roles are assigned different levels of permissions; rights and permissions are based on job function. In the mandatory access control model, an administrator centrally controls permissions. In the discretionary access control model, the owner of the user sets permissions. In the rule-based access control model, rules are defined by the administrator and are stored in an ACL.
22. **D.** By implementing password complexity requirements, users will be forced to select and enter complex passwords—for example, eight characters or more, uppercase characters, special characters, and more. Disabling the SSID deals with wireless networks, time-of-day restrictions are applied only after persons log in with their username and password, and changing default passwords should be part of a password policy.
23. **D.** If a network has a large number of users, the administrator should set up a system, and policies to enforce the system, that will allow for users to reset their own passwords. The passwords should be stored centrally, not locally. Also, it would be best if single sign-on were implemented and not a multiple access method.
24. **D.** By implementing **CAPTCHA**, another level of security is added that users have to complete before they can register to and/or post to a bulletin board. Although banning a user or the user's IP address can help to eliminate that particular person from spamming the site, the best way is to add another level of security, such as **CAPTCHA**. This applies to all persons who attempt to attack the bulletin board.
25. **A.** Password length is the policy that deals with how many characters are in a password. Password expiration and minimum (and maximum) password age define how long a password will be valid. Password complexity defines whether the password should have uppercase letters, numbers, and special characters.

26. **C.** The password expiration policy should be configured. For example, in Windows, the maximum password age policy should be set to 30 days. Password length deals with how many characters are in the password. Password recovery defines how (and if) a user can get back his password or create a new one. Account lockout policies dictate how many times the user has to type a password incorrectly to be locked out of the system, and for how long the user will remain locked out.
27. **C.** Conduct user permission reviews to ensure that long-term users are getting the proper permissions to data. Privilege creep is when, over time, additional permissions are given to a particular user because that user needs to access certain files on a temporary basis. Mandatory vacations are enforced on many personnel to ensure that there is no kind of fraud or other illegitimate activity going on. Job rotation is implemented so that multiple people can perform the same job, in the case that one person is not available. Separation of duties is when a group of users will each perform an individual task, which collectively forms the entire job.
28. **B.** When you are dealing with access controls based on the classification of data and need-to-know information, you are most likely working with a mandatory access control (MAC) system. Least privilege means the lowest amount of permissions possible. This differs from need-to-know in that a user configured as need-to-know might need to have access to a lot of data, and actually require a good deal of permissions. Role-based access control (RBAC), like MAC, is controlled by the system, but it works with sets of permissions based on user roles. Implicit deny means that unless otherwise configured, all access to data is denied.
29. **D.** Firewalls are most often considered to be based off of the rule-based access control model. This is because you indeed create rules (ACLs) that govern how data is transmitted through the firewall.
30. **C.** The hacker most likely exploited the account lockout policy, a security control originally implemented by the organization. The script modified the policy and caused all of the users to be locked out when they attempted to log in. Password complexity is the level of intricacy of a password; it usually entails using uppercase letters, numerals, and special characters, and is defined by a policy, just as the account lockout threshold is. DoS stands for denial-of-service, an attack that floods a network device (or server) with so much data that the device cannot perform its duties. Password length is the number of characters in a password, also definable by policy.

Case Studies for Chapter 10

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

Case Study 10-1: Configuring Complex Passwords

Scenario: You are not only the security administrator for your organization, but also the IT trainer! Teach your users how to set passwords in Windows, Linux, and OS X. But more importantly, show them how to check if their passwords are complex enough to meet today's standards. Finally, show the junior network admins how to enforce complex passwords.

In Table 10-3, describe the following:

- How you would set passwords in Windows, Linux, and OS X
- How to check the complexity of passwords online
- What method should be used to enforce complex passwords

Table 10-3 Configuring Complex Passwords

Task	Your Solution
Configure Windows password	
Configure Linux password	
Configure OS X password	
Identify where to check complexity of passwords online	
Choose method to enforce complex passwords	

Case Study 10-2: Configuring Password Policies and User Account Restrictions

Scenario: As the network security administrator of a company with 5000 users, you are required to enforce complex passwords, and make sure that user access to the network is restricted to specific times. More importantly, you *must* employ a certain level of automation. Let's face it, even the fastest computer operator wouldn't be able to keep up with all of the password requests and timeframe configurations for

users on an individual basis. Your organization has a Windows domain with three domain controllers.

In your own words, describe how you would enforce complex passwords and user account restrictions. Explain how you would automate the process, utilize templates, and work with organizational units.

Case Study 10-3: Understanding Access Control Models

Access control can deal with a lot of different things, but in technology what we are most concerned with is the access to data and how it is controlled.

Use the Internet to research the three main types of access control, and in Table 10-4 give a description of each and an example of technology environments for each.

Table 10-4 Access Control Models

Access Control Model	Description	Example
DAC		
MAC		
RBAC		

Case Study 10-4: Configuring User and Group Permissions

Scenario: You are required to configure permissions for users on your network. To simplify the process, also create user groups that will allow you to group the users together (most likely by the department of your organization) and apply permissions to multiple users within the group at one time.

Using this book and the Internet, research how you would apply permissions to users, and how you can create groups on a Windows computer.

Case Study Solutions

Case Study 10-1 Solution

Training users is one of the best ways to increase the security of your IT environment. It can be difficult to keep some users' attention, so you have to make it interesting. Appeal to their curiosity, and have the users practice, practice, practice to make things stick. Remember that users are not techies (usually), and might learn in a different way and at a different pace.

Remember too that users might work with Windows, Linux, OS X, iOS, Android, or other operating systems, each with its own way of configuring passwords and passcodes. Also keep in mind that there are many ways to accomplish something in Windows and other operating systems. Table 10-5 gives a few examples.

Table 10-5 Configuring Complex Passwords Solution

Task	Possible Solution
Windows password configuration	Press Ctrl+Alt+Del and select Change Password. Change the password in Control Panel > User Accounts.
Linux password configuration	Open Terminal, then type passwd.
OS X password configuration	Open Terminal, then type passwd. Change the password in System Preferences > Users & Groups.
Where to check complexity of passwords	Use online password checkers such as the Microsoft Password Checker or The Password Meter.
What method should you use to enforce complex passwords	Implement well-written password policies to enforce the use of complex passwords.

Video Solution: Watch the video solution “10-1: Configuring Complex Passwords” on the accompanying disc.

Simulation: Complete the simulation “10-1: Password Strength.”

Case Study 10-2 Solution

A network security administrator will have far too much work to do to have to worry about individual password requests, or to deal with configuring users one at a time.

So, the smart admin will utilize password policies that are based on individual organizational units (OUs) in Windows or other similar grouping structures in other operating systems. These policies will default to a self-reset mode, where the users change the passwords themselves, when prompted by the system. And the policy will make sure that the user meets the complexity requirements.

User account restrictions can be configured through policies and also by creating a basic user template, from which other user accounts are based off of, effectively copying any restrictions from the template to the new user.

By automating as much as possible, the admin reduces the amount of time required on basic configurations, and can spend more time researching the latest CVEs and installing their updates.

Video Solution: Watch the video solution “10-2: Configuring Password Policies and User Account Restriction” on the accompanying disc.

Simulation: Complete the simulation “10-2: Configuring Logon Hours.”

Case Study 10-3 Solution

There is some overlap when it comes to access control models. That is partially true because the functional definitions of the various access models have changed over time, and the software that uses them has changed over time as well. For example, you might see that FreeBSD is considered to be either MAC-based or RBAC-based depending on its implementation.

Table 10-6 gives sample descriptions and examples of the three main access control models.

Table 10-6 Access Control Models—Solution

Access Control Model	Description	Examples
DAC	Access control policy generally determined by the owner. Objects such as files and printers can be created and accessed by the owner.	Windows domains Linux Red Hat networks
MAC	Access control policy determined by a computer system, not by a user or owner. Defines sensitivity labels that are assigned to <i>subjects</i> (users) and <i>objects</i> (files and folders).	Military Government SELinux Multilevel secure (MLS) systems; for example, NSA, Boeing, Honeywell, and so on
RBAC	Controlled by the system, but works with sets of permissions known as roles.	Solaris SAP Active Directory (server roles)

Simulation: Complete the simulation “10-3: Understanding Access Control Models.”

Case Study 10-4 Solution

One great resource on the Internet for details about configuring permissions is Microsoft TechNet (<http://technet.microsoft.com>). It has all kinds of step-by-step instructions that show you how to do just about anything in Windows operating systems. Case in point: working with users and groups, whether on a Windows client or server. Practice working with users and groups and watch the video on this subject on the disc.

Video Solution: Watch the video solution “10-4: Configuring User and Group Permissions” on the accompanying disc.

This page intentionally left blank



This chapter covers the following subjects:

- **Conducting Risk Assessments:** This section covers risk management and assessment. It discusses the differences between qualitative and quantitative risk and describes the methodologies of an important part of risk management—vulnerability management. Also covered are various ways to assess vulnerabilities and how to perform penetration tests.
- **Assessing Vulnerability with Security Tools:** In this section, you learn how to use common network security tools to measure the vulnerability of your computer systems and network devices. These tools include network mappers, vulnerability scanners, protocol analyzers, packet sniffers, and password crackers.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 2.1, 2.2, 2.7, 3.2, 3.7, 3.8, and 4.5.

Vulnerability and Risk Assessment

Let's take it to the next level and talk some serious security. As people, we're all vulnerable to something. They say that you need to "manage your own health-care"—our computers are no different. The potential health of your computers and network is based on vulnerabilities. One of the most important tasks of a security administrator is to find vulnerabilities and either remove them or secure them as much as possible—within acceptable parameters. **Vulnerabilities** are weaknesses in your computer network design and individual host configuration. Vulnerabilities, such as open ports, unnecessary services, weak passwords, systems that aren't updated, lack of policy, and so on, are invitations to threats such as malicious attacks. Of course, your computer network can be vulnerable to other types of threats as well, such as environmental or natural threats, but these are covered in more depth in Chapter 15, "Redundancy and Disaster Recovery," and Chapter 16, "Policies, Procedures, and People."

Vulnerability assessment is just part of overall risk management. Risk includes computer vulnerabilities, potential dangers, possible hardware and software failure, man hours wasted, and of course, monetary loss. Having a computer network is inherently a risky business, so we need to conduct risk assessments to define what an organization's risks are and how to reduce those risks.

Foundation Topics

Conducting Risk Assessments

When dealing with computer security, a **risk** is the possibility of a malicious attack or other threat causing damage or downtime to a computer system. Generally, this is done by exploiting vulnerabilities in a computer system or network. The more vulnerability—the more risk. Smart organizations are extremely interested in managing vulnerabilities, and thereby managing risk. **Risk management** can be defined as the identification, assessment, and prioritization of risks, and the mitigating and monitoring of those risks. Specifically, when talking about computer hardware and software, risk management is also known as **information assurance (IA)**. The two common models of IA include the

well-known CIA triad (which we covered in Chapter 1, “Introduction to Security”), and the DoD “Five Pillars of IA,” which comprise the concepts of the CIA triad (confidentiality, integrity, and availability) but also include authentication and non-repudiation.

Organizations usually employ one of the four following general strategies when managing a particular risk:

- Transfer the risk to another organization or third party.
- Avoid the risk.
- Reduce the risk.
- Accept some or all of the consequences of a risk.

It is possible to transfer *some* risk to a third party. An example of **risk transference** (also known as risk sharing) would be an organization that purchases insurance for a group of servers in a data center. The organization still takes on the risk of losing data in the case of server failure, theft, and disaster, but transfers the risk of losing the money those servers are worth in case they are lost.

Some organizations opt to avoid risk. **Risk avoidance** usually entails not carrying out a proposed plan because the risk factor is too great. An example of risk avoidance: If a high-profile organization decided not to implement a new and controversial website based on its belief that too many attackers would attempt to exploit it.

However, the most common goal of risk management is to *reduce* all risk to a level acceptable to the organization. It is impossible to eliminate all risk, but it should be mitigated as much as possible within reason. Usually, budgeting and IT resources dictate the level of **risk reduction**, and what kind of deterrents can be put in place. For example, installing antivirus/firewall software on every client computer is common; most companies do this. However, installing a high-end, hardware-based firewall at every computer is not common; although this method would probably make for a secure network, the amount of money and administration needed to implement that solution would make it unacceptable.

This leads to **risk acceptance**, also known as risk retention. Most organizations are willing to accept a certain amount of risk. Sometimes, vulnerabilities that would otherwise be mitigated by the implementation of expensive solutions are instead dealt with when and if they are exploited. IT budgeting and resource management are big factors when it comes to these risk management decisions.

After the risk transference, risk avoidance, and risk reduction techniques have been implemented, an organization is left with a certain amount of **residual risk**—the risk left over after a detailed security plan and disaster recovery plan have been implemented. There is always risk, as a company cannot possibly foresee every future

event, nor can it secure against every single threat. Senior management as a collective whole is ultimately responsible for deciding how much residual risk there will be in a company's infrastructure, and how much risk there will be to the company's data. Often, no one person will be in charge of this, but it will be decided on as a group.

There are many different types of risks to computers and computer networks. Of course, before you can decide what to do about a particular risk, you need to assess what those risks are.

Risk assessment is the attempt to determine the amount of threats or hazards that could possibly occur in a given amount of time to your computers and networks. When you assess risks, they are often recognized threats—but risk assessment can also take into account new types of threats that might occur. When risk has been assessed, it can be mitigated up until the point in which the organization will accept any additional risk. Generally, risk assessments follow a particular order, for example:

- Step 1.** Identify the organization's assets.
- Step 2.** Identify vulnerabilities.
- Step 3.** Identify threats and threat likelihood.
- Step 4.** Identify potential monetary impact.

The fourth step is also known as *impact assessment*. This is when you determine the potential monetary costs related to a threat. See the section “Vulnerability Management” later in this chapter for more on information on Steps 2 and 3, including how to mitigate potential threats.

The two most common risk assessment methods are qualitative and quantitative. Let's discuss these now.

Qualitative Risk Assessment

Qualitative risk assessment is an assessment that assigns numeric values to the probability of a risk and the impact it can have on the system or network. Unlike its counterpart, quantitative risk assessment, it does not assign monetary values to assets or possible losses. It is the easier, quicker, and cheaper way to assess risk but cannot assign asset value or give a total for possible monetary loss.

With this method, ranges can be assigned, for example, 1 to 10 or 1 to 100. The higher the number, the higher the probability of risk, or the greater the impact on the system. As a basic example, a computer without antivirus software that is connected to the Internet will most likely have a high probability of risk; it will also

most likely have a great impact on the system. We could assign the number 99 as the probability of risk. We are not sure exactly when it will happen but are 99% sure that it will happen at some point. Next, we could assign the number 90 out of 100 as the impact of the risk. This number implies a heavy impact; probably either the system has crashed or has been rendered unusable at some point. There is a 10% chance that the system will remain usable, but it is unlikely. Finally, we multiply the two numbers together to find out the qualitative risk: $99 \times 90 = 8910$. That's 8910 out of a possible 10,000, which is a high level of risk. **Risk mitigation** is when a risk is reduced or eliminated altogether. The way to mitigate risk in this example would be to install antivirus software and verify that it is configured to auto-update. By assigning these types of qualitative values to various risks, we can make comparisons from one risk to another and get a better idea of what needs to be mitigated and what doesn't.

The main issue with this type of risk assessment is that it is difficult to place an exact value on many types of risks. The type of qualitative system varies from organization to organization, even from person to person; it is a common source of debate as well. This makes qualitative risk assessments more descriptive than truly measurable. However, by relying on group surveys, company history, and personal experience, you can get a basic idea of the risk involved.

Quantitative Risk Assessment

Quantitative risk assessment measures risk by using exact monetary values. It attempts to give an expected yearly loss in dollars for any given risk. It also defines asset values to servers, routers, and other network equipment.

Three values are used when making quantitative risk calculations:

- **Single loss expectancy (SLE):** The loss of value in dollars based on a single incident.
- **Annualized rate of occurrence (ARO):** The number of times per year that the specific incident occurs.
- **Annualized loss expectancy (ALE):** The total loss in dollars per year due to a specific incident. The incident might happen once or more than once; either way, this number is the total loss in dollars for that particular type of incident. It is computed with the following calculation:

$$\text{SLE} \times \text{ARO} = \text{ALE}$$

So, for example, suppose we wanted to find out how much an e-commerce web server's downtime would cost the company per year. We would need some additional information such as the average web server downtime in minutes and the

amount of times this occurs per year. We also would need to know the average sale amount in dollars and how many sales are made per minute on this e-commerce web server. This information can be deduced by using accounting reports and by further security analysis of the web server, which we discuss later. For now, let's just say that over the past year our web server failed 7 times. The average downtime for each failure was 45 minutes. That equals a total of 315 minutes of downtime per year, close to 99.9% uptime. (The more years we can measure, the better our estimate will be.) Now let's say that this web server processes an average of 10 orders per minute with average revenue of \$35. That means that \$350 of revenue comes in per minute. As we mentioned, a single downtime averages 45 minutes, corresponding to a \$15,750 loss per occurrence. So, the SLE is \$15,750. Ouch! Some salespeople are going to be unhappy with your 99.9% uptime! But we're not done. We want to know the annualized loss expectancy (ALE). This can be calculated by multiplying the SLE (\$15,750) by the annualized rate of occurrence (ARO). We said that the web server failed 7 times last year, so the $SLE \times ARO$ would be $\$15,750 \times 7$, which equals \$110,250 (the ALE). This is shown in Table 11-1.

Table 11-1 Example of Quantitative Risk Assessment

Key Topic

SLE	ARO	ALE
\$15,750	7	\$110,250
Revenue lost due to each web server failure	Total web server failures over the past year	Total loss due to web server failure per year

Whoa! Apparently, we need to increase the uptime of our e-commerce web server! Many organizations demand 99.99% or even 99.999% uptime; 99.999% uptime means that the server will only have 5 minutes of downtime over the entire course of the year. Of course, to accomplish this we first need to scrutinize our server to see precisely why it fails so often. What exactly are the vulnerabilities of the web server? Which ones were exploited? Which threats exploited those vulnerabilities? By exploring the server's logs, configurations, and policies, and by using security tools, we can discern exactly why this happens so often. However, this analysis should be done carefully because the server does so much business for the company. We continue this example and show the specific tools you can use in the section "Assessing Vulnerability with Security Tools."

It isn't possible to assign a specific ALE to incidents that will happen in the future, so new technologies should be monitored carefully. Any failures should be documented thoroughly. For example, a spreadsheet could be maintained that contains the various technologies your organization uses, their failure history, their SLE, ARO, and ALE, and mitigation techniques that you have employed, and when they were implemented.

Although it's impossible to predict the future accurately, it can be quantified on an average basis using concepts such as **mean time between failures (MTBF)**. This term deals with reliability. It defines the average number of failures per million hours of operation for a product in question. This is based on historical baselines among various customers that use the product. It can be very helpful when making quantitative assessments.

NOTE Another way of describing MTBF is called failure in time (FIT), which is the number of failures per *billion* hours of operation.

There are two other terms you should know that are related to MTBF: mean time to repair (MTTR), which is the time needed to repair a failed device; and mean time to failure (MTTF), which is a basic measure of reliability for devices that cannot be repaired. All three of these concepts should also be considered when creating a disaster recovery (DR) plan, which we will discuss more in Chapter 15.

So, we can't specifically foretell the future, but by using qualitative and quantitative risk assessment methods we can get a feel for what is likely to happen (more so with the latter option), and prepare accordingly. Table 11-2 summarizes the risk assessment types discussed in this chapter.

Key Topic

Table 11-2 Summary of Risk Assessment Types

Risk Assessment Type	Description	Key Points
Qualitative risk assessment	Assigns numeric values to the probability of a risk, and the impact it can have on the system or network.	Numbers are arbitrary. Examples: 1–10 or 1–100.
Quantitative risk assessment	Measures risk by using exact monetary values. It attempts to give an expected yearly loss in dollars for any given risk.	Values are specific monetary amounts. $SLE \times ARO = ALE$ MTBF can be used for additional data.

NOTE Most organizations within the medical, pharmaceutical, and banking industries make use of quantitative risk assessments—they need to have specific monetary numbers to measure risk. Taking this one step further, many banking institutions adhere to the recommendations within the Basel I, II, and III accords. These recommended standards describe how much capital a bank should put aside to aid with financial and operational risks if they occur.

Security Analysis Methodologies

To assess risk properly, we must analyze the security of our computers, servers, and network devices. But before making an analysis, the computer, server, or other device should be backed up accordingly. This might require a backup of files, a complete image backup, or a backup of firmware. It all depends on the device in question. When this is done, an analysis can be made. Hosts should be analyzed to discern whether a firewall is in place, what type of configuration is used (or worse if the device is using a default configuration), what anti-malware software is installed, if any, and what updates have been made. A list of vulnerabilities should be developed, and a security person should watch for threats that could exploit these vulnerabilities; they might occur naturally, might be perpetuated by malicious persons using a variety of attack and threat vectors, or might be due to user error.

Security analysis can be done in one of two ways: actively or passively.

Active security analysis is when actual hands-on tests are run on the system in question. These tests might require a device to be taken off the network for a short time, or might cause a loss in productivity. Active scanning is used to find out if ports are open on a specific device, or to find out what IP addresses are in use on the network. A backup of the systems to be analyzed should be accomplished before the scan takes place. Active scanning (also known as intrusive scanning) can be detrimental to systems or the entire network, especially if you are dealing with a mission-critical network that requires close to 100% uptime. In some cases, you can pull systems off the network or run your test during off-hours. But in other cases you must rely on passive security analysis.

Passive security analysis is when servers, devices, and networks are not affected by your analyses, scans, and other tests. It could be as simple as using documentation only to test the security of a system. For example, if an organization's network documentation shows computers, switches, servers, and routers, but no firewall, you have found a vulnerability to the network (a rather large one). Passive security analysis might be required in real-time, mission-critical networks or if you are conducting computer forensics analysis, but even if you are performing a passive security

analysis, a backup of the system is normal procedure. Passive security analysis is also known as non-intrusive or non-invasive analysis.

One example of the difference between active and passive is fingerprinting, which is when a security person (or hacker) scans hosts to find out what ports are open, ultimately helping the person to distinguish the operating system used by the computer. It is also known as OS fingerprinting or TCP/IP fingerprinting. Active fingerprinting is when a direct connection is made to the computer starting with ICMP requests. This type of test could cause the system to respond slowly to other requests from legitimate computers. Passive fingerprinting is when the scanning host sniffs the network by chance, classifying hosts as the scanning host observes its traffic on the occasion that it occurs. This method is less common in port scanners but can help to reduce stress on the system being scanned.

Security Controls

Before we get into managing vulnerabilities, I'd like to revisit the concept of security controls. In Chapter 1 we discussed three basic security controls that are often used to develop a security plan: physical, technical, and administrative. However, in the CompTIA 2.1 objective, we see the technical, management, and operational controls. This is another way to divide up the security plan for your organization's information security, and was devised by the National Institute of Standards and Technology (NIST). Collectively these controls are referred to by the (NIST) as *compensating* security control. The link to the entire document detailing these three categories of controls can be found in the "View Recommended Resources" PDF on the disc that accompanies this book. But in short, the three can be described as the following:

Key Topic

- **Management controls:** These are techniques and concerns addressed by an organization's management (managers and executives). Generally, these controls focus on decisions and the management of risk. They also concentrate on procedures, policies, legal and regulatory, the systems development life cycle (SDLC), the computer security life cycle, information assurance, and vulnerability management/scanning. In short, these controls focus on how the security of your data and systems is managed.
- **Operational controls:** These are the controls executed by people. They are designed to increase individual and group system security. They include user awareness and training, fault tolerance and disaster recovery plans, incident handling, computer support, baseline configuration development, and environmental security. The people who carry out the specific requirements of these controls must have technical expertise and understand how to implement what management desires of them.

- **Technical controls:** These are the logical controls executed by the computer system. Technical controls include authentication, access control, auditing, and cryptography. The configuration and workings of firewalls, session locks, RADIUS servers, or **RAID 5** arrays would be within this category, as well as concepts such as least privilege implementation.

The previous controls are categorical. There are also more definitive security controls:

- **Preventive controls:** These controls are employed before the event and are designed to prevent an incident. Examples include biometric systems designed to keep unauthorized persons out, NIPSs to prevent malicious activity, and **RAID 1** to prevent loss of data. These are also sometimes referred to as deterrent controls.
- **Detective controls:** These controls are used during an event and can find out whether malicious activity is occurring or has occurred. Examples include CCTV/video surveillance, alarms, NIDSs, and auditing.
- **Corrective controls:** These controls are used after an event. They limit the extent of damage and help the company recover from damage quickly. Tape backup, hot sites, and other fault tolerance and disaster recovery methods are also included here. These are sometimes referred to as compensating controls.

Key Topic

And of course, many security concepts can be placed in the category of physical as well as other categories listed previously. For example, a locking door would be an example of a physical control as well as a preventive control.

When you see technologies, policies, and procedures in the future, attempt to place them within their proper control category. Semantics will vary from one organization to the next, but as long as you can categorize security features in a general fashion such as the ones listed above, you should be able to define and understand just about any organization's security controls.

Vulnerability Management

Vulnerability management is the practice of finding and mitigating software vulnerabilities in computers and networks. It consists of analyzing network documentation, testing computers and networks with a variety of security tools, mitigating vulnerabilities, and periodically monitoring for effects and changes. Vulnerability management can be broken down into five steps:

Key Topic

Step 1. Define the desired state of security—An organization might have written policies defining the desired state of security, or you as the security administrator might have to create those policies. These policies include access control

rules, device configurations, network configurations, network documentation, and so on.

Step 2. Create baselines—After the desired state of security is defined, baselines should be taken to assess the current security state of computers, servers, network devices, and the network in general. These baselines are known as **vulnerability assessments**. The baselines should find as many vulnerabilities as possible utilizing vulnerability scans and other scanning and auditing methods. These baselines will be known as premitigation baselines and should be saved for later comparison.

Step 3. Prioritize vulnerabilities—Which vulnerabilities should take precedence? For example, the e-commerce web server we talked about earlier should definitely have a higher priority than a single client computer that does not have antivirus software installed. Prioritize all the vulnerabilities; this creates a list of items that need to be mitigated in order.

Step 4. Mitigate vulnerabilities—Go through the prioritized list and mitigate as many of the vulnerabilities as possible. This depends on the level of acceptable risk your organization allows. Mitigation techniques might include secure code review, and a review of system and application architecture and system design.

Step 5. Monitor the environment—When you finish mitigation, monitor the environment and compare the results to the original baseline. Use the new results as the post-mitigation baseline to be compared against future analyses. (Consider tools that can perform automated baseline reporting.) Because new vulnerabilities are always being discovered, and because company policies may change over time, you should periodically monitor the environment and compare your results to the post-mitigation baseline. Do this anytime policies change or the environment changes.

This five-step process has helped me when managing vulnerabilities for customers. It should be noted again that some organizations already have a defined policy for their desired security level. You might come into a company as an employee or consultant who needs to work within the company's existing mindset. In other cases, an organization won't have a policy defined; it might not even know what type of security it needs. Just don't jump the gun and assume that you need to complete Step 1 from scratch.

The most important parts of vulnerability management are the finding and mitigating of vulnerabilities. Actual tools used to conduct vulnerability assessments include network mappers, port scanners, and other vulnerability scanners, ping scanners, protocol analyzers (also called network sniffers), and password crackers. Vulnerability assessments might discover confidential data or sensitive data that is not properly

protected, open ports, weak passwords, default configurations, prior attacks, system failures, and so on. Vulnerability assessments or vulnerability scanning can be taken to the next level by administering a penetration test.

Penetration Testing

Penetration testing is a method of evaluating the security of a system by simulating one or more attacks on that system. One of the differences between regular vulnerability scanning and penetration testing is that vulnerability scanning *may* be passive or active, whereas penetration testing *will* be active. Generally, vulnerability scans will not exploit found threats, but penetration testing will definitely exploit those threats. Another difference is that vulnerability scanning will seek out all vulnerabilities and weaknesses within an organization. But penetration tests are designed to determine the impact of a particular threat against an organization. For each individual threat, a different penetration test will be planned.

Penetration tests can be done blind, as in black-box testing, where testers have little or no knowledge of the computer, infrastructure, or environment that they are testing. This simulates an attack from a person who is unfamiliar with the system. White-box testing is the converse, where the tester is provided with complete knowledge of the computer, infrastructure, or environment to be tested. And gray-box testing is when the tester is given limited inside knowledge of the system or network. Generally, penetration testing is performed on servers or network devices that face the Internet publicly. This would be an example of external security testing—when a test is conducted from outside the organization’s security perimeter. Following are a couple methodologies for accomplishing penetration testing:

- **The Open Source Security Testing Methodology Manual (OSSTMM):** This manual and corresponding methodology define the proper way to conduct security testing. It adheres to the scientific method. The manual is freely obtained from ISECOM. (The link for this can be found in the “View Recommended Resources” document on the accompanying disc.)
- **NIST penetration testing:** This is discussed in the document SP800-115. (The link for this can be found in the “View Recommended Resources” document on the accompanying disc.) This document and methodology is less thorough than the OSSTMM; however, many organizations find it satisfactory because it comes from a department of the U.S. government. At times, it refers to the OSSTMM instead of going into more detail.

NOTE Penetration testing can become even more intrusive (active) when it is associated with DLL injection testing. This is when dynamic link libraries are forced to run within currently used memory space, influencing the behavior of programs in a way the creator did not intend or anticipate.

OVAL

The **Open Vulnerability and Assessment Language (OVAL)** is a standard designed to regulate the transfer of secure public information across networks and the Internet utilizing any security tools and services available at the time. It is an international standard but is funded by the U.S. Department of Homeland Security. A worldwide OVAL community contributes to the standard, storing OVAL content in several locations, such as the MITRE Corporation (<http://oval.mitre.org/>). OVAL can be defined in two parts: the OVAL Language and the OVAL Interpreter.

- **OVAL Language:** Three different XML schemas have been developed that act as the framework of OVAL:
 1. System testing information
 2. System state analysis
 3. Assessment results reporting

OVAL is not a language like C++ but is an XML schema that defines and describes the XML documents to be created for use with OVAL.

- **OVAL Interpreter:** A reference developed to ensure that the correct syntax is used by comparing it to OVAL schemas and definitions. Several downloads are associated with the OVAL Interpreter and help files and forums that enable security people to check their work for accuracy.

OVAL has several uses, one of which is as a tool to standardize security advisory distributions. Software vendors need to publish vulnerabilities in a standard, machine-readable format. By including an authoring tool, definitions repository, and definition evaluator, OVAL enables users to regulate their security advisories. Other uses for OVAL include vulnerability assessment, patch management, auditing, threat indicators, and so on.

Some of the entities that use OVAL include Hewlett-Packard, Red Hat Inc., CA Inc., and the U.S. Army CERDEC (Communications-Electronics Research, Development and Engineering Center).

Assessing Vulnerability with Security Tools

Until now, we have talked about processes, methodologies, and concepts. But without actual security tools, testing, analyzing, and assessing cannot be accomplished. This section delves into the security assessment tools you might use in the field today, and shows how to interpret the results that you receive from those tools.

Computers and networks are naturally vulnerable. Whether it is an operating system or an appliance installed out-of-the-box, they are inherently insecure. Vulnerabilities could come in the form of backdoors or open ports. They could also be caused after installation due to poor design.

To understand what can be affected, security administrators should possess thorough computer and network documentation, and if they don't already, they should develop it themselves. Tools such as Microsoft Visio and network mapping tools can help to create proper network documentation. Then, tools such as vulnerability scanners, protocol analyzers, and password crackers should be used to assess the level of vulnerability on a computer network. When vulnerabilities are found, they should be eliminated or reduced as much as possible. Finally, scanning tools should be used again to prove that the vulnerabilities to the computer network have been removed.

You will find that most of the tools described in this section are used by security administrators and hackers alike. The former group uses the tools to find vulnerabilities and mitigate risk. The latter group uses the tools to exploit those vulnerabilities. However, remember that not all hackers are malevolent. Some are just curious, but they can cause just as much damage and downtime as a malicious hacker.

Network Mapping

Network documentation is an important part of defining the desired state of security. To develop adequate detailed network documentation, network mapping software should be used with network diagramming software. **Network mapping** is the study of physical and logical connectivity of networks. One example of network mapping software is the Network Topology Mapper by SolarWinds. This product can map elements on layers 1 through 3 of the OSI model, giving you a thorough representation of what is on the network. This type of network scan is not for the “weak of bandwidth.” It should be attempted only during off-hours (if there is such a thing nowadays), if possible; otherwise, when the network is at its lowest point of usage. Figure 11-1 shows an example of a test network mapped with a LANsurveyor (the predecessor to Network Topology Mapper). It was configured to map the 10.254.254.0 network but can be arranged to analyze a larger network space. You will notice that a computer named Server2003 is listed twice. This could be a possible security issue, or it could mean that the computer is multihomed or has two IP addresses bound to the same network adapter. Either way, it should be verified and

possibly fixed during the mitigation phase of vulnerability assessment. This program shows routers, layer 3 switches, client computers, servers, and virtual machines. It can also export the mapped contents directly to Microsoft Visio, a handy time-saver.

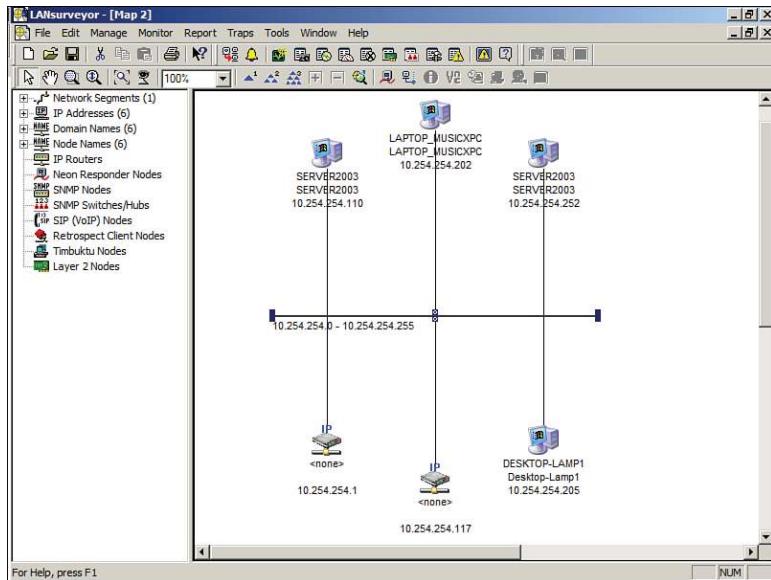


Figure 11-1 Example Network Map

Plenty of other free and pay versions of network mapping software are available. A quick Internet search displays a list. Try out different programs, get to know them, and decide what works best for your infrastructure.

Wireless networks can be surveyed in a similar fashion. Applications such as Air-Magnet can map out the wireless clients on your network and output the information as you want to aid in your network documentation efforts.

When you are working on your network documentation, certain areas of the network probably need to be filled in manually. Some devices are tough to scan, and you have to rely on your eyes and other network administrators' knowledge to get a clear picture of the network. Network documentation can be written out or developed with a network diagramming program, such as Microsoft Visio. (A free trial is available at Microsoft's Office website.) Visio can make all kinds of diagrams and flowcharts that can be real time-savers and helpful planning tools for network administrators and security people. An example of a network diagram is shown in Figure 11-2. This network diagram was created by mapping a now-defunct network with network mapping software, exporting those results to Visio, and then making some tweaks to the diagram manually. Names and IP addresses (among other

things) were changed to protect the innocent. This documentation helped to discover a few weaknesses such as the lack of firewalling and other DMZ issues such as the lack of CIDR notation on the DMZ IP network. Just the act of documenting revealed some other issues with some of the servers on the DMZ, making it much easier to mitigate risk. When the risks were mitigated, the resulting final network documentation acted as a foundation for later security analysis and comparison to future baselines.

At times, you might be tempted to put passwords into a network diagram—don't do it! If there are too many passwords to memorize, and you need to keep passwords stored somewhere, the best way is to write them on a piece of paper and lock that paper in a fireproof, non-removable safe, perhaps offsite. The people (admins) who know the combination to the safe should be limited. Don't keep passwords on any computers!

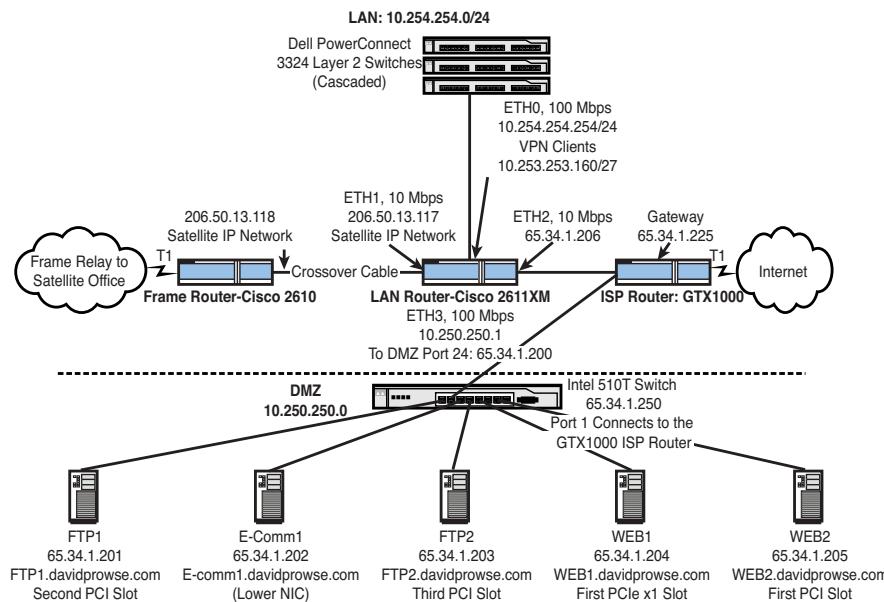


Figure 11-2 Network Diagram Created with Microsoft Visio

You might also want to keep a list of IP addresses, computer names, and so on. This can be done on paper, within Excel or Access, or can be developed within your network mapping program and exported as you want. I find that Excel works great because you can sort different categories by the column header.

To summarize, network mapping can help in several of the vulnerability assessment phases. Be sure to use network mapping programs and document your network thoroughly. It can aid you when baselining and analyzing your networks and systems.

Vulnerability Scanning

Vulnerability scanning is a technique that identifies threats on your network, but does not exploit them. When you are ready to assess the level of vulnerability on the network, it is wise to use a general vulnerability scanner and a port scanner (or two). By scanning all the systems on the network, you determine the attack surface of those systems, and you can gain much insight as to the risks that you need to mitigate, and malicious activity that might already be going on underneath your nose.

One such vulnerability scanner is called Nessus. Originally developed for Unix, you can now obtain versions for Linux and Windows as well. As of the writing of this book, Nessus 5 is the current version. It is available for home study use for free, but if you use it in the business world, there is a subscription fee (which is a common theme when it comes to third-party software of this sort). Vulnerability scanners like this one are usually active and can discover vulnerabilities within your network and beyond. Because it is a powerful, active-scanning, high-speed software tool, it should be used cautiously and most likely when there is a lull in network usage or perhaps off-hours.

The tool has a server side and a client side. The server side is used to manage users and settings and store scans. The client side runs within a browser and is where you do your actual scans. To scan a host or network, you must first create a policy defining what you want to scan for. Then, you scan according to the policy you created. In a non-credentialed environment (remotely scanning), these types of active scans can be quite resource-intensive, so they can take some time to complete. However, you can perform credentialed scanning with a tool such as Nessus as well. This means that by presenting the appropriate credentials to the local computer, the scan can be run locally, instead of across the network, saving resources. This also results in a more complete list of client application vulnerabilities and missing patches to the OS, and in general provides a more descriptive vulnerability assessment.

An example of a vulnerability scan with Nessus is shown in Figure 11-3. It shows some open ports on the IP 10.254.254.1 and their corresponding services that may or may not be vulnerabilities. The tool can also check for backdoors, denial-of-service attacks, and lots of other families of threats. If you suspect that a particular computer is the victim of a malicious attack, this is an excellent tool to use to make that determination. Even if you are not sure, scanning important hosts on the network can help to put your mind at ease or...uncover risks that you must mitigate.

Key Topic

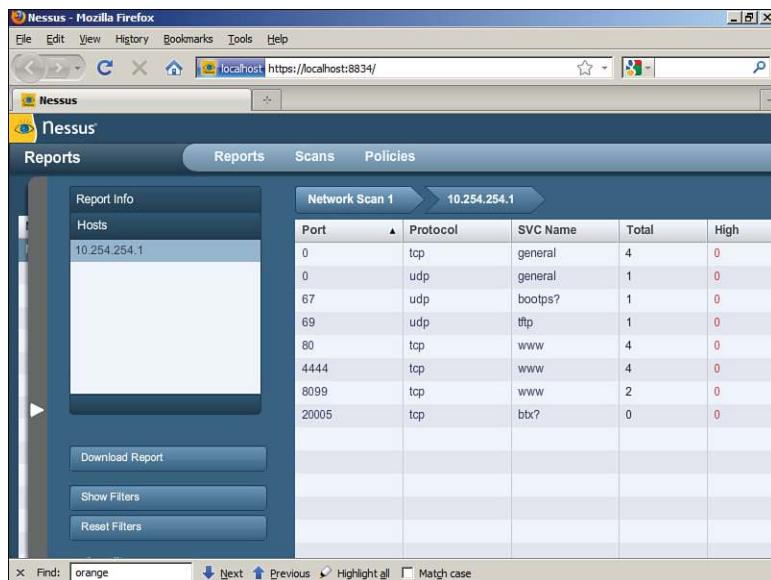


Figure 11-3 Network Vulnerability Scan with Nessus

Other formidable vulnerability scanners include Nsauditor (Network Security Auditor), NetBrute, GFI LanGuard, and ISS Internet Scanner. Sometimes, these tools are referred to as network scanners if they are used to find open ports within multiple computers on the network or the entire network. Although some vulnerability scanners will scan the ports of a system (which is considered to be active scanning), the use of vulnerability scanners is generally considered to be a passive attempt at identifying weaknesses.

Sometimes, a full-blown vulnerability scanner isn't necessary. There will be times when you simply want to scan ports or run other basic tests. As previously discussed in Chapter 6, an example of a good **port scanner** is Nmap. Although this tool has other functionality in addition to port scanning, it is probably best known for its port scanning capability. Figure 11-4 shows an example of a port scan with Nmap. This shows a scan (using the `-ss` parameter) to a computer that runs Kerberos (port 88), DNS (port 53), and web services (port 80), among other things. By using a port scanner like this one, you are taking a fingerprint of the operating system. The port scanner tells you what inbound ports are open on the remote computer and what services are running. From this, you can discern much more information, for example, what operating system the computer is running, what applications, and so on. In the example in Figure 11-4, you can gather that the scanned computer is a Microsoft domain controller running additional services. So this is an example of OS fingerprinting.



```

C:\>cd nmap
C:\nmap>nmap -sS 172.29.250.200
Starting nmap 3.75 (< http://www.insecure.org/nmap >) at 2009-02-04 12:06 Eastern Standard Time
Interesting ports on 172.29.250.200:
(The 1645 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
697/tcp   open  h323
1025/tcp  open  NPS-or-IIS
1027/tcp  open  IIS
1433/tcp  open  ms-sql-s
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-term-serv

Nmap run completed -- 1 IP address (1 host up) scanned in 1.883 seconds
C:\nmap>

```

Figure 11-4 Port Scan with Nmap

Open ports should be examined. You should be fully aware of the services or processes that use those ports. If services are unnecessary, they should be stopped and disabled. For example, if this computer was indeed a domain controller but wasn't supposed to be a DNS server, the DNS service (port 53) should be stopped. Otherwise, the DNS port could act as a vulnerability of the server. Afterward, the computer should be rescanned to ensure that the risk has been mitigated.

Nonessential services are often not configured, monitored, or secured by the network administrator. It is imperative that network administrators scan for nonessential services and close any corresponding ports. Even though services may be nonessential, that doesn't necessarily mean that they are not in use, maliciously or otherwise.

As discussed in Chapter 9, "Physical Security and Authentication Models, another tool that can be used to display the ports in use is the `netstat` command. Examples include the `netstat`, `netstat -a`, `netstat -n`, and `netstat -an` commands. However, this is only for the local computer, but it does show the ports used by the remote computer for the sessions that the local computer is running.

NOTE Other port scanners include PortScan, SuperScan, and Angry IP Scanner (there are plenty of other free port scanners on the Internet). Some of these tools can be used as ping scanners, sending out ICMP echoes to find the IP addresses within a particular network segment.

Tools such as Nmap and Nessus are also known as network enumerators. *Enumeration* refers to a complete listing of items (such as port numbers); network enumerators extract information from servers including network shares, services running, groups of users, and so on. It is this additional extraction of information (enumerating) that sets them apart from a basic network mapping tool. This type of enumeration is also referred to as banner grabbing. **Banner grabbing** is a technique used to find out information about web servers, FTP servers, and mail servers. For example, it might be used by a network administrator to take inventory of systems and services running on servers. Or, it could be used by an attacker to grab information such as HTTP headers, which can tell the attacker what type of server is running, its version number, and so on. Examples of banner grabbing applications include Netcat and Telnet. Aside from the security administrator (and perhaps auditors), no one should be running banner grabbing tools, or network enumeration tools in general. A good security admin will attempt to sniff out any unpermitted usage of these tools.

Network Sniffing

For all intents and purposes, the terms protocol analyzer, packet sniffer, and network sniffer all mean the same thing. “Sniffing” the network is when you use a tool to find and investigate other computers on the network; the term is often used when capturing packets for later analysis. **Protocol analyzers** can tell you much more about the traffic that is coming and going to and from a host than a vulnerability scanner or port scanner might. In reality, the program captures Ethernet frames of information directly from the network adapter and displays the packets inside those frames within a capture window. Each packet is *encapsulated* inside a frame.

One common example of a protocol analyzer is Wireshark, previously known as Ethereal, which is a free download that can run on a variety of platforms. By default, it captures packets on the local computer that it was installed on. Figure 11-5 shows an example of a packet capture. This capture is centered on frame number 10, which encapsulates an ICMP packet. This particular packet is a ping request sent from the local computer (10.254.254.205) to the remote host (10.254.254.1). Although my local computer can definitely send out pings, it is unknown whether 10.254.254.1 should be replying to those pings. Perhaps there is a desired policy that states that this device (which is actually a router) should not reply to pings. As we learned in Chapter 6, “Networking Protocols and Threats,” an ICMP reply can

be a vulnerability. Now, if we look at frame 11 we see it shows an echo reply from 10.254.254.1—not what we want. So, to mitigate this risk and remove the vulnerability, we would turn off ICMP echo replies on the router.

This is just one example of many that we could show with this program. I've used this program to find, among other things, unauthorized FTP, gaming, and P2P traffic! You'd be surprised how often network admins and even regular old users set up these types of servers. It uses up valuable bandwidth and resources, so you can imagine that an organization would want these removed. Not only that, but they can be vulnerabilities as well. By running these services, a person opens up the computer system to a whole new set of threats. By removing these unauthorized servers, we are reducing risk. I know—I'm such a buzzkill. But really now, work is work, and play is play; that's how companies are going to look at it.

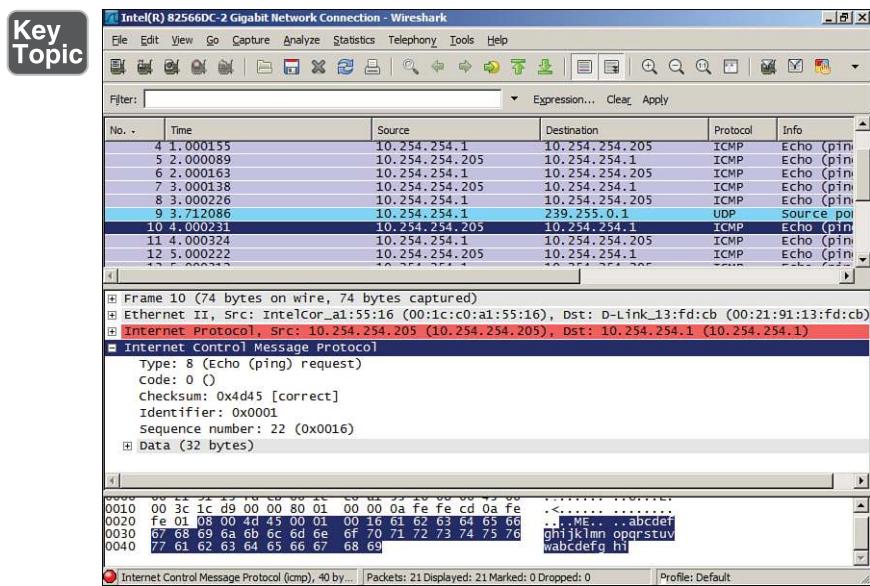


Figure 11-5 Packet Capture with Wireshark

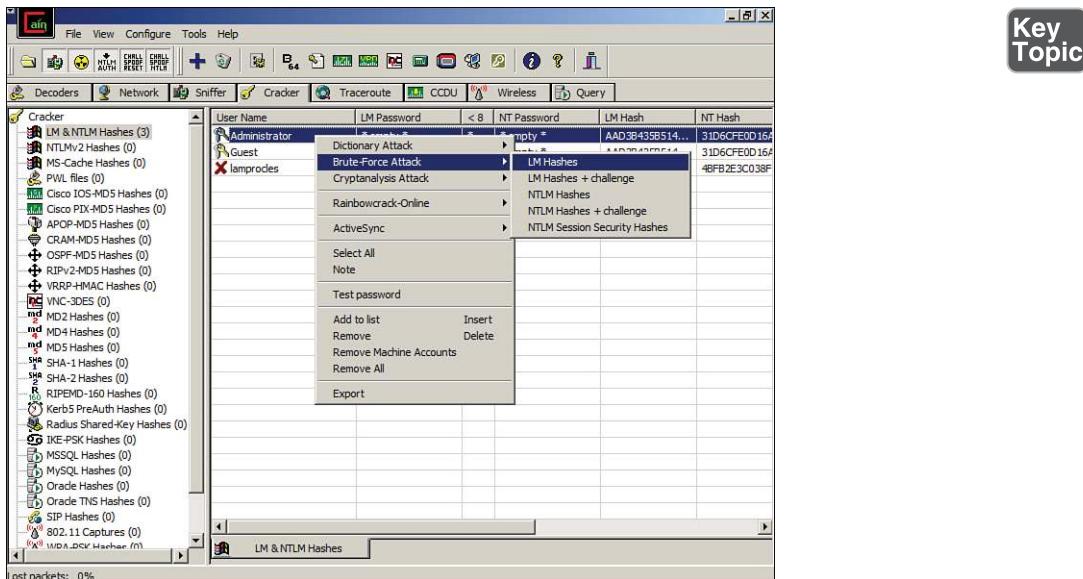
On the other side of things, malicious users will utilize a protocol analyzer to capture passwords and other confidential information. We discuss software-based protocol analyzers more in Chapter 12, “Monitoring and Auditing.”

Other software-based packet sniffers include TCPdump, WinDump, Sniffer Pro, and EtherDetect. Also, hardware-based devices can analyze your networks and hosts; for example, Fluke Networks offers a variety of network testers. These handheld computers often have a GUI-based or text-based menu system that can be used to monitor ports, troubleshoot authentication issues, identify network resources and

IP addresses, and lots more. The name *Fluke* is used by some techs even if they use a handheld device by a different vendor; the brand is that well-known.

Password Analysis

Well, we've mapped the network, documented it, scanned for vulnerabilities, scanned ports, and analyzed packets. But wait, let's not forget about passwords. We've mentioned more than once in this book that weak passwords are the bane of today's operating systems and networks. This could be because no policy for passwords was defined, and people naturally gravitate toward weaker, easier-to-remember passwords. Or it could be that a policy was defined but is not complex enough, or is out of date. Whatever the reason, it would be wise to scan computers and other devices for weak passwords with a **password cracker**, which uses comparative analysis to break passwords and systematically guesses until it cracks the password. And of course, a variety of password-cracking programs can help with this. For Windows computers, there is the well-documented Cain & Abel password recovery tool. This program has a bit of a learning curve but is quite powerful. It can be used to crack all kinds of different passwords on the local system or on remote devices and computers. It sniffs out other hosts on the network the way a protocol analyzer would. This is an excellent tool to find out whether weak passwords are on the network, or to help if users forget their passwords (when password resets are not possible). Figure 11-6 shows an example of Cain & Abel. You can see hashed passwords (encrypted) that the program has discovered for various accounts on a test computer. From these hashes, the program can attempt to crack the password and deliver the original plaintext version of the password.



Key Topic

Figure 11-6 Password Cracking with Cain & Abel

We talk more about hashes and hashing algorithms in Chapter 13, “Encryption and Hashing Concepts.”

Cain & Abel is a free download, and many other tools are available for various platforms; some free, some not, including ophcrack, John the Ripper, THC-Hydra, Aircrack-ng (used to crack WPA preshared keys), and RainbowCrack. Some of these tools have additional functionality but are known best as password/passphrase-cracking tools, although they can be used by security administrators in a legitimate sense as password recovery programs.

The following list shows the various password-cracking methods. Password recovery (or cracking) can be done in several different ways:

Key Topic

- **Guessing:** Weak passwords can be guessed by a smart person, especially if the person has knowledge of the user he is trying to exploit. Blank passwords are all too common. And then there are common passwords such as password, admin, secret, love, and many more. If a guessing attacker knew the person and some of the person’s details, he might attempt the person’s username as the password, or someone the person knows, date of birth, and so on. Reversing letters or adding a 1 to the end of a password are other common methods. Although guessing is not as much of a technical method as the following three options, it reveals many passwords every day all over the world.
- **Dictionary attack:** Uses a prearranged list of likely words, trying each of them one at a time. It can be used for cracking passwords, passphrases, and keys. It works best with weak passwords and when targeting multiple systems. The power of the dictionary attack depends on the strength of the dictionary used by the password cracking program.
- **Brute-force attack:** When every possible password instance is attempted. This is often a last resort due to the amount of CPU resources it might require. It works best on shorter passwords but can theoretically break any password given enough time and CPU power. For example, a four-character, lowercase password with no numbers or symbols could be cracked fairly quickly. But a ten-character, complex password would take much longer; some computers will fail to complete the process. Also, you have to consider whether the attack is online or offline. Online means that a connection has been made to the host, giving the password-cracking program only a short window to break the password. Offline means that there is no connection and that the password-cracking computer knows the target host’s password hash and hashing algorithm, giving the cracking computer more (or unlimited) time to make the attempt. Some password-cracking programs are considered hybrids and make use of dictionary attacks (for passwords with actual words in them) and brute-force attacks (for complex passwords).

NOTE Some attackers will utilize software that can perform hybrid attacks that consist of successive dictionary and brute-force attacks.

- **Cryptanalysis attack:** Uses a considerable set of precalculated encrypted passwords located in a lookup table. These tables are known as **rainbow tables**, and the type of password attack is also known as precomputation, where all words in the dictionary (or a specific set of possible passwords) are hashed and stored. This is done in an attempt to recover passwords quicker. It is used with the ophcrack and RainbowCrack applications. This attack can be defeated by implementing **salting**, which is the randomization of the hashing process.

Knowledgeable attackers understand where password information is stored. In Windows it is stored in an encrypted binary format within the SAM hive. In Linux, the data used to verify passwords was historically stored in the /etc/passwd file, but in newer Linux systems the passwd file only shows an X, and the real password information is stored in another file, perhaps /etc/shadow, or elsewhere in an encrypted format.

Aside from using password-cracking programs, passwords can be obtained through viruses and Trojans, wiretapping, keystroke logging, network sniffing, phishing, shoulder surfing, and dumpster diving. Yikes! It should go without mentioning that protecting passwords is just as important as creating complex passwords and configuring complex password policies that are also periodically monitored and updated. Remember that password policies created on a Windows Server do not have jurisdiction where other vendors' devices are concerned, such as Cisco routers and firewalls or Check Point security devices. These need to be checked individually or by scanning particular network segments.

We could talk about password cracking for days because there are so many types of hashes, hashing algorithms, and password-cracking tools and ways to crack the passwords. But for the Security+ exam, a basic understanding of password cracking is enough.

There were a lot of tools discussed in this chapter. Table 11-3 quickly reviews those tools.

**Table 11-3** Summary of Chapter 11 Security Tools

Security Tool	Description
Network Topology Mapper (LANsurveyor)	Network mapping tool
Microsoft Visio	Network diagramming tool
Nessus	Vulnerability scanner
Nmap	Port scanner
Wireshark	Protocol analyzer
Fluke	Handheld protocol analyzer/network sniffer
Cain & Abel	Password-cracking tool
John the Ripper	Password-cracking tool
Ophcrack	Password-cracking tool

Chapter Summary

It's a fact: As people, we are vulnerable to all kinds of medical conditions, injuries, maladies, and so on. However, the typical human being tends to find an equilibrium with himself or herself...and with nature. By this I mean that a person tends to automatically prevent medical problems from happening, and performs a certain level of self-healing when many problems do occur. We are intuitive. We drink water *before* we become dehydrated. We sleep before we become overtired. Most of the time, we automatically defend ourselves from germs and viruses, because we have consciously (and unconsciously) focused on preventative maintenance for our bodies and minds.

In a way, this philosophy can also be applied to technology. Your organization's technology environment—in all of its parts—can be treated as a sort of entity; similar to the bond a captain might have with a seagoing vessel. When this synergy happens, a person spends more productive time working on preventing problems, and as a result, spends less time fixing issues that occurred due to a compromise simply because compromises end up happening less frequently. Just as the captain will inspect the hull of a ship with a keen set of eyes, you must constantly inspect all parts of your technology for current and potential vulnerabilities. As Benjamin Franklin said, “An ounce of prevention is worth a pound of cure.” It’s a cliché, yet so necessary to revisit from time to time.

There are a great many terms, acronyms, and definitions when it comes to security analysis, but it all boils down to vulnerabilities, and how to prevent threats from exploiting them—that is, minimizing risk. You must plan ahead; not just for current

attacks and CVEs, but also for what is on the horizon. Time must be spent considering what will happen to an installed device or computer in a year, or five years. That time will be here before you know it!

Define the risk, as it appears now, and as it will appear in the future. Reduce as much risk as possible, so that all but the most unlikely threats will be prevented. It's that prevention that is the key. Of all the security controls, prevention is the most important. One excellent way to be sure that you are doing your best to *prevent* problems is to use a vulnerability management process. This leaves nothing to chance. Another masterful way to manage vulnerabilities is to utilize automation. You can't clone yourself (yet), but you can clone your administrations. The size of your IT environment and the level of automation you employ should be proportionate.

Penetration testing, vulnerability scanning, port scanning, network sniffing, and password analysis are all just methods to be used within your risk and vulnerability assessments. You might use some methodologies, and not others, and you might perform assessments in an active or passive manner. That will depend on the particulars of your network and the level of criticality of your IT environment. And you may use different methods than the ones listed in this chapter, or develop new ones in the future. The list is in no way finite. The crucial point is to realize that you are taking the consolidated information you glean and using it to define the real risk to your organization in an intuitive way.

So think of your IT infrastructure as a sort of living, breathing entity: One that relies on you as much as you rely on it.

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 11-4 lists a reference of these key topics and the page number on which each is found.

Table 11-4 Key Topics for Chapter 11

Key Topic Element	Description	Page Number
Table 11-1	Example of quantitative risk assessment	427
Table 11-2	Summary of risk assessment types	428

Key Topic Element	Description	Page Number
Bulleted list	NIST security controls	430
Bulleted list	Event-based security controls	431
Numbered list	Five steps of vulnerability management	431
Figure 11-3	Network vulnerability scan with Nessus	439
Figure 11-4	Port scan with Nmap	440
Figure 11-5	Packet capture with Wireshark	442
Figure 11-6	Password cracking with Cain & Abel	443
Bulleted list	Password-cracking methods	444
Table 11-3	Summary of Chapter 11 security tools	446

Define Key Terms

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

vulnerability, risk, risk management, information assurance (IA), risk transference, risk avoidance, risk reduction, risk acceptance, residual risk, risk assessment, qualitative risk assessment, risk mitigation, quantitative risk assessment, mean time between failures (MTBF), vulnerability management, vulnerability assessment, penetration testing, Open Vulnerability and Assessment Language (OVAL), network mapping, vulnerability scanning, port scanner, banner grabbing, protocol analyzer, password cracker, dictionary attack, brute-force attack, cryptanalysis attack, rainbow tables, salting

Review Questions

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

1. Which type of vulnerability assessments software can check for weak passwords on the network?
 - A. Wireshark
 - B. Antivirus software
 - C. Performance Monitor
 - D. A password cracker

2. You are contracted to conduct a forensic analysis of the computer. What should you do first?
 - A. Back up the system.
 - B. Analyze the files.
 - C. Scan for viruses.
 - D. Make changes to the operating system.
3. Which of the following has schemas written in XML?
 - A. OVAL
 - B. 3DES
 - C. WPA
 - D. PAP
4. Russ is using only documentation to test the security of a system. What type of testing methodology is this known as?
 - A. Active security analysis
 - B. Passive security analysis
 - C. Hybrid security analysis
 - D. Hands-on security analysis
5. Of the following, which is the best way for a person to find out what security holes exist on the network?
 - A. Run a port scan.
 - B. Use a network sniffer.
 - C. Perform a vulnerability assessment.
 - D. Use an IDS solution.
6. After using Nmap to do a port scan of your server, you find that several ports are open. Which of the following should you do next?
 - A. Leave the ports open and monitor them for malicious attacks.
 - B. Run the port scan again.
 - C. Close all ports.
 - D. Examine the services and/or processes that use those ports.

- 7.** Which of the following is a vulnerability assessment tool?
 - A.** John the Ripper
 - B.** Aircrack-ng
 - C.** Nessus
 - D.** Cain & Abel
- 8.** You are a consultant for an IT company. Your boss asks you to determine the topology of the network. What is the best device to use in this circumstance?
 - A.** Network mapper
 - B.** Protocol analyzer
 - C.** Port scanner
 - D.** Vulnerability scanner
- 9.** Which of the following can enable you to find all the open ports on an entire network?
 - A.** Protocol analyzer
 - B.** Network scanner
 - C.** Firewall
 - D.** Performance monitor
- 10.** What can hackers accomplish using malicious port scanning?
 - A.** “Fingerprint” of the operating system
 - B.** Topology of the network
 - C.** All the computer names on the network
 - D.** All the usernames and passwords
- 11.** Many companies send passwords via clear text. Which of the following can view these passwords?
 - A.** Rainbow table
 - B.** Port scanner
 - C.** John the Ripper
 - D.** Protocol analyzer

- 12.** Which of the following persons is ultimately in charge of deciding how much residual risk there will be?
- A.** Chief security officer
 - B.** Security administrator
 - C.** Senior management
 - D.** Disaster recovery plan coordinator
- 13.** To show risk from a monetary standpoint, which of the following should risk assessments be based upon?
- A.** Survey of loss, potential threats, and asset value
 - B.** Quantitative measurement of risk, impact, and asset value
 - C.** Complete measurement of all threats
 - D.** Qualitative measurement of risk and impact
- 14.** The main objective of risk management in an organization is to reduce risk to a level _____. (Fill in the blank.)
- A.** The organization will mitigate
 - B.** Where the ARO equals the SLE
 - C.** The organization will accept
 - D.** Where the ALE is lower than the SLE
- 15.** Why would a security administrator use a vulnerability scanner? (Select the best answer.)
- A.** To identify remote access policies
 - B.** To analyze protocols
 - C.** To map the network
 - D.** To find open ports on a server
- 16.** An example of a program that does comparative analysis is what?
- A.** Protocol analyzer
 - B.** Password cracker
 - C.** Port scanner
 - D.** Event Viewer

17. Why do hackers often target nonessential services? (Select the two best answers.)

- A.** Often they are not configured correctly.
- B.** They are not monitored as often.
- C.** They are not used.
- D.** They are not monitored by an IDS.

18. Which of the following tools uses ICMP as its main underlying protocol?

- A.** Ping scanner
- B.** Port scanner
- C.** Image scanner
- D.** Barcode scanner

19. Which command would display the following output?

Active Connections			
Proto	Local Address	Foreign Address	State
TCP	laptop-musicxpc:1395	8.15.228.165:http	ESTABLISHED

- A.** Ping
- B.** Ipconfig
- C.** Nbtstat
- D.** Netstat

20. Which of the following is used when performing a quantitative risk analysis?

- A.** Asset value
- B.** Surveys
- C.** Focus groups
- D.** Best practices

21. You have been tasked with running a penetration test on a server. You have been given limited knowledge about the inner workings of the server. What kind of test will you be performing?

- A.** White box
- B.** Gray box
- C.** Black box
- D.** Passive vulnerability scan

- 22.** Which of the following is a technical control?
- A.** Disaster recovery plan
 - B.** Baseline configuration development
 - C.** Least privilege implementation
 - D.** Categorization of system security
- 23.** Which of the following is a detective security control?
- A.** Bollards
 - B.** Firewall
 - C.** Tape backup
 - D.** CCTV
- 24.** Which of the following is a management control?
- A.** Least privilege implementation
 - B.** Baseline configuration development
 - C.** Written security policy
 - D.** Session locks
- 25.** Which of the following would you make use of when performing a qualitative risk analysis?
- A.** Judgment
 - B.** Asset value
 - C.** Threat frequency
 - D.** SLE
- 26.** What is the best action to take when you conduct a corporate vulnerability assessment?
- A.** Document your scan results for the change control board
 - B.** Examine vulnerability data with a network sniffer
 - C.** Update systems
 - D.** Organize data based on severity and asset value
- 27.** You are implementing a new enterprise database server. After you evaluate the product with various vulnerability scans you determine that the product is not a threat in of itself but it has the potential to introduce new vulnerabilities

to your network. Which assessment should you now take into consideration while you continue to evaluate the database server?

- A.** Risk assessment
 - B.** Code assessment
 - C.** Vulnerability assessment
 - D.** Threat assessment
- 28.** Why should penetration testing only be done during controlled conditions?
- A.** Because vulnerability scanners can cause network flooding.
 - B.** Because penetration testing actively tests security controls and can cause system instability.
 - C.** Because white-box penetration testing cannot find zero-day attacks.
 - D.** Because penetration testing passively tests security controls and can cause system instability.
- 29.** You are attempting to prevent unauthorized access to the desktop computers on your network. You decide to have the computers' operating systems lock after 5 minutes of inactivity. What type of security control is this?
- A.** Detective
 - B.** Operational
 - C.** Management
 - D.** Technical
- 30.** Which of the following methods can be used by a security administrator to recover a user's forgotten password from a password protected file?
- A.** Brute force
 - B.** Packet sniffing
 - C.** Social engineering
 - D.** Cognitive password

Answers and Explanations

- 1. D.** A password cracker can check for weak passwords on the network. Antivirus software can scan for viruses on a computer. Performance Monitor enables you to create baselines to check the performance of a computer. Wireshark is a protocol analyzer.

2. **A.** Back up the system before you do anything else. This way, you have a backup copy in case anything goes wrong when you analyze or make changes to the system. When doing a forensic analysis (one that might be required for legal proceedings), be sure to image the system, and work off of the copied image.
3. **A.** OVAL (Open Vulnerability and Assessment Language) uses XML as a framework for the language. It is a community standard dealing with the standardization of information transfer. 3DES is an encryption algorithm. WPA is a wireless encryption standard, and the deprecated PAP is the Password Authentication Protocol, used for identifying users to a server.
4. **B.** Passive security analysis or passive security testing would be one that possibly does not include a hands-on test. It is less tangible and often includes the use of documentation only. To better protect a system or network, a person should also use active security analysis.
5. **C.** The best way to find all the security holes that exist on a network is to perform a vulnerability assessment. This may include utilizing a port scanner and using a network sniffer and perhaps using some sort of IDS.
6. **D.** If you find ports open that you don't expect, be sure to examine the services and/or processes that use those ports. You may have to close some or all those ports. When you finish with your examination, and after you have taken action, run the port scan again to verify that those ports are closed.
7. **C.** Nessus is a vulnerability assessment tool. Aircrack-ng is used to crack wireless encryption codes. John the Ripper and Cain & Abel are password-cracking programs.
8. **A.** A network mapper is the best tool to use to determine the topology of the network and to find out what devices and computers reside on that network. One example of this is the Network Topology Mapper.
9. **B.** A network scanner is a port scanner used to find open ports on multiple computers on the network. A protocol analyzer is used to delve into packets. A firewall protects a network, and a performance monitor is used to create baselines for and monitor a computer.
10. **A.** Port scanning can be used in a malicious way to find out all the openings to a computer's operating system; this is known as the "fingerprint" of the operating system. Port scanning cannot find out the topology of the network, computer names, usernames, or passwords.
11. **D.** A protocol analyzer can delve into the packets sent across the network and determine whether those packets contain clear-text passwords. Rainbow

tables and John the Ripper deal with cracking passwords that were previously encrypted; they aren't necessary if the passwords were sent via clear text. Port scanners scan computers for any open ports.

12. **C.** Residual risk is the risk left over after a security plan and a disaster recovery plan have been implemented. There is always risk, because a company cannot possibly foresee every future event, nor can it secure against every single threat. Senior management as a collective whole is ultimately responsible for deciding how much residual risk there will be in a company's network. No one person should be in charge of this, but it should be decided on as a group. If the group decides that residual risk is too high, the group might decide to get insurance in addition to its security plan. The security administrator is in charge of finding and removing risks to the network and systems and should mitigate risks if possible. The disaster recovery plan (DRP) coordinator usually assesses risks and documents them, along with creating strategies to defend against any disastrous problems that might occur from that risk, but that person does not decide on the amount of acceptable residual risk to a company.
13. **B.** When dealing with dollars, risk assessments should be based upon a quantitative measurement of risk, impact, and asset value.
14. **C.** The main objective of risk management is to reduce risk to a level that the organization or company will accept. Mitigation is the act of reducing threats in general.
15. **D.** The best answer for why a security administrator would use a vulnerability scanner is to find open ports on a particular computer. Although a vulnerability scanner can do more than scan for open ports, it is the best answer listed.
16. **B.** A password cracker is considered to be a program that does comparative analysis. It systematically guesses the password and compares all previous guesses before making new ones until it cracks the password.
17. **A. and B.** Nonessential services are often not configured and secured by the network administrator; this goes hand-in-hand with the fact that they are not monitored as often as essential services. It is imperative that network administrators scan for nonessential services and close any corresponding ports. Even though services may be nonessential, that doesn't necessarily mean that they are not used. An IDS, if installed properly, should monitor everything on a given system.
18. **A.** A ping scanner uses the Internet Control Message Protocol (ICMP) to conduct its scans. Ping uses ICMP as its underlying protocol and IP and ARP. Image scanners are found in printers and as standalone items that scan images, photos, and text into a computer. Barcode scanners are used to scan barcodes, for example, at the supermarket.

- 19.** **D.** Netstat shows sessions including the local computer and remote computer. It shows these connections by computer name (or IP) and port name (or number).
- 20.** **A.** Asset value is assigned when performing quantitative risk analysis. Surveys, focus groups, and best practices might help with qualitative risk analysis but do not offer concrete data that a quantitative risk analysis requires. Money is the key ingredient here when it comes to quantitative risk analysis.
- 21.** **B.** When you are given limited information of a system or network, it is known as gray-box testing. White-box testing is when you are given in-depth or complete information about the system. Black-box testing is when you know very little (or nothing) about the system to be tested. Penetration tests are active and are meant to test for a single threat and exploit it. Passive vulnerability scans are different tests altogether and test for as many threats as they can find, without exploiting one of them.
- 22.** **C.** The least privilege concept is executed as a technical control. A process that is severely limited in its functionality and a user who has very limited rights are some of the things that must be initiated technically. A disaster recovery plan and baseline configuration development would be operational controls. The categorization of system security would be a management control.
- 23.** **D.** CCTV (closed-circuit television) is an example of a detective security control. It can detect who is entering a building and when it happened. Bollards (vertical posts often found in parking lots or in front of doorways) and firewalls are preventive controls, while tape backup is a corrective control.
- 24.** **C.** A written security policy would be an example of a management control. Another example would be a report developed based on a vulnerability assessment. Least privilege implementation and session locks would be examples of technical controls. Baseline configuration development would be an example of an operational control.
- 25.** **A.** When performing a qualitative risk analysis, a person often uses his own judgment. Asset value, threat frequency, and SLE (single loss expectancy) are all components of a quantitative risk analysis.
- 26.** **D.** When conducting vulnerability assessments, you should organize the collected data by vulnerability and exploit severity as well as the asset value of the possibly affected equipment/systems. Documenting your scan results for a change control board may come later depending on some decision-making by the corporation. You should have already used a network sniffer to find vulnerabilities and possible exploits. Updating the systems will most likely happen at some point, but for the time being, it should be a recommendation

within your vulnerability assessment. Management will decide how and if that will occur.

27. **A.** If a new solution poses the potential for new vulnerabilities to your network, you should run an in-depth risk assessment of the new product. In this case, you are not yet doing any coding, so a code assessment is not necessary, but should be implemented as part of a secure code review in the case that you make any programming changes to the database server. You have already run a vulnerability assessment when you did the vulnerability scans. You found that the solution is not a threat but could pose other threats. The risk assessment defines what kind of issues your organization could face due to the threats and vulnerabilities.
28. **B.** Penetration testing is an active test that seeks to exploit one vulnerability. It can indeed cause system instability, so it should be run only during controlled conditions and with express consent of the system owner. Vulnerability scanners are usually passive and should not cause network flooding. Zero-day attacks are based on vulnerabilities that are unknown to the system designer. In a white-box testing environment, zero-day vulnerabilities may become uncovered (at which point they are not quite zero-day anymore), but the fact remains that penetration testing can cause system instability.
29. **D.** An operating system lock (or screen saver lock) is an example of a technical control; it is also considered more technically to be a preventive control. An example of a detective control would be CCTV. An example of an operational control would be security awareness training. An example of a management security control would be the systems development life cycle (SDLC).
30. **A.** The brute-force method can be used to recover a user's password from a protected file or otherwise protected area of an operating system. Tools such as these are used by security administrators to recover passwords, but are also used by attackers to crack password codes in order to obtain unauthorized access. Packet sniffing can be used to find passwords that have been sent over the network in clear text (which happens more often than you might suspect), but cannot crack the password stored in a protected file. Social engineering is when con artists attempt to find out information (such as a password) from unsuspecting users. But in the scenario of the question, the user has forgotten the password (thus the need for recovery), so social engineering would be pointless. The cognitive password is an authentication type where, in addition to the password, the user must answer a question of some sort; used collectively, the authentication system grants access if the answer and the password are correct. This is an excellent method to use in the case an attacker does crack a password, because that second level of authentication (based on the user's knowledge) is necessary. And that is when social engineering could perform

wonders, attempting to elicit that information from the user. But again, for this question, brute force is the answer, because the security administrator is simply trying to recover the password for the user.

Case Studies for Chapter 11

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

Case Study 11-1: Understanding Risk and Vulnerability

Risk is the possibility of an attack or threat compromising your IT infrastructure. It is normally accomplished by exploiting vulnerabilities in computers, networks, and even people.

Scenario: You work for a medium-sized business with 200 computers and users. The company has experienced extremely fast growth, and until now, has not been concerned with risk. Your task is to define risk to your company, and develop plans to deal with it effectively. The board of directors is interested in finding out the annualized loss expectancy for the company's servers. The board also wishes to have some kind of management plan in place that includes the analyzing of network documentation, and the mitigating of threats and potential compromise.

Question 1: What type of risk assessment should you recommend?

Question 2: Because you don't know exactly what will happen to your company's servers in the future, it is impossible to predict exactly what will happen to them, and when, and how much it will cost. What concept, in addition to your risk assessment method, can aid in this?

Question 3: What kind of management plan should you implement? What basic steps does it entail?

(View the solution to this case study before moving on to the next case study.)

Case Study 11-2: Mapping and Scanning the Network

Scenario: Now that you have developed plans for risk assessment and vulnerability assessment, it's time to get your hands dirty and find out what's actually happening on your network. Your job is to use utilities that will help you identify the servers and other computers on the network, and scan for vulnerabilities on those computers.

Warning: The following should be performed on a closed, test network.

Access the Internet and locate two network mapping programs and two network scanning programs. Look for free utilities, or utilities that have free trials. Download and install those programs, then create a basic map of the network, and define some of the vulnerabilities such as open ports on your computers.

Case Study 11-3: Defending Against Password Cracking

It's been said over and over again—weak passwords can easily be cracked. There are plenty of free tools available on the Internet that can crack a weak password in a matter of seconds.

Scenario: You are in charge of a small peer-to-peer Windows network where people configure their own passwords on computers that have no other configured security than the out-of-the-box security that comes with the operating system. Your task is to test the users' passwords, and set up a way to enforce the usage of complex passwords. You are not allowed to know the current user passwords (unless of course you can crack them!).

Use freely downloadable tools to test accounts (and their passwords). Then define what a complex password is. Finally, explain how you can enforce whether people use complex passwords.

Case Study Solutions

Case Study 11-1 Solution

Remember, solutions to these types of scenarios will vary. The following is one possible solution to the needs of your company.

First, you should recommend a *quantitative* risk assessment. This uses exact monetary values: $SLE \times ARO = ALE$ (the aforementioned annualized loss expectancy).

The problem with quantitative risk assessments is that they are based on the past history of your actual organization. To go beyond this, and perhaps predict the future with a bit more certainty, consider using concepts such as mean time between failures (MTBF). This information can be obtained from the manufacturer of a device. It consists of data gathered from many customers that ultimately shows the average failure time of the device in question. Instead of relying solely on your own data and how costly failures were, you can utilize the data of other customers (anonymous of course) to better find the median, or average, for failures, and predict the future with more clarity.

Finally, you should implement a vulnerability management plan. This means documenting the network, testing the attack surface of servers, scanning systems internally and remotely, mitigating any vulnerabilities you find, and monitoring carefully.

Simulation: Complete the simulations 11-1a, 11-1b, and 11-1c on the accompanying disc.

Case Study 11-2 Solution

Remember to perform these types of tests on a closed network that you are allowed to have access to.

A couple examples of network scanning programs include Network Topology Mapper (previously LANsurveyor) and Spiceworks, but there are others as well. Use what works best for you. Two examples of port scanners are Nessus and Nmap (though these are actually full-blown vulnerability scanners). On a Windows client computer, type in the command `netstat -an`. In the left-hand column you will more than likely find that ports 135 and 139 are open (among many others). Some ports such as these need to be open so the computer can be “networkable.” But other ports might need to be closed. From a remote system, scan the same computer with the Nessus and Nmap programs to find out what ports are visible from the network.

Video Solution: Watch the video solution “11-2: Mapping and Scanning the Network” on the accompanying disc.

Case Study 11-3 Solution

Remember to perform these types of tests on a closed network that you are allowed to have access to.

Passwords can be very insecure out-of-the-box. An account is generally configured with no password by default. In addition, different operating systems have different ways of hashing the password. In fact, in Windows there are multiple ways of hashing, depending on the Windows version and several other factors. (We’ll discuss more about hashing later in the book.) Aside from the lack of default security, users often select very simple passwords such as *love*, *secret*, or the best one, *password*. Those passwords are just about as good as using no password at all. For example, a

four-character password can be cracked by today's password-cracking programs in a matter of seconds.

There are plenty of tools out there that you can download for free and use to check the quality of users' passwords; for example, Cain & Abel, ophcrack, and Rainbow-Crack. Try out some of these programs on a closed network (and a clean machine) and see how they function. You will see that they are designed to use various password-cracking methods (brute force, for example) that are very good at breaking LM and NTLM password hashes in Windows.

In many networks, the chances are you will find a lot of non-complex passwords—ones that can be cracked very easily. How to fix this? Do the following:

- Give the administrator account a complex password. (Also consider making a secondary administrator account—with a complex password—and disabling the original admin account.)
- Disable generic accounts and give them a complex password.
- Set up a policy that governs the type of password that is chosen by users.

Now, that last bullet will vary depending on the type of network. In a small peer-to-peer network that has, say, five or six Windows computers, the policy would have to be configured on one machine, then exported, and imported to the rest of the computers. In this scenario you would go to Run and type `secpol.msc`. That displays the Local Security Policy, and from there you would access Account Policies > Password Policy, where you would enforce complexity and a minimum password length. In a larger network, such as a Windows domain, you would configure the policy based on the OU in question, and/or use the `gpedit.msc` utility.

Video Solution: Watch the video solution "11-3: Defending Against Password Cracking" on the accompanying disc.

This page intentionally left blank



This chapter covers the following subjects:

- **Monitoring Methodologies:** Monitoring the network is extremely important, yet often overlooked by security administrators. In this section, you learn about the various monitoring methodologies that applications and IDS/IPS solutions use.
- **Using Tools to Monitor Systems and Networks:** Here, we delve into the hands-on again. Included in this section are performance analysis tools, such as Performance Monitor, and protocol analysis tools, such as Wireshark and Network Monitor.
- **Conducting Audits:** Full-blown audits might be performed by third-party companies, but you as the security administrator should be constantly auditing and logging the network and its hosts. This section gives some good tips to follow when executing an audit and covers some of the tools you would use in a Windows server to perform audits and log them properly.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 2.3, 3.6, and 3.7.

Monitoring and Auditing

This chapter discusses monitoring and auditing. Key point: Monitoring alone does not constitute an audit, but audits usually include monitoring. So we cover some monitoring methodologies and monitoring tools before we get into computer security audits. This chapter assumes that you have read through Chapter 11, “Vulnerability and Risk Assessment,” and that you will employ the concepts and tools you learned about in that chapter when performing an audit. Chapter 11 and this chapter are strongly intertwined; I broke them into two chapters because there was a bit too much information for just one, and I want to differentiate somewhat between risk and audits. But regardless, these two chapters are all about putting on your sleuthing hat. You might be surprised, but many networking and operating system security issues can be solved by using that old Sherlockian adage: “When you have eliminated the impossible, whatever remains, however improbable, must be the truth.” This process of elimination is one of the cornerstones of a good IT troubleshooter and works well in the actual CompTIA Security+ exam.

Foundation Topics

Monitoring Methodologies

To operate a clean, secure network, you must keep an eye on your systems, applications, servers, network devices, and the entire network in general. One way to do this is to monitor the network. This surveillance of the network in of itself increases the security of your entire infrastructure. By periodically watching everything that occurs on the network, you become more familiar with day-to-day happenings and over time get quicker at analyzing whether an event is legitimate. It can help to think of yourself as Hercule Poirot, the Belgian detective—*seeing* everything that happens on your network, and ultimately *knowing* everything that happens. It might be a bit egotistical sounding, but whoever said that IT people don’t have an ego?

This surveillance can all be done in one of two ways: manual monitoring or automated monitoring. When manually monitoring the network, you are systematically viewing log files, policies, permissions, and so on. But this can also be

automated. For example, there are several data mining programs available that can automatically sift through logs and other files for the exact information you want to know. In addition, applications such as antivirus, intrusion detection systems, and intrusion prevention systems can automatically scan for errors, malicious attacks, and anomalies. The three main types of automated monitoring are signature-based, anomaly-based, and behavior-based. The following acts as a review of the first two types of monitoring and adds the third type: behavior-based monitoring.

Signature-Based Monitoring

In a **signature-based monitoring** scenario, frames and packets of network traffic are analyzed for predetermined attack patterns. These attack patterns are known as signatures. The signatures are stored in a database that must be updated regularly to have any effect on the security of your network. Many attacks today have their own distinct signatures. However, only the specific attack that matches the signature will be detected. Malicious activity with a slightly different signature might be missed. This makes signature-based monitoring vulnerable to false negatives—when an IDS, IPS, or antivirus system fails to detect an actual attack or error. To protect against this, the signature-based system should be updated to bring the system up to date with the latest signatures. When it comes to intrusion detection systems, the most basic form is the signature-based IDS. However, some signature-based monitoring systems are a bit more advanced and use heuristic signatures. These signatures incorporate an algorithm that determines whether an alarm should be sounded when a specific threshold is met. This type of signature is CPU-intensive and requires fine-tuning. For example, some signature-based IDS solutions use these signatures to conform to particular networking environments.

Anomaly-Based Monitoring

An **anomaly-based monitoring** system (also known as statistical anomaly-based) establishes a performance baseline based on a set of normal network traffic evaluations. These evaluations should be taken when the network and servers are under an average load during regular working hours. This monitoring method then compares current network traffic activity with the previously created baseline to detect whether it is within baseline parameters. If the sampled traffic is outside baseline parameters, an alarm will be triggered and sent to the administrator (as long as the system was configured properly). This type of monitoring is dependent on the accuracy of the baseline. An inaccurate baseline increases the likelihood of obtaining false indicators, such as false positives. Normally, false positives are when the system reads a legitimate event as an attack or other error. This can happen with an improperly configured IDS or IPS solution. If too many false indicator alerts are received by the security administrator, then the IDS/IPS should be reconfigured and baselines re-collected, and/or those types of false alarms should be disabled.

Behavior-Based Monitoring

A **behavior-based monitoring** system looks at the previous behavior of applications, executables, and/or the operating system and compares that to current activity on the system. If an application later behaves improperly, the monitoring system will attempt to stop the behavior. This has advantages compared to signature-based and anomaly-based monitoring in that it can to a certain extent help with future events, without having to be updated. However, because there are so many types of applications, and so many types of relationships between applications, this type of monitoring could set off a high amount of false positives. Behavior monitoring should be configured carefully to avoid the system triggering alarms due to legitimate activity. Table 12-1 summarizes the monitoring methods discussed. Keep in mind that some systems (IDS, IPS, and so on) might combine more than one of these monitoring methods.

Table 12-1 Summary of Monitoring Methodologies

Key Topic

Monitoring Methodology	Description
Signature-based monitoring	<p>Network traffic is analyzed for predetermined attack patterns.</p> <p>These attack patterns are known as signatures.</p>
Anomaly-based monitoring	<p>Establishes a performance baseline based on a set of normal network traffic evaluations.</p> <p>Requires a baseline.</p>
Behavior-based monitoring	<p>Looks at the previous behavior of applications, executables, and/or the operating system and compares that to current activity on the system.</p> <p>If an application later behaves improperly, the monitoring system will attempt to stop the behavior.</p> <p>Requires a baseline.</p>

Using Tools to Monitor Systems and Networks

All the methodologies in the world won't help you unless you know how to use some monitoring tools and how to create baselines. By using performance monitoring gizmos and software, incorporating protocol analyzers, and using other analytical utilities in the GUI and the command-line, you can really "watch" the network and quickly mitigate threats as they present themselves.

In this section, we use the Performance tool in Windows, the Wireshark and Network Monitor protocol analyzers, and other analytical tools within the command-line and the GUI. These are just a couple examples of performance and network

monitoring tools out there, but they are commonly used in the field and should give you a decent idea of how to work with any tools in those categories.

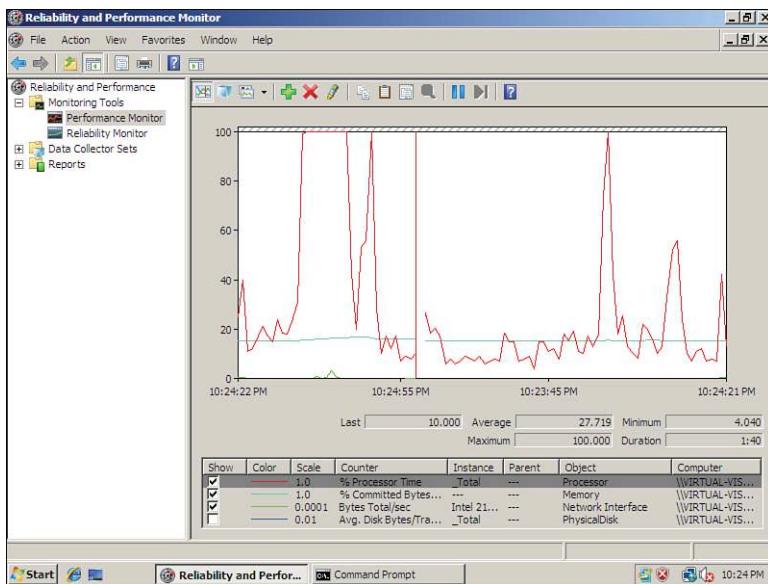
Performance Baselining

We mentioned in Chapter 3, “OS Hardening and Virtualization,” that **baselining** is the process of measuring changes in networking, hardware, software, applications, and so on. Documenting and accounting for changes in a baseline is known as **baseline reporting**. Baseline reporting enables a security administrator to identify the **security posture** of an application, system, or network. The security posture can be defined as the risk level to which a system, or other technology element, is exposed. **Security posture assessments (SPAs)** use baseline reporting and other analyses to discover vulnerabilities and weaknesses in systems.

Let’s get into baselining a little more and show one of the software tools you can use to create a baseline.

Creating a baseline consists of selecting something to measure and measuring it consistently for a period of time. For example, we might want to know what the average hourly data transfer is to and from a server’s network interface. There are a lot of ways to measure this, but we could possibly use a performance monitoring tool or a protocol analyzer to find out how many packets cross through the server’s network adapter. This could be run for 1 hour (during business hours of course) every day for 2 weeks. Selecting different hours for each day would add more randomness to the final results. By averaging the results together, we get a baseline. Then we can compare future measurements of the server to the baseline. This helps us define what the standard load of our server is and the requirements our server needs on a consistent basis. It also helps when installing other like computers on the network. The term *baselining* is most often used to refer to monitoring network performance, but it actually can be used to describe just about any type of performance monitoring. The term *standard load* is often used when referring to servers. A configuration baseline defines what the standard load of the server is for any measured objects. When it comes to performance monitoring applications, objects are all of the components in the server (for example, CPU, RAM, hard disk, and so on). They are measured using counters. A typical counter would be the % Processor Time of the CPU. This is used by the Task Manager.

An example of one of these tools is the Performance Monitor tool in Windows. It can help to create baselines measuring network activity, CPU usage, memory, hard drive resources used, and so on. It should also be used when monitoring changes to the baseline. Figure 12-1 shows an example of Performance Monitor in Windows. The program works basically the same in all version of Windows, be it client or server, but the navigation to the program will vary. To simplify matters, go to the Run prompt and type `perfmon.exe` in Windows to open the program.



Key Topic

Figure 12-1 Performance Monitor in Windows

The CPU is probably the most important component of the computer. In Figure 12-1, the CPU counter has hit 100% several times. If the CPU maxes out often, as it does in the figure, a percentage of clients cannot obtain access to resources on the computer. If the computer is a server, then that means trouble. This CPU spiking that we see could be due to normal usage, or it could be due to malicious activity or perhaps bad design. Further analysis would be necessary to determine the exact cause. If the system is a virtual machine, there is a higher probability of CPU spikes. Proper design of VMs is critical, and they must have a strong platform to run on if they are to serve clients properly. Known as a counter, the CPU % Processor Time is just one of many counters. A smart security auditor measures the activity of other objects such as the hard drive, paging file, memory (RAM), network adapter, and whatever else is specific to the organization's needs. Each object has several counters to select from. For example, if you are analyzing a web server, you would probably want to include the HTTP Service Request Queries object, and specifically the ArrivalRate and CurrentQueueSize counters, in your examination.

Now, Figure 12-1 shows the Performance Monitor screen, but this only gives us a brief look at our system. The window of time is only a minute or so before the information refreshes. However, we can record this information over x periods of time and create reports from the recorded information. By comparing the Performance Monitor reports and logs, we ultimately create the baseline. The key is to measure the same way at the same time each day or each week. This provides accurate

comparisons. However, keep in mind that performance recording can be a strain on resources. Verify that the computer in question can handle the tests first before you initiate them.

Making reports is all fine and good (and necessary), but it is wise to also set up alerts. Alerts can be generated automatically by the system and sent to administrators and other important IT people. These alerts can be set off in a myriad of ways, all of your choosing; for example, if the CPU were to trip a certain threshold or run at 90% for more than a minute (although this is normal in some environments). Or maybe the physical disk was peaking at 100 MB/s for more than 5 minutes. If these types of things happen often, the system should be checked for malicious activity, illegitimate usage, or the need for an upgrade.

A tool similar to Performance Monitor used in Linux systems is called System Monitor. The different versions of Linux also have many third-party tools that can be used for performance monitoring. OS X uses Activity Monitor.

Protocol Analyzers

We've mentioned protocol analyzers a couple of times already in this book but haven't really delved into them too much. There are many protocol analyzers available, some free, some not, and some that are part of an operating system. In this section, we focus on two: Wireshark and Network Monitor. Note that network adapters can work in one of two different modes:

- **Promiscuous mode:** The network adapter captures all packets that it has access to regardless of the destination of those packets.
- **Non-promiscuous mode:** The network adapter captures only the packets addressed to it specifically.

Packet capturing programs have different default settings for these modes. Some programs and network adapters can be configured to work in different modes.

Protocol analyzers can be useful in diagnosing where broadcast storms are coming from on your LAN. A **broadcast storm** (or extreme broadcast radiation) is when there is an accumulation of broadcast and multicast packet traffic on the LAN coming from one or more network interfaces. These storms could be intentional or could happen due to a network application or operating system error. The protocol analyzer can specify exactly which network adapter is causing the storm.

Protocol analyzers are also effective in finding header manipulation. Header manipulation can be accomplished by entering unvalidated data into the header of a packet and can ultimately enable XSS attacks, poisoning attacks, hijacking, and cookie manipulation. Header manipulation is common in HTTP response packets.

The exploit can be prevented/corrected with proper input validation and detected with a protocol analyzer.

Protocol analyzers can look inside a packet that makes up a TCP/IP handshake. Information that can be viewed includes the SYN, which is the “synchronized sequence numbers,” and the ACK, which is “acknowledgment field significant.” By using the protocol analyzer to analyze a TCP/IP handshake, you can uncover attacks such as TCP hijacking. But that is just one way to use a protocol analyzer to secure your network. Let’s talk about a couple protocol analyzers now.

Wireshark

Wireshark (previously known as Ethereal) is a free download that works on several platforms including Windows and Windows portables, Linux, Unix, and OS X. It is meant to capture packets on the local computer that it is installed on. But often, this is enough to find out vulnerabilities and monitor the local system and remote systems such as servers. Because Wireshark works in promiscuous mode, it can delve into packets even if they weren’t addressed to the computer it runs on. To discern more information about the remote systems, simply start sessions from the client computer to those remote systems and monitor the packet stream. If that is not enough, the program can be installed on servers as well. However, you should check company policy (and get permission) before ever installing any software on a server.

Imagine that you were contracted to find out whether an organization’s web server was transacting secure data utilizing TLS version 1.0. But the organization doesn’t want anyone logging in to the server—all too common! No problem; you could use Wireshark on a client computer, initiate a packet capture, make a connection to the web server’s secure site, and verify that TLS 1.0 is being used by analyzing the packets, as shown in Figure 12-2. If you saw other protocols such as SSL 2.0 that should happen to raise a red flag, then you would want to investigate further, most likely culminating in a protocol upgrade or change.

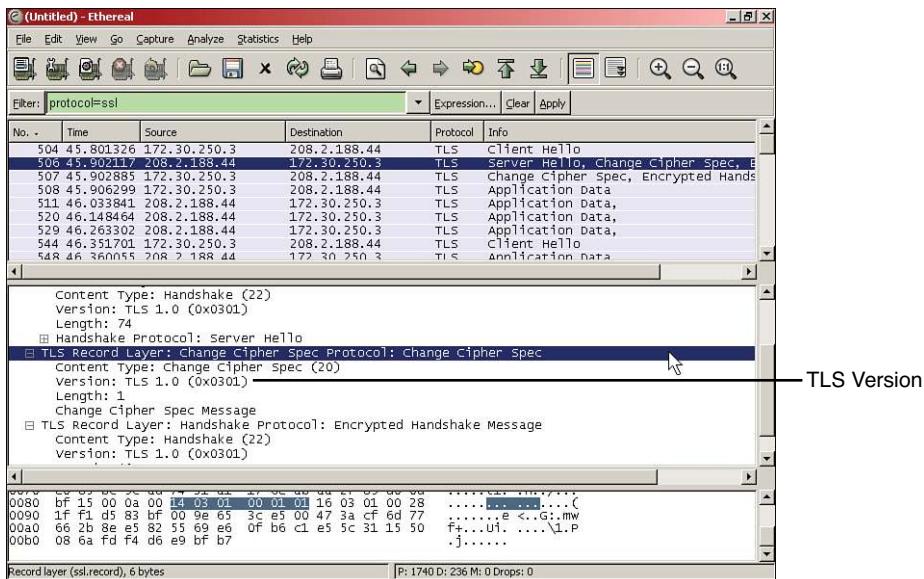


Figure 12-2 Wireshark Showing a Captured TLS Version 1.0 Packet

Always take screen captures and save your analysis as proof of the work that you did, and as proof of your conclusions and ensuing recommendations. You can also save the packet capture file (with the .pcap extension) for future analysis.

Remember that Wireshark can be used with a network adapter configured for promiscuous mode. It is set up by default to collect packets locally and from other sources.

Network Monitor

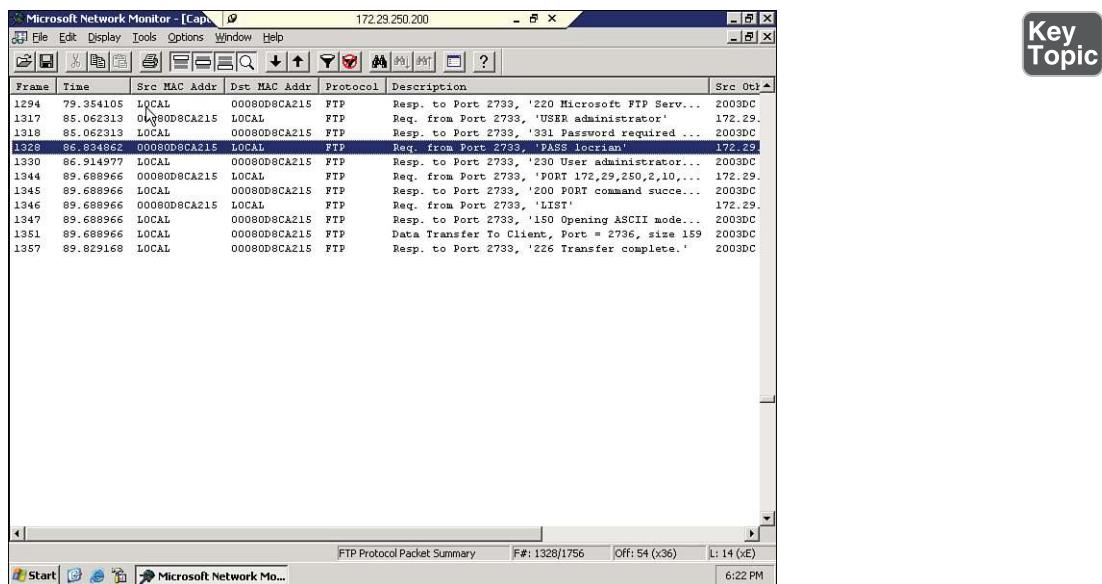
Network Monitor is a built-in network sniffer used in Windows Server products. Called netmon for short, it behaves in basically the same fashion as Wireshark. However, built-in versions of Network Monitor up until Windows Server 2003 work in non-promiscuous mode by default. The full version of the program (available with SCCM or the older SMS Server) can also monitor network adapters on remote computers. For now, we'll stick to the default Network Monitor version that comes stock with Windows Server 2003 and higher.

NOTE You can run Network Monitor from the Run prompt by typing `netmon.exe`. You can download Network Monitor 3.4 for Windows clients (for example, Windows 7) from the following link:
<http://www.microsoft.com/en-us/download/details.aspx?id=4865>

NOTE Microsoft also offers the newer Microsoft Message Analyzer, which can trace and assess system events and messages, in addition to capturing packets. It is available for download at this link:

<http://www.microsoft.com/en-us/download/details.aspx?id=40308>

How about another real-world example? Let's just say you were contracted to monitor an FTP server. The organization is not sure whether FTP passwords are truly being encrypted before being sent across the network. (By the way, some FTP programs with a default configuration do not encrypt the password.) You could use the Network Monitor program to initiate a capture of packets on the monitoring server. Then, start up an FTP session on the monitoring server and log in to the FTP server. Afterward, stop the capture and view the FTP packets. Figure 12-3 shows an example of an FTP packet with a clear-text password. Notice that frame 1328 shows the password "locrian" in the details.



Key Topic

Figure 12-3 Network Monitor Showing a Captured FTP Packet with Clear-Text Password

This particular connection was made with the default FTP client within the Microsoft Command Prompt of a Windows Server to a built-in FTP server on a separate Windows Server set up with a default configuration. However, you could discern the same information by using Wireshark on a client computer and logging in to the FTP server from that client computer.

Clear-text passwords being passed across the network is a definite risk. The vulnerabilities could be mitigated by increasing the level of security on the FTP server and by using more secure programs. For example, if the FTP server were part of Windows IIS, domain-based or other authentication could be implemented. Or perhaps a different type of FTP server could be used, such as Pure-FTPd. And secure FTP client programs could be used as well. Instead of using the Command Prompt or a browser to make FTP connections, the FileZilla or WS_FTP programs could be used.

NOTE See Case Study 12-1 at the end of the chapter to learn more about Wireshark and protocol analyzers in general.

SNMP

The **Simple Network Management Protocol (SNMP)** is a TCP/IP protocol that aids in monitoring network-attached devices and computers. It's usually incorporated as part of a network management system, such as Windows SMS, or free software, such as Net-SNMP. A typical scenario that uses SNMP can be broken down into three components:

- **Managed devices:** Computers or other network-attached devices monitored through the use of agents by a network management system.
- **Agent:** Software deployed by the network management system that is loaded on managed devices. The software redirects the information that the NMS needs to monitor the remote managed devices.
- **Network management system (NMS):** The software run on one or more servers that controls the monitoring of network-attached devices and computers.

So, if the IT director asked you to install agents on several computers and network printers, and monitor them from a server, this would be an example of SNMP and the use of a network management system.

SNMP uses ports 161 and 162. SNMP agents receive requests on port 161; these requests come from the network management system or simply “manager.” The manager receives notifications on port 162.

Because applications that use SNMP versions 1 and 2 are less secure, they should be replaced by software that supports SNMP version 3. SNMPv3 provides confidentiality through the use of encrypted packets that prevent snooping and provide additional message integrity and authentication.

Analytical Tools

In this book we try to distinguish between monitoring, auditing, vulnerability assessment, and forensics, but from a hands-on point of view, they are all quite similar. Many analytical tools can be used for multiple security purposes. This section discusses a few more tools that are more fine-tuned for monitoring, but that doesn't mean that they can't be used for other security purposes; and there are plenty of other tools not mentioned here that can also be used for monitoring.

You will probably want to monitor open sessions and files. In Windows, any files and shares that are being accessed by remote computers can be monitored within Computer Management (Run > compmgmt.msc). Inside Computer Management, navigate to System Tools > Shared Folders. From there you can see what shares and open files are being accessed, and what network sessions are open to that computer.

NOTE On some versions of Windows the Performance Monitor utility (discussed previously) can also be found within Computer Management.

One thing you can't see in this utility is the files that were opened locally. But for this you can use the `openfiles` command, which also allows you to see files opened by remote computers. The `openfiles` command must be run in elevated mode within the Command Prompt, and by default the Maintain Objects List global flag must be enabled, which can be done with the following syntax:

```
openfiles /local on
```

Then, simply run the `openfiles` command to see what files are opened locally, and by remote computers, as shown in Figure 12-4. Of course, there are switches that you can use to modify the command; view them with the `/?` option.

```

C:\Administrator: Command Prompt
528 WINWORD.EXE C:\..\AppData\Local\Temp\~DF3A0BF75EBAA706E3.TMP
544 WINWORD.EXE C:\..\Content.Word\~WRS0000.tmp
728 WINWORD.EXE C:\..\ie18e3b_8_0.50727..6195_none_cbf5e994470a1a8f
732 WINWORD.EXE C:\..\ie18e3b_8_0.50727..6195_none_d09154e044272b9a
736 WINWORD.EXE C:\..\ie18e3b_8_0.50727..6195_none_03ce2c72205943d3
740 WINWORD.EXE C:\..\Nuance\NaturallySpeaking10\Program
744 WINWORD.EXE C:\..\ie18e3b_8_0.50727..6195_none_d09154e044272b9a
760 WINWORD.EXE C:\..\ie18e3b_8_0.50727..6195_none_d09154e044272b9a
820 WINWORD.EXE C:\..\TechSmith\Snagit 8\Snagit Hdd-in.dot
832 WINWORD.EXE C:\..\Microsoft Office\OFFICE11\NSWORD.OLB
846 WINWORD.EXE C:\..\AppData\Local\Temp\~DFC4332B179C989456.TMP
848 WINWORD.EXE C:\..\4ccfd1f_6_0.7600.16385_none_421189da2b7fabfc
1016 WINWORD.EXE D:\..\Chapters\CH12_Monitoring_and_Auditing.doc
1032 WINWORD.EXE C:\..\AppData\Local\Temp\~DFBBFF63EF4EB472B91.TMP
1040 WINWORD.EXE
1044 WINWORD.EXE C:\..\AppData\Local\Temp\~DF842CE9DB3B60B946.TMP
1116 WINWORD.EXE C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
1120 WINWORD.EXE C:\..\Microsoft shared\PROF\MSHV2_EN.LEX
1132 WINWORD.EXE C:\..\Content.Word\~WRF0001.tmp
1144 WINWORD.EXE C:\PROGRA~2\COMMON\1\MICROS~1\UBA\UBA6\UBE6.DLL
1152 WINWORD.EXE C:\PROGRA~2\COMMON\1\MICROS~1\UBA\UBA6\UBE6.DLL
1160 WINWORD.EXE C:\..\Microsoft shared\OFFICE11\MSO.DLL
1168 WINWORD.EXE C:\Windows\SysWOW64\stdole2.tlb
1204 WINWORD.EXE C:\PROGRA~2\COMMON\1\MICROS~1\SMARTIT\1\FPERSON.DLL
1212 WINWORD.EXE C:\PROGRA~2\COMMON\1\MICROS~1\SMARTIT\1\FSSTOCK.DLL
1224 WINWORD.EXE C:\PROGRA~2\COMMON\1\MICROS~1\SMARTIT\1\MOPL.DLL
1296 WINWORD.EXE C:\..\MICROS~1\SMARTIT\1\LISTS\1033 STOCKS.DAT
1316 WINWORD.EXE C:\PROGRA~2\COMMON\1\MICROS~1\SMARTIT\1\FDATE.DLL
1324 WINWORD.EXE C:\PROGRA~2\COMMON\1\MICROS~1\SMARTIT\1\FPLACE.DLL
1528 WINWORD.EXE C:\..\Microsoft shared\PROF\MSSP3EN.LEX
1532 WINWORD.EXE C:\PROGRA~2\COMMON\1\MICROS~1\SMARTIT\1\FNAME.DLL
8 openfiles.exe C:\Windows\System32
64 openfiles.exe C:\Windows\System32\en-US\openfiles.exe.mui

Files opened remotely via local share points:

ID Accessed By Type Open File <Path\executable>
----- -----
2 Lamprokes Windows D:\Data_Main\
35 Lamprokes Windows D:\Data_Main\Pearson
56 Lamprokes Windows D:\..\Pearson\Security+_CG_3rd-ed
66 Lamprokes Windows D:\..\Security+_CG_3rd-ed\Chapters
80 Lamprokes Windows D:\..\_dies - Videos - Simulations.doc
113 Lamprokes Windows D:\Data_Main\
139 Lamprokes Windows D:\..\Chapters\Thumbs.db
146 Lamprokes Windows D:\..\ded Resources - PDF on disc.doc
409 Lamprokes Windows D:\..\ded Resources - PDF on disc.doc

C:\Windows\system32>

```

Figure 12-4 openfiles Command Results in Windows

You might have to increase the screen buffer for the Command Prompt to see all of the results. As you can see in the figure, there is a long list of locally accessed files, but more importantly, the second list (starting with ID 2) shows any files that remote computers are connected to. You can also use `openfiles` to disconnect those remote computers. Example syntax for this is

```
openfiles /disconnect /id ##
```

where ## is the ID number associated with the file, shown at the left of the figure.

You might also find that files have been opened and possibly compromised. When you are not sure if the integrity of a file (or files) has been affected, you can use the `FC` command to compare the file that is suspected of compromise with an older version of the file.

Files can also be viewed and closed with the `net file` command (must be run in elevated mode). You'll probably also want to make use of the `net config`, `net session`, and `net view` commands. Better yet—just know the whole `net` command

like the back of your hand. And of course there's the `netstat` command; for example, `netstat -an` is a good way to show open ports in numeric format, and `netstat -e` gives the amount of bytes and packets (and errors) sent and received.

We previously mentioned a few commands in Linux that can be used to view processes, services, and open files. Another command that can be used to show open files is `lsof` (list openfiles). The `netstat` command functions similarly in Linux as it does in Windows (with `netstat -l` being very informative).

Changing gears somewhat: What makes up a lot of the files stored on servers? Individual keystrokes—a bunch of them. And these too can be monitored, with keyloggers—both hardware-based and software-based. The hardware variety is usually an inline (or pass-through) device that connects to the end of a keyboard's cable just before the port on the computer. These are tricky little devices that often look like a basic adapter. But in reality they are fairly expensive devices that can store gigabytes of data and can transmit data wirelessly. You can identify a potential keylogger by the fact that it has the same port on each end, albeit one male and one female. Often they are heavier than a basic adapter of similar size due to the additional processors and the antenna that are built in. The basic countermeasure for these is to deny physical access to areas of the building with important data, such as server rooms. If people have free access to your building, then there is a definite vulnerability. As a security administrator, you should lobby against such access, but if it is inescapable, then a thorough visual search of computers should be periodically undertaken. Sometimes, a computer's ports cannot be visualized very easily, but have no fear, there are software tools that can be used to locate these physical keyloggers as well. Speaking of software tools, keyloggers come in software format as well, and some are very difficult to detect (such as Actual Keylogger). These software tools can be prevented by using anti-keylogger software and security tokens. They can be detected through the use of live CD/DVD operating systems and network monitoring programs.

The list of analytical tools goes on and on, both integrated into the operating system and offered by third parties. Most of the analytical tools discussed in this section are static in nature. Because of this they are not best suited for monitoring environments where you are attempting to create a baseline. Other, more dynamic tools such as Performance Monitor and Wireshark will work better. However, there is something to be said about taking a snapshot of the moment with tools such as `openfiles` and getting a quick glimpse at what happened at just that moment. Taking it to the next level, it's the combination of static *and* dynamic tools that will allow you to properly conduct an audit.

Conducting Audits

Computer security audits are technical assessments conducted on applications, systems, or networks. They are an example of a detective security control. Audits can be done manually or with computer programs. Manual assessments usually include the following:

- Review of security logs
- Review of access control lists
- Review of user rights and permissions
- Review of group policies
- Performance of vulnerability scans
- Review of written organization policies
- Interviewing organization personnel

Programs used to audit a computer or network could be as simple as a program such as Belarc Advisor to more complex programs such as Nsauditor to open source projects such as OpenXDAS.

When I have conducted IT security audits in the past, the following basic steps have helped me organize the entire process:

Step 1. Define exactly what is to be audited.

Step 2. Create backups.

Step 3. Scan for, analyze, and create a list of vulnerabilities, threats, and issues that have already occurred.

Step 4. Calculate risk.

Step 5. Develop a plan to mitigate risk and present it to the appropriate personnel.

Although an independent security auditor might do all these things, a security administrator will be most concerned with the auditing of files, logs, and systems security settings.

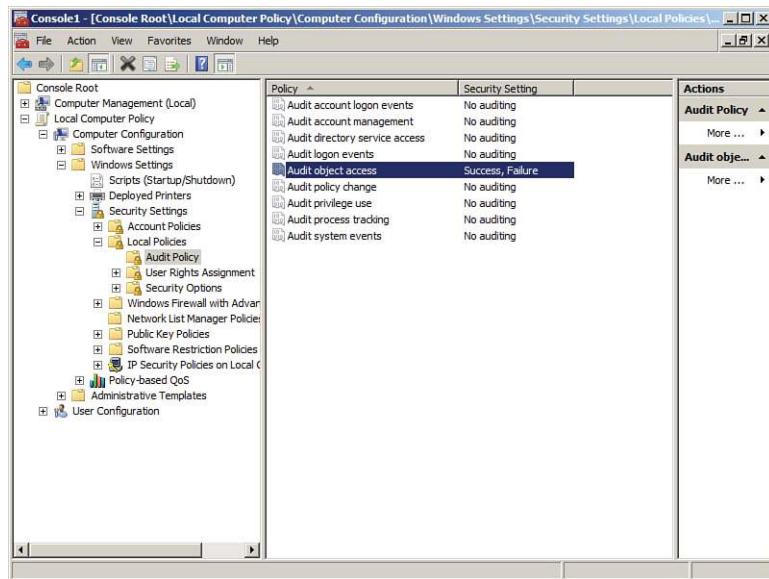
Auditing Files

When dealing with auditing, we are interested in the who, what, and when. Basically, a security administrator wants to know *who* did *what* to a particular resource and *when* that person did it.

Auditing files can usually be broken down into a three-step process:

- Step 1.** Turn on an auditing policy.
- Step 2.** Enable auditing for particular objects such as files, folders, and printers.
- Step 3.** Review the security logs to determine who did what to a resource and when.

As an example, let's use a Windows client computer. First, we would need to turn on a specific auditing policy such as "audit object access." This can be done within the Local Computer Policy, as shown in Figure 12-5. You can select from several different auditing policies such as logon events and privilege use, but object access is probably the most common, so we'll use that as the example.



Key Topic

Figure 12-5 Audit Policy Within the Local Computer Policy of a Windows Computer

Next, we would need to enable auditing for particular objects. Let's say that we are auditing a folder of data. We would want to go to the Properties dialog box for that folder, then navigate to the Security tab, then click the Advanced button, and finally access the Auditing tab, as shown in Figure 12-6.

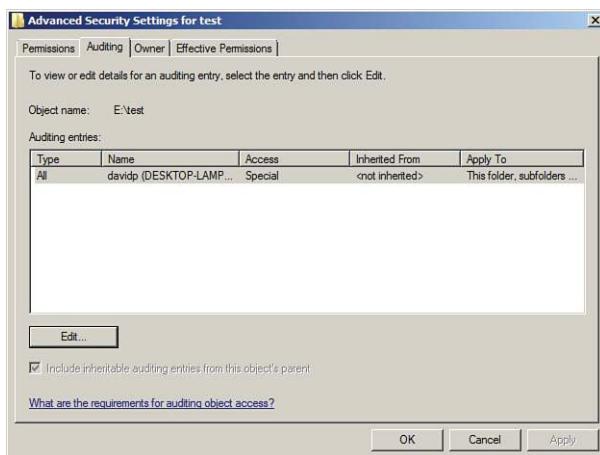


Figure 12-6 Auditing Advanced Security Settings for a Folder in Windows

From there, we can add users that we want to audit, and we can specify one or more of many different attributes to be audited.

Finally, we need to review the security logs to see exactly what is happening on our system and who is accessing what and when. The security logs also tell us whether users have succeeded or failed in their attempts to access, modify, or delete objects. And if users deny that they attempted to do something, these logs act as proof that their user account was indeed involved. This is one of several ways of putting *non-repudiation* into force. Non-repudiation is the idea of ensuring that a person or group cannot refute the validity of your proof against them.

A common problem with security logs is that they fail to become populated, especially on older systems. If users complain to you that they cannot see any security events in the Event Viewer, you should ask yourself the following:

- Has auditing been turned on in a policy? And was it turned on in the correct policy?
- Was auditing enabled for the individual object?
- Does the person attempting to view the log have administrative capabilities?

In addition, you have to watch out for overriding policies. By default, a policy gets its settings from a parent policy; you might need to turn off the override option. On another note, perhaps the audit recording failed for some reason. Many auditing systems also have the capability to send an alert to the administrator in the case that a recording fails. Hopefully, the system attempts to recover from the failure and continue recording auditing information while the administrator fixes the issue. By

answering all these questions and examining everything pertinent to the auditing scenario, you should be able to populate that security log! Now, security logs are just one component of logging that we cover in the next section.

Logging

When it comes to auditing an organized set of information, logging is the method of choice. Frequent monitoring of logs is an important part of being a security person. Possibly the most important log file in Windows is the Security log, as shown in Figure 12-7.

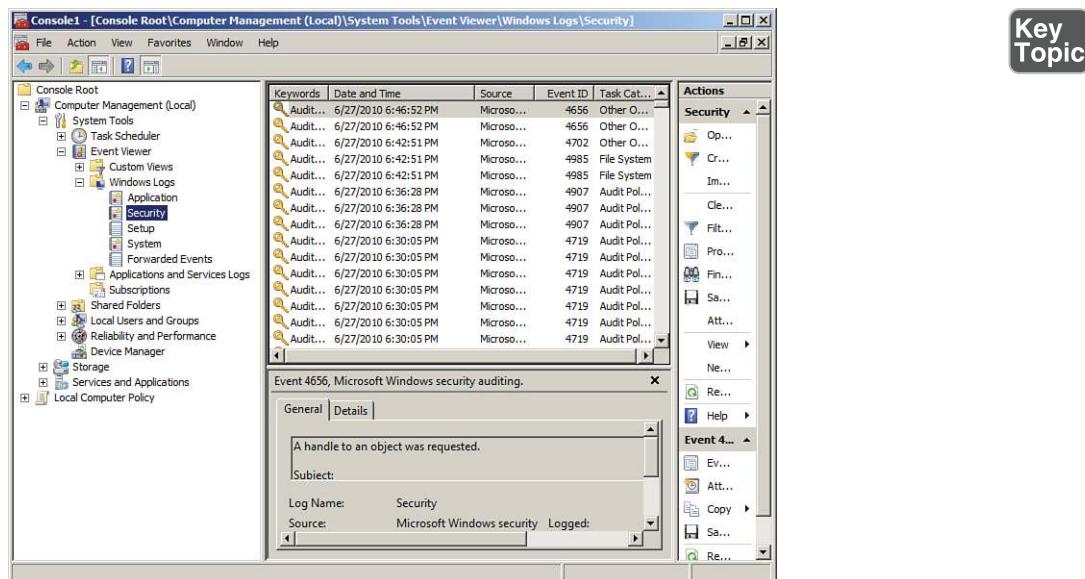


Figure 12-7 Security Log in Windows

The Security log can show whether a user was successful at doing a variety of things, including logging on to the local computer or domain; accessing, modifying, or deleting files; modifying policies; and so on. Of course, many of these things need to be configured first before they can be logged. Newer versions of Windows automatically log such events as logon or policy modification. All these Security log events can be referred to as **audit trails**. Audit trails are records or logs that show the tracked actions of users, whether the user was successful in the attempt or not.

A security administrator should monitor this log file often to keep on top of any breaches, or attempted breaches, of security. By periodically reviewing the logs of applications, operating systems, and network devices, we can find issues, errors, and threats quickly and increase our general awareness of the state of the network.

Several other types of Windows log files should be monitored periodically, including the following:

- **System:** Logs events such as system shutdown or driver failure
- **Application:** Logs events for operating system applications and third-party programs

The System and Application logs exist on client and server versions of Windows. A few log files that exist only on servers include the following:

- File Replication Service
- DNS Server
- Directory Service

The File Replication Service log exists on all Windows Servers, the Directory Service log will appear if the server has been promoted to a domain controller, and the DNS Server log will appear only if the DNS service has been installed to the server. We've mentioned the importance of reviewing DNS logs previously in the book but it is worth reminding you that examining the DNS log can uncover unauthorized zone transfers and other malicious or inadvertent activity on the DNS server. And let's not forget about web servers—by analyzing and monitoring a web server, you can determine whether the server has been compromised. Drops in CPU and hard disk speed are common indications of a web server that has been attacked. Of course, it could just be a whole lot of web traffic! It's up to you to use the log files to find out exactly what is going on.

Other types of operating systems, applications, and devices have their own set of log files—for example, applications such as Microsoft Exchange and SQL database servers, and firewalls. The firewall log especially is of importance, as shown in Figure 12-8. Note in the figure the dropped packets from addresses on the 169.254.0.0 network, which we know to be the APIPA network number. This is something that should be investigated further because most organizations have a policy against the use of APIPA addresses.

LOG DETAILS		
Priority	Time	Message
511 Log Entries:		
[INFO]	Sun Jun 27 22:15:25 2010	Allowed configuration authentication by IP address 10.254.254.205
[INFO]	Sun Jun 27 22:15:17 2010	Dropped packet from 169.254.246.127 to 169.254.255.255 (IP protocol 17) as unable to create new session
[INFO]	Sun Jun 27 22:14:55 2010	Blocked incoming TCP connection request from 202.102.234.71:12200 to 216.164.145.27:1080
[INFO]	Sun Jun 27 22:14:54 2010	Blocked incoming TCP connection request from 202.102.234.71:12200 to 216.164.145.27:3246
[INFO]	Sun Jun 27 22:14:53 2010	Blocked incoming TCP connection request from 202.102.234.71:12200 to 216.164.145.27:9415
[INFO]	Sun Jun 27 22:14:12 2010	Dropped packet from 169.254.246.127 to 169.254.255.255 (IP protocol 17) as unable to create new session

Figure 12-8 A Basic Firewall's Log

The firewall log can show all kinds of other things such as malicious port scans and other vulnerability scans. For example, when digging into a firewall log event, if you see the following syntax, you would know that a port scan attack has occurred:

```
S=207.50.135.54:53 – D=10.1.1.80:0  
S=207.50.135.54:53 – D=10.1.1.80:1  
S=207.50.135.54:53 – D=10.1.1.80:2  
S=207.50.135.54:53 – D=10.1.1.80:3  
S=207.50.135.54:53 – D=10.1.1.80:4  
S=207.50.135.54:53 – D=10.1.1.80:5
```

Note the source IP address (which is public and therefore most likely external to your network) uses port 53 outbound to run a port scan of 10.1.1.80, starting with port 0 and moving on from there. The firewall is usually the first line of defense, but even if you have an IDS or IPS in front of it, you should review those firewall logs often.

A very useful tool for the security administrator is Syslog. Syslog is the standard for computer message logging. Most devices such as switches, routers, and firewalls use it, or can be updated to use it. For example, the log in Figure 12-8 was generated while adhering to the Syslog protocol. In addition, that log can be exported in real time to a computer running a Syslog server. The Syslog server is really just a repository for the logs that already exist on your routers and other devices. The key is that the Syslog server can run directly on your workstation, and pull the logs from those devices, so that you can easily monitor what is happening on those devices from the comfort of your seat. Yes, you could check the logs by logging in to the router or other device, but the logs won't be readily available; you will have to locate them, and different devices will store them in different places. With a Syslog server, you can view multiple devices' logs from one screen.

To illustrate this technology in action, take a look at Figure 12-9. This shows a Syslog program that is getting a log fed to it from a SOHO router. You can see that it is very easy to read the details of that log within the Syslog program; much easier than it would be to read them from within the SOHO router's interface.

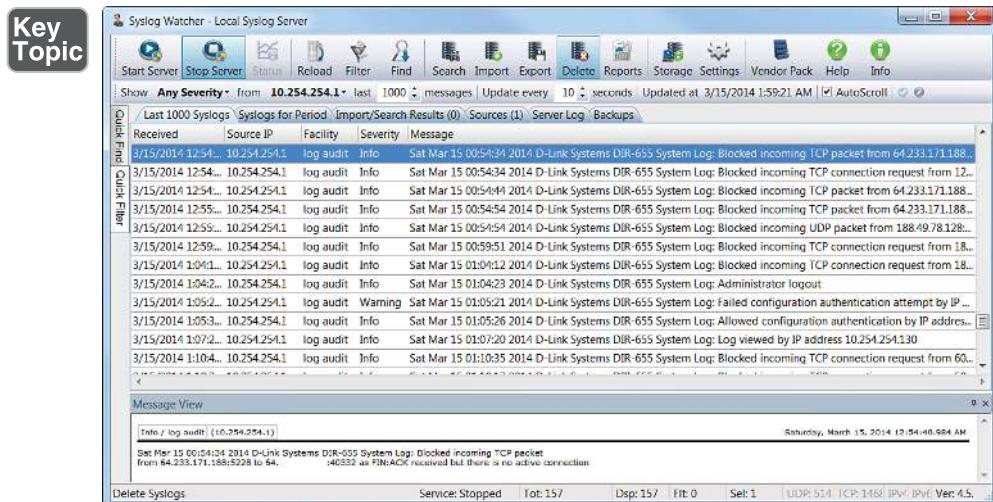


Figure 12-9 Syslog Program Running in Windows Detailing a SOHO Router Log

Figure 12-9 shows a list of logs. The one at the top is highlighted. It shows that the Source IP is 10.254.254.1. That is the internal IP address of the SOHO router—the device that is creating the log, and the one that is being monitored. The highlighted entry also has details at the bottom of the screen. You can see that the SOHO router blocked a TCP packet from the IP address 64.233.171.188 (in this case from port 5228). This is real, and it happens all the time as you can see from the log. It really reinforces the fact that you need to make sure your router (or other device) has its ports closed, and is patched and up to date!

By default, Syslog uses port 514 and works over a UDP transport mechanism. There are several companies that offer Syslog programs (SolarWinds Kiwi and Syslog Watcher, for example), and they all work in basically the same way, though some use a proprietary port number instead of the standard 514, and may offer TCP connectivity as well, to avoid packet loss. Port 6514 is used for secure connections known as Syslog over TLS.

NOTE Though Windows does not by default support exporting of logs to a Syslog server, there are utilities you can download that will convert event logs from the Event Viewer into Syslog messages.

Log File Maintenance and Security

The planning, maintenance, and security of the log files should be thoroughly considered. A few things to take into account include the configuration and saving of the log files, backing up of the files, and securing and encrypting of the files.

Before setting up any type of logging system, you should consider the amount of disk space (or other form of memory) that the log files will require. You should also contemplate all the different information necessary to reconstruct logged events later. Are the logs stored in multiple locations? Were they encrypted? Were they hashed for integrity? Also up for consideration is the level of detail you will allow in the log. Verbose logging is something that admins apply to get as much information as possible. Also, is the organization interested in exactly when an event occurred? If so, time stamping should be incorporated. Although many systems do this by default, some organizations opt to not use time stamping to reduce CPU usage.

Log files can be saved to a different partition of the logging system, or saved to a different system altogether; although, the latter requires a fast secondary system and a fast network. The size and overwriting configuration of the file should play into your considerations. Figure 12-10 shows an example of the properties of a Windows Server Security log file. Currently, the file is 640 KB but can grow to a maximum size of 131072 KB (128 MB). Although 128 MB might sound like a lot, larger organizations can eat that up quickly because they will probably audit and log a lot of user actions. When the file gets this big, log mining becomes important. There can be thousands and thousands of entries, making it difficult for an admin to sort through them all, but several third-party programs can make the mining of specific types of log entries much simpler. You can also note in the figure that the log is set to overwrite events if the log reaches its maximum size. Security is a growing concern with organizations in general, so the chances are that they will not want events overwritten. Instead, you would select Do Not Overwrite Events (Clear Log Manually). As an admin, you would save and back up the log monthly or weekly, and clear the log at the beginning of the new time period to start a new log. If the log becomes full for any reason, you should have an alert set up to notify you or another admin.

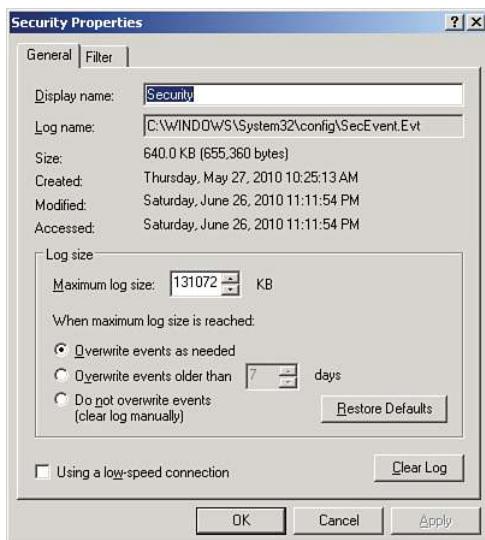


Figure 12-10 Windows Server Security Log Properties Dialog Box

As with any security configurations or files, the log files should be backed up. The best practice is to copy the files to a remote log server. The files could be backed up to a separate physical offsite location. Or, WORM (write-once read-many) media types could be utilized. WORM options such as CD-R and DVD-R are good ways to back up log files, but not *re*-write optical discs, mind you. USB Flash drives and USB removable hard drives should not be allowed in any area where a computer stores log files. One way or another, a retention policy should be in place for your log files—meaning they should be retained for future reference.

Securing the log files can be done in several ways: First, by employing the aforementioned backup methods. Second, by setting permissions to the actual log file. Figure 12-10 shows the filename for the Security log: SecEvent.Evt, located in C:\Windows\system32\config. That is the file you would access to configure NTFS permissions. Just remember that by default, this file inherits its permissions from the parent folder. File integrity is also important when securing log files. Encrypting the log files through the concept known as hashing is a good way to verify the integrity of the log files if they are moved and/or copied. And finally, you could flat-out encrypt the entire contents of the file so that other users cannot view it. We talk more about hashing and encryption in Chapter 13, “Encryption and Hashing Concepts,” and Chapter 14, “PKI and Encryption Protocols.”

Auditing System Security Settings

So far, we have conducted audits on object access and log files, but we still need to audit system security settings. For example, we should review user permissions and group policies.

For user access, we are most concerned with shared folders on the network and their permissions. Your file server (or distributed file system server) can easily show you all the shares it contains. This knowledge can be obtained on a Windows Server by navigating to Computer Management > System Tools > Shared Folders > Shares, as shown in Figure 12-11.

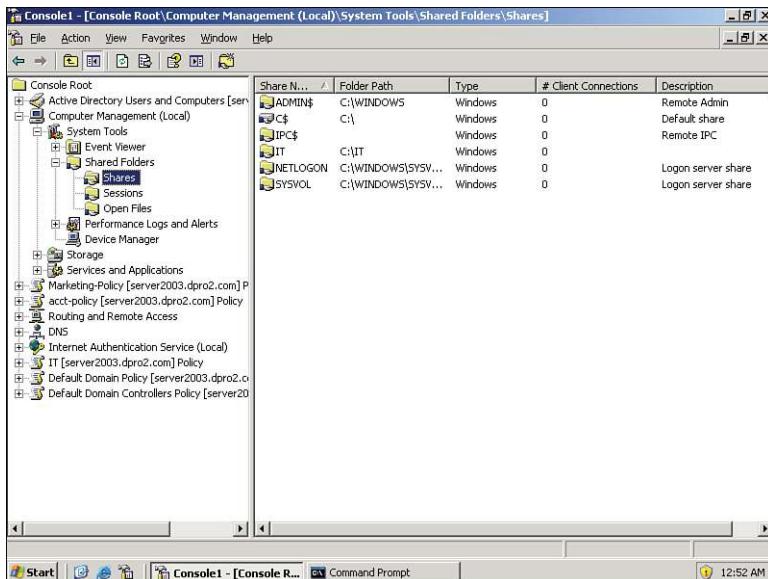


Figure 12-11 Network Shares on a Windows Server

Notice the IT share. There are a couple of things that pique my interest from the get-go. For starters, the shared folder is located in the C: drive of this server. Shared folders should actually be on a different partition, drive, or even a different computer. Second, it is in the root. That isn't a good practice either (blame the author). Of course, this is just a test folder that we created previously, but we should definitely consider the location of our shared folders.

NOTE Some companies opt to secure administrative shares, such as IPC\$ and Admin\$. Although this isn't actually an option on servers, it is a smart idea for client computers.

Either way, we now know where the IT share is located and can go to that folder in Windows Explorer (or File Explorer) and review the permissions for it, as shown in Figure 12-12.

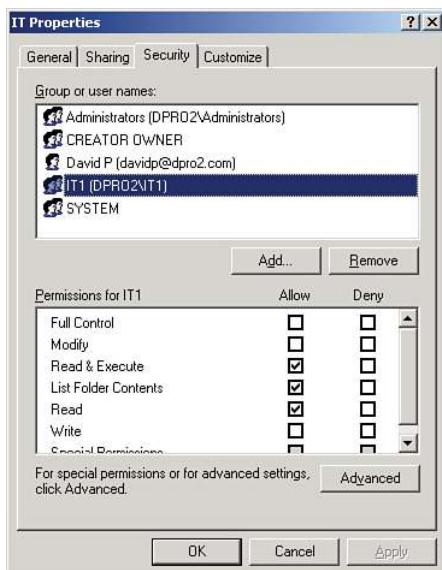


Figure 12-12 The IT Folder's Permissions

In the figure, you can see that the IT1 group has Read & Execute, List Folder Contents, and Read permissions. It is wise to make sure that individual users and groups of users do not have more permissions than necessary, or allowed. It is also important to verify proper ownership of the folder; in this example it can be done by clicking the Advanced button and selecting the Owner tab. Figure 12-13 shows that the Administrator is the owner of this resource. We want to make sure that no one else has inadvertently or maliciously taken control.

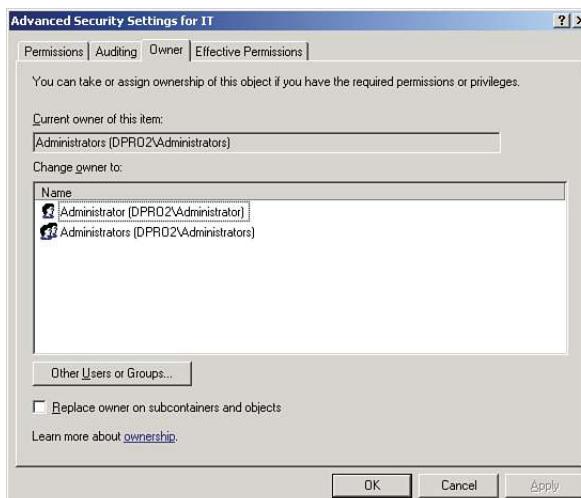


Figure 12-13 The IT Folder's Owner Tab in Advanced Security Settings

While you are in the Advanced Security Settings dialog box, you can check what auditing settings have been implemented and whether they correspond to an organization's written policies.

Speaking of policies, computer policies should be reviewed as well. Remember that there might be different policies for each department in an organization. This would match up with the various organizational units on a Windows Server. Figure 12-14 shows the Security Settings section of the IT Policy we created earlier in the book. I haven't counted them, but there are probably thousands of settings. Due to this, an organization might opt to use a security template; if this is the case, verify that the proper one is being used, and that the settings included in that template take into account what the organization has defined as part of its security plan. Templates are accessed by right-clicking Security Settings and selecting Import Policy. If a template is not being used, you will need to go through as many policy objects as possible, especially things such as password policy, security options, and the audit policy itself.

Individual computers will probably use User Account Control and adhere to the policies created on the server. A spot check should be made of individual computers to verify that they are playing by the rules. In some cases, an organization will require that all client computers are checked. Auditing can be a lot of work, so plan your time accordingly, and be ready for a few hiccups along the way.

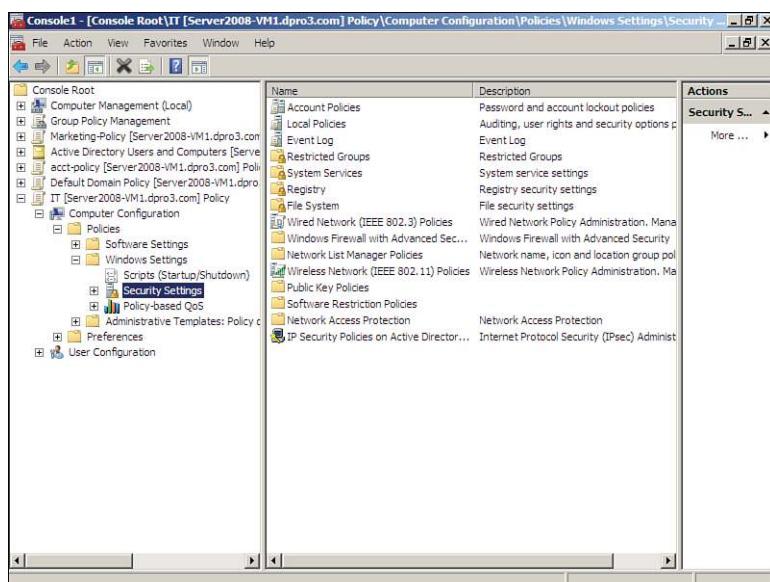


Figure 12-14 Security Settings Within the IT Policy on a Windows Server

Chapter Summary

In the previous chapter we discussed treating your IT infrastructure as more of an entity, and less of a collection of technologies. That philosophy of the synergy between man and computer is nothing novel—the idea dates back to von Neumann. But the extension of this synergy between disparate IT systems—and the security administrators that protect them—is an outlook that is being applied by more and more IT professionals.

Protect is the key word here. To do so effectively means to apply hands-on, continuous monitoring that: enables an already secure organization to assess weaknesses in real-time; tracks the growth of the IT infrastructure; and provides a glimpse of what is to be. But then there is also the Monday morning quarterbacking, the investigation of negative occurrences, the reference to historical anomalies—in short, the auditing of the IT infrastructure. It's that interpretive digging into the past, coupled with protective monitoring, that can ensure the stability of an IT infrastructure.

Now we can wax poetic until we are blue in the face, but all the pontification in the world won't provide the hands-on execution required to meticulously, and methodically, defend the IT environment. For example, it's the IDS/IPS solutions that will provide you with actual statistics concerning the behavior of data, and any anomalies that may present themselves. It's the concrete baselining with tools such as Performance Monitor and Wireshark that supplies analytics about the health of your servers and the types of data passing through them.

There is a myriad of other analytical tools at your disposal. The command-line included with each type of operating system has a huge variety of utilities that can bestow the bulk of the answers you are looking for about your computers. Plus, there are seemingly countless third-party applications available—some free, and some for a fee—that can help to fill any knowledge gaps about your computer network.

The detective in you will require periodic audits. In some cases, an organization requires that this be done by an independent consultant. However, your honor will probably require that you conduct occasional audits as well. Review your ACLs, permissions, and policies. But especially, keep a watchful eye on your security logs. These are some of the most important analytics that you will possess. They explain who did what and when it occurred (and possibly why). Define strong auditing policies, implement them, enforce them, review them often, and back them up.

Finally, we made mention of the von Neumann mindset. As IT infrastructures become more complex, and data gets “bigger,” and computers become “smarter,” this ideal becomes all the more vital. I'm not saying to pat the server on the back and tell it everything is going to be okay, but rather provide your IT infrastructure with a sort of compassion that will nurture it and help it to grow. You may say: “Dave, it

sounds like you treat your computer networks almost as if they are living beings!" Is that so strange? Is AI so far away? Time will tell. As of the writing of this book (2014) there are learning algorithms, self-healing servers and networks, super-computers such as Watson, and advances in robotics that were unimaginable just a decade ago. Besides, many of the geeks out there (and I use that term with high regard) do indeed already treat their servers—even entire IT environments—like pets or even friends. And so, that compassion manifests itself in the form of robust monitoring and scrupulous auditing. That is the *way* to the goal of providing the highest level of protection possible.

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 12-2 lists a reference of these key topics and the page number on which each is found.

Table 12-2 Key Topics for Chapter 12

Key Topic Element	Description	Page Number
Table 12-1	Summary of monitoring methodologies	467
Figure 12-1	Performance Monitor in Windows	469
Figure 12-2	Wireshark showing a captured TLS Version 1.0 packet	472
Figure 12-3	Network Monitor showing a captured FTP packet with clear-text password	473
Figure 12-5	Audit Policy within the Local Computer Policy of a Windows computer	479
Figure 12-7	Security log in Windows	481
Figure 12-9	Syslog program running in Windows	484
Figure 12-10	Windows Server Security Log Properties dialog box	486

Define Key Terms

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

signature-based monitoring, anomaly-based monitoring, behavior-based monitoring, baselining, baseline reporting, security posture, security posture assessment (SPA), promiscuous mode, non-promiscuous mode, broadcast storm, Simple Network Management Protocol (SNMP), computer security audits, audit trail

Review Questions

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

1. Which of the following is a record of the tracked actions of users?
 - A. Performance Monitor
 - B. Audit trails
 - C. Permissions
 - D. System and event logs

2. What tool can alert you if a server's processor trips a certain threshold?
 - A. TDR
 - B. Password cracker
 - C. Event Viewer
 - D. Performance Monitor

3. The IT director has asked you to install agents on several client computers and monitor them from a program at a server. What is this known as?
 - A. SNMP
 - B. SMTP
 - C. SMP
 - D. Performance Monitor

4. One of your co-workers complains to you that he cannot see any security events in the Event Viewer. What are three possible reasons for this? (Select the three best answers.)
 - A. Auditing has not been turned on.
 - B. The log file is only 512 KB.

- C. The co-worker is not an administrator.
 - D. Auditing for an individual object has not been turned on.
5. Which tool can be instrumental in capturing FTP GET requests?
- A. Vulnerability scanner
 - B. Port scanner
 - C. Performance Monitor
 - D. Protocol analyzer
6. Your manager wants you to implement a type of intrusion detection system (IDS) that can be matched to certain types of traffic patterns. What kind of IDS is this?
- A. Anomaly-based IDS
 - B. Signature-based IDS
 - C. Behavior-based IDS
 - D. Heuristic-based IDS
7. You are setting up auditing on a Windows computer. If set up properly, which log should have entries?
- A. Application log
 - B. System log
 - C. Security log
 - D. Maintenance log
8. You have established a baseline for your server. Which of the following is the best tool to use to monitor any changes to that baseline?
- A. Performance Monitor
 - B. Anti-spyware
 - C. Antivirus software
 - D. Vulnerability assessments software
9. In what way can you gather information from a remote printer?
- A. HTTP
 - B. SNMP
 - C. CA
 - D. SMTP

- 10.** Which of the following can determine which flags are set in a TCP/IP handshake?
 - A.** Protocol analyzer
 - B.** Port scanner
 - C.** SYN/ACK
 - D.** Performance Monitor

- 11.** Which of the following is the most basic form of IDS?
 - A.** Anomaly-based
 - B.** Behavioral-based
 - C.** Signature-based
 - D.** Statistical-based

- 12.** Which of the following deals with the standard load for a server?
 - A.** Patch management
 - B.** Group Policy
 - C.** Port scanning
 - D.** Configuration baseline

- 13.** Your boss wants you to properly log what happens on a database server. What are the most important concepts to think about while you do so? (Select the two best answers.)
 - A.** The amount of virtual memory that you will allocate for this task
 - B.** The amount of disk space you will require
 - C.** The information that will be needed to reconstruct events later
 - D.** Group Policy information

- 14.** Which of the following is the best practice to implement when securing logs files?
 - A.** Log all failed and successful login attempts.
 - B.** Deny administrators access to log files.
 - C.** Copy the logs to a remote log server.
 - D.** Increase security settings for administrators.

- 15.** What is the main reason to frequently view the logs of a DNS server?
- A.** To create aliases
 - B.** To watch for unauthorized zone transfers
 - C.** To defend against denial-of-service attacks
 - D.** To prevent domain name kiting
- 16.** As you review your firewall log, you see the following information. What type of attack is this?
- ```
S=207.50.135.54:53 - D=10.1.1.80:0
S=207.50.135.54:53 - D=10.1.1.80:1
S=207.50.135.54:53 - D=10.1.1.80:2
S=207.50.135.54:53 - D=10.1.1.80:3
S=207.50.135.54:53 - D=10.1.1.80:4
S=207.50.135.54:53 - D=10.1.1.80:5
```
- A.** Denial-of-service
  - B.** Port scanning
  - C.** Ping scanning
  - D.** DNS spoofing
- 17.** Of the following, which two security measures should be implemented when logging a server? (Select the two best answers.)
- A.** Cyclic redundancy checks
  - B.** The application of retention policies on log files
  - C.** Hashing of log files
  - D.** Storing of temporary files
- 18.** You suspect a broadcast storm on the LAN. Which tool should you use to diagnose which network adapter is causing the storm?
- A.** Protocol analyzer
  - B.** Firewall
  - C.** Port scanner
  - D.** Network intrusion detection system
- 19.** Which of the following should be done if an audit recording fails?
- A.** Stop generating audit records.
  - B.** Overwrite the oldest audit records.

- C. Send an alert to the administrator.
  - D. Shut down the server.
- 20. Which of the following log files should show attempts at unauthorized access?
  - A. DNS
  - B. System
  - C. Application
  - D. Security
- 21. To find out when a computer was shut down, which log file would an administrator use?
  - A. Security
  - B. System
  - C. Application
  - D. DNS
- 22. Which of the following requires a baseline? (Select the two best answers.)
  - A. Behavior-based monitoring
  - B. Performance Monitor
  - C. Anomaly-based monitoring
  - D. Signature-based monitoring
- 23. Jason is a security administrator for a company of 4000 users. He wants to store 6 months of logs to a logging server for analysis. The reports are required by upper management due to legal obligations but are not time-critical. When planning for the requirements of the logging server, which of the following should not be implemented?
  - A. Performance baseline and audit trails
  - B. Time stamping and integrity of the logs
  - C. Log details and level of verbose logging
  - D. Log storage and backup requirements
- 24. One of the developers in your organization installs a new application in a test system to test its functionality before implementing into production. Which of the following is most likely affected?
  - A. Application security
  - B. Initial baseline configuration

- C. Application design
  - D. Baseline comparison
25. Michael has just completed monitoring and analyzing a web server. Which of the following indicates that the server might have been compromised?
- A. The web server is sending hundreds of UDP packets.
  - B. The web server has a dozen connections to inbound port 80.
  - C. The web server has a dozen connections to inbound port 443.
  - D. The web server is showing a drop in CPU speed and hard disk speed.
26. What kind of security control do computer security audits fall under?
- A. Detective
  - B. Preventive
  - C. Corrective
  - D. Protective
27. You have been alerted to suspicious traffic without a specific signature. Under further investigation, you determine that the alert was a false indicator. Furthermore, the same alert has arrived at your workstation several times. Which security device needs to be configured to disable false alarms in the future? (Select the best answer.)
- A. Anomaly-based IDS
  - B. Signature-based IPS
  - C. Signature-based IDS
  - D. UTM
28. You have been tasked with providing daily network usage reports of layer 3 devices without compromising any data during the information gathering process. Which of the following should you select in this scenario?
- A. ICMP
  - B. SNMP
  - C. SNMPv3
  - D. SSH

**29.** Which of the following techniques enables an already secure organization to assess security vulnerabilities in real time?

- A.** Baseling
- B.** ACLs
- C.** Continuous monitoring
- D.** Video surveillance

**30.** Which of the following protocols are you observing in the packet capture below?

16:42:01 - SRC 192.168.1.5:3389 - DST 10.254.254.57:8080 - SYN/ACK

- A.** HTTP
- B.** HTTPS
- C.** RDP
- D.** SFTP

## Answers and Explanations

- 1. B.** Audit trails are records showing the tracked actions of users. Performance Monitor is a tool in Windows that enables you to track the performance of objects such as CPU, RAM, network adapter, physical disk, and so on. Permissions grant or deny access to resources. To see whether permissions were granted, auditing must be enabled. The System log and other logs record events that happened in other areas of the system—for example, events concerning the operating system, drivers, applications, and so on.
- 2. D.** Performance Monitor can be configured in such a way that alerts can be set for any of the objects (processor, RAM, paging file) in a computer. For example, if the processor were to go beyond 90% usage for more than 1 minute, an alert would be created and could be sent automatically to an administrator. A TDR is a time-domain reflectometer, an electronic instrument used to test cables for faults. A password cracker is a software program used to recover or crack passwords; an example would be Cain & Abel. The Event Viewer is a built-in application in Windows that enables a user to view events on the computer such as warnings, errors, and other information events. It does not measure the objects in a server in the way that Performance Monitor does.
- 3. A.** SNMP (Simple Network Management Protocol) is used when a person installs agents on client computers to monitor those systems from a single remote location. SMTP is used by e-mail clients and servers. SMP is symmetric multiprocessing, which is not covered in the Security+ exam objectives.

Performance Monitor enables a person to monitor a computer and create performance baselines.

4. **A., C., and D.** To audit events on a computer, an administrator would need to enable auditing within the computer's policy, then turn on auditing for an individual object (folder, file, and so on), and then view the events within the Security log of the Event Viewer. 512 KB is big enough for many events to be written to it.
5. **D.** A protocol analyzer captures data including things such as GET requests that were initiated from an FTP client. Vulnerability scanners and port scanners look for open ports and other vulnerabilities of a host. Performance Monitor is a Windows program that reports on the performance of the computer system and any of its parts.
6. **B.** When using an IDS, particular types of traffic patterns refer to signature-based IDS. Heuristic signatures are a subset of signature-based monitoring systems, so signature-based IDS is the best answer. Anomaly-based and behavior-based systems use different methodologies.
7. **C.** After auditing is turned on and specific resources are configured for auditing, you need to check the Event Viewer's Security log for the entries. These could be successful logons or misfired attempts at deleting files; there are literally hundreds of options. The Application log contains errors, warnings, and informational entries about applications. The System log deals with drivers, system files, and so on. A System Maintenance log can be used to record routine maintenance procedures.
8. **A.** Performance monitoring software can be used to create a baseline and monitor for any changes to that baseline. An example of this would be the Performance console window within Windows Server. (It is commonly referred to as Performance Monitor.) Antivirus and anti-spyware applications usually go hand-in-hand and are not used to monitor server baselines. Vulnerability assessing software such as Nessus or Nmap is used to see whether open ports and other vulnerabilities are on a server.
9. **B.** SNMP (Simple Network Management Protocol) enables you to gather information from a remote printer. HTTP is the Hypertext Transfer Protocol that deals with the transfer of web pages. A CA is a certificate authority, and SMTP is the Simple Mail Transfer Protocol.
10. **A.** A protocol analyzer can look inside the packets that make up a TCP/IP handshake. Information that can be viewed includes SYN, which is synchronize sequence numbers, and ACK, which is acknowledgment field-significant. Port scanners and Performance Monitor do not have the capability to view flags set in a TCP/IP handshake, nor can they look inside packets in general.

11. **C.** Signature-based IDS is the most basic form of intrusion detection systems, or IDS. This monitors packets on the network and compares them against a database of signatures. Anomaly-based, behavioral-based, and statistical-based are all more complex forms of IDS. Anomaly-based and statistical-based are often considered to be the same type of monitoring methodology.
12. **D.** A configuration baseline deals with the standard load of a server. By measuring the traffic that passes through the server's network adapter, you can create a configuration baseline over time.
13. **B.** and **C.** It is important to calculate how much disk space you will require for the logs of your database server and verify that you have that much disk space available on the hard drive. It is also important to plan what information will be needed in the case that you need to reconstruct events later. Group Policy information and virtual memory are not important for this particular task.
14. **C.** It is important to copy the logs to a secondary server in case something happens to the primary log server; this way you have another copy of any possible security breaches. Logging all failed and successful login attempts might not be wise, because it will create many entries. The rest of the answers are not necessarily good ideas when working with log files.
15. **B.** Security administrators should frequently view the logs of a DNS server to monitor any unauthorized zone transfers. Aliases are DNS names that redirect to a hostname or FQDN. Simply viewing the logs of a DNS server will not defend against denial-of-service attacks. Domain name kiting is the process of floating a domain name for up to five names without paying for the domain name.
16. **B.** The information listed is an example of a port scan. The source IP address perpetuating the port scan should be banned or blocked on the firewall. The fact that the source computer is using port 53 is of no consequence during the port scan and does not imply DNS spoofing. It is not a denial-of-service attack; note that the destination IP address ends in 80, but the number 80 is part of the IP address and is not the port.
17. **B.** and **C.** The log files should be retained in some manner either on this computer or on another computer. By hashing the log files, the integrity of the files can be checked even after they are moved. Cyclic redundancy checks, or CRCs, have to deal with the transmission of Ethernet frames over the network. Temporary files are normally not necessary when dealing with log files.
18. **A.** A protocol analyzer should be used to diagnose which network adapter on the LAN is causing the broadcast storm. It is also useful for detecting flooding attacks and fragmented packets. A firewall cannot diagnose attacks perpetuated

on a network. A port scanner is used to find open ports on one or more computers. A network intrusion detection system (NIDS) is implemented to locate and possibly quarantine some types of attacks but will not be effective when it comes to broadcast storms.

19. **C.** If an audit recording fails, there should be sufficient safeguards employed that can automatically send an alert to the administrator, among other things. Audit records should not be overwritten and in general should not be stopped.
20. **D.** The Security log file should show attempts at unauthorized access to a Windows computer. The Application log file deals with events concerning applications within the operating system and some third-party applications. The System log file deals with drivers, system files, and so on. A DNS log will log information concerning the domain name system.
21. **B.** The System log will show when a computer was shut down (and turned on, for that matter, or restarted). The Security log shows any audited information on a computer system. The Application log deals with OS apps and third-party apps. The DNS log shows events that have transpired on a DNS server.
22. **A. and C.** Behavior-based monitoring and anomaly-based monitoring require creating a baseline. Many host-based IDS systems will monitor parts of the dynamic behavior and the state of the computer system. An anomaly-based IDS will classify activities as either normal or anomalous; this will be based on rules instead of signatures. Both behavior-based and anomaly-based monitoring require a baseline to make a comparative analysis. Signature-based monitoring systems do not require this baseline because they are looking for specific patterns or signatures and are comparing them to a database of signatures. Performance Monitor can be used to create a baseline on Windows computers, but it does not necessarily require a baseline.
23. **A.** A performance baseline and audit trails are not necessarily needed. Because the reports are not time-critical, a performance baseline should not be implemented. Auditing this much information could be unfeasible for one person. However, it is important to implement time stamping of the logs and store log details. Before implementing the logging server, Jason should check whether he has enough storage and backup space to meet his requirements.
24. **B.** The initial baseline configuration is most likely affected. Because the application has just been installed, there is only an initial baseline, but no other baselines to yet compare with. Since it is a testing environment, and the developer has just installed the application, security is not a priority. The developer probably wants to see what makes the application tick, and possibly reverse engineer it, but is not yet at the stage of application design, and probably won't be until a new application or modification of the current application is designed.

- 25. D.** If the web server is showing a drop in processor and hard disk speed, it might have been compromised. Further analysis and comparison to a pre-existing baseline would be necessary. All the other answers are common for a web server.
- 26. A.** A computer security audit is an example of a detective security control. If a security administrator found that a firewall was letting unauthorized ICMP echoes into the network, the administrator might close the port on the firewall—a corrective control, and for the future, a preventive control. The term protective control is not generally used in security circles as it is a somewhat ambiguous term.
- 27. A.** Most likely, the anomaly-based IDS needs to be re-configured. It is alerting you to legitimate traffic, which amounts to false positives. These are not actually anomalies. If the traffic being analyzed has no specific signature (or known signature), then a signature-based IDS or IPS will not be able to identify it as legitimate or illegitimate. A UTM is a unified threat management device. This device may or may not have an IDS or IPS, and even then, it may or may not be capable of anomaly-based analysis, so it is not as likely an answer as the anomaly-based IDS.
- 28. C.** SNMPv3 should be used because it provides a higher level of security (encryption of packets, message integrity, and authentication), allowing you to gather information without fear of the data being compromised. SNMPv1 and v2 do not have the elaborate security of SNMPv3. ICMP is the Internet Control Message Protocol used with the ping utility, among other things. It has little to do with monitoring. SSH is Secure Shell, which is a more secure way of remotely controlling systems; it acts as a secure alternative to Telnet.
- 29. C.** Continuous monitoring will help an already secure organization to assess security vulnerabilities and weaknesses in real time. Baseling and ACLs are things that have happened, or were configured in the past. Video surveillance is surely in real time, but it is doubtful as to whether it can *assess* security vulnerabilities in real time, even if someone is watching the video stream as it happens.
- 30. C.** You are observing a Remote Desktop Protocol (RDP) acknowledgement packet. You can tell because the source IP address (192.168.1.5) is using port 3389, the default port for RDP, and is sending the ACK to 10.254.254.57 (which was connecting on the secondary HTTP port 8080). So the client is using an HTTP port, but that is inconsequential because the packet is being generated by the source (SRC) IP. HTTPS (port 443) is not involved in this packet capture. Neither is SFTP, as it rides on SSH using port 22.

## Case Studies for Chapter 12

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

### Case Study 12-1: Capturing and Analyzing Packets

**Scenario:** You are doing work for a medium-sized business with several servers. There is concern that one of the servers is running a non-secured FTP service, and is possibly being used for non-work purposes. Your task is to analyze the traffic coming in and out of the server.

What technology should you use to analyze the traffic?

What are a couple of examples of this technology?

Which layer of the OSI model will tell you about the ports being used by applications?

### Case Study 12-2: Deciphering Log Files

**Scenario:** The same organization used in Case Study 12-1 has concerns about its firewall. The IT director thinks that an attacker on the Internet is attempting (and possibly succeeding) in bypassing the firewall, but doesn't know how it is potentially being done or what port is being used to do it.

What application/protocol can you use to easily analyze the firewall logs from your workstation?

How would you configure this on the firewall and at your workstation?

Describe a typical log message with attempted communication and the two main components of it.

If you see a message such as the one listed below, what does it tell you?

```
Tues Apr 21 12:36:01 2014 Cisco Firewall System Log: Blocked incoming
TCP packet
From 64.58.137.211:23475 65.82.117.241:23 as SYN:ACK received but
there is no active connection.
```

### Case Study 12-3: Auditing Files

**Scenario:** You've analyzed packets, checked Syslogs, and checked for vulnerabilities on the firewall. As a final precaution you want to make sure that no one is accessing your file server and compromising the integrity of your data files.

You decide to enable auditing on the server. What steps are involved to accomplish this?

## Case Study Solutions

### Case Study 12-1 Solution

It's a good idea to periodically analyze the traffic that is sent and received by servers. This can help when you are concerned about a potential compromise, or just think that the server is being used incorrectly.

There are lots of technologies used to analyze traffic, but the best for this scenario is the protocol analyzer, otherwise known as a network sniffer or packet sniffer. Examples of these tools include Wireshark, Network Monitor, NetScout, TCPdump and snoop (command-line only), WinDump, Network Observer, and so on. Wireshark is extremely common and (as of the writing of this book) is a free download. It's the transport layer of the OSI model that tells all. It defines the port number being used on the source computer and the destination. It also describes the transport mechanism being used (TCP or UDP). The network layer is also important as this shows the IP addresses being used by the communicating systems. The application layer shows what program is being used, but many network and security admins will jump right to the transport layer and glean that information (and much more info) from the port numbers.

**Video Solution:** Watch the video solution “12-1: Capturing and Analyzing Packets” on the accompanying disc.

**Simulation:** Complete the simulation “12-1: Capturing and Analyzing Packets” on the accompanying disc.

### Case Study 12-2 Solution

Use the Syslog protocol. There are many Syslog programs available, such as SolarWinds Kiwi Syslog Server. This can pull the logs from a firewall and other network devices so that you can watch them in real time from your workstation.

The firewall would need to have Syslogging enabled and configured to stream log messages to the IP address of your workstation. A typical log message will be generated by the firewall when someone on the Internet attempts to connect to it. It will have the source IP address and port as well as the destination IP address and port; for example:

S=207.50.135.54:53 – D=10.1.1.80:1

In the Case Study's Syslog message listed, you are told a lot of information, including the potential attacker's IP address and the port used, as well as the IP address of your firewall and the port that was attempted for access; in this case port 23 Telnet. The important part here is that the TCP packet was *blocked*. So the firewall succeeded in blocking the potential attack and remained secure. However, devices will fail sometimes. The key is to fail securely. An example of a secure failure would be if a firewall let a packet through (which *will* happen) but the result was that the firewall was shut off immediately after by an automated mechanism. Another example would be if an IPS blocked a packet that was legitimate. This is a failure, but a secure one, albeit an inefficient one. Another example is if a WAP let a potential attacker through but redirected the person to a honeypot, or if the WAP shut down altogether.

If you believe that an attacker is possibly getting through the firewall, then some active scanning will be appropriate. Connect to the firewall from the public side and use a port scanner such as Nmap or a vulnerability scanner such as Nessus (or both) to find out what (if any) open ports there are and if any of these are substantial vulnerabilities.

**Video Solution:** Watch the video solution "12-2: Deciphering Log Files" on the accompanying disc.

**Simulation:** Complete the simulation "12-2: Deciphering Log Files" on the accompanying disc.

### Case Study 12-3 Solution

Auditing is an excellent way to check for data integrity issues, check for breach of permissions, or to simply make sure that your files are being accessed exactly the way you want!

For example, auditing can be enabled on a Windows Server and you can review who tried to access what, and whether they succeeded or failed. What you are most interested in is the attempted deletion or modification of data. The basic steps involved with auditing include enabling auditing in a policy, turning on auditing for a data folder (or other resource) in question, and finally, reviewing the Security log often.

**Video Solution:** Watch the video solution "12-3: Auditing Files" on the accompanying disc.



### This chapter covers the following subjects:

- **Cryptography Concepts:** This section covers the basic terminology of cryptography, including encryption, ciphers, and keys. It also discusses private versus public keys, symmetric versus asymmetric encryption, and public key encryption.
- **Encryption Algorithms:** This section delves into the various symmetric algorithms, such as DES and AES, and some of the popular asymmetric algorithms such as RSA and elliptic curve.
- **Hashing Basics:** Here, we investigate the most common way to verify the integrity of files: hashing. We cover basic hashing concepts and cryptographic hash functions, such as MD5, SHA, and NTLM.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 4.4, 6.1, and 6.2.

# Encryption and Hashing Concepts

When data is encrypted, it is modified in such a way that it cannot be understood by anyone who does not have the correct key. If you have the correct key, you can decrypt the data, and it will once again become intelligible. Though almost everyone has dealt with encrypted data and/or encrypted Internet sessions of some sort, chances are that the majority of the readers of this book will have limited *hands-on* experience with encryption. Because of this, I have written this chapter, and the following one, in a very to-the-point manner with simple analogous examples. I cover only what you need to know about encryption concepts, methods, and types. Encryption by itself is an entire IT field, but the CompTIA Security+ exam requires that you know only the basics—the exam objectives only scrape the surface of encryption concepts. Keep all this in mind as you go through this chapter and the next. I have left some links to more advanced encryption books and websites in the disc’s View Recommended Resources section, although they are not necessary for the exam. That being said, the “basics” of cryptography is a pretty huge chunk of information—there is a lot to cover, and some of the topics can be difficult to understand.

It can help to pose the following question: What is it that we need to encrypt? Without a doubt, it is the data that needs to be encrypted, but more specifically three types of data: data in use, data at rest, and data in motion. Data in use can be described as actively used data undergoing constant change; it could be stored in databases or spreadsheets, for example. Data at rest is inactive data that is archived—backed up to tape or otherwise. Data in motion (also known as data in transit) is data that crosses the network or data that currently resides in computer memory. Consider thinking in these terms as we progress through the chapter.

## Foundation Topics

### Cryptography Concepts

Cryptography is the practice of hiding the meaning of a message. The word is roughly derived from the Greek words *kryptos* (meaning “hidden”) and *graphein* (meaning “to write”). However, in cryptography it is not the message that is hidden, but rather the significance of the message.

Let's give a basic example of cryptography. When I was younger, some of the girls I knew would keep a black book with names, phone numbers, and so on. I'm still pretty sure to this day that I wasn't in any of them! Anyway, a couple of those people did something that fascinated me—they would modify phone numbers according to a code they had developed. This was done to hide the true phone number of a special friend from their parents, or from teachers, and so on. It was a basic form of encryption, although at the time I didn't realize it. I just referred to it as a "code."

Essentially, it worked like this:

The person with the black book would take a real phone number such as 555-0386. They would then modify the number by stepping each number backward or forward  $x$  number of steps. Let's say the person decided to step each number between 0 and 9 backward by three steps; the resulting coded phone number would be 222-7053. I'm sure you see how that was done, but let's break it down so that we can make an analogy to today's data encryption. Table 13-1 shows the entire code used.

### Key Topic

**Table 13-1** Black Book Phone Number Encryption

| Original Number | Modifier | Modified Number |
|-----------------|----------|-----------------|
| 0               | Minus 3  | 7               |
| 1               |          | 8               |
| 2               |          | 9               |
| 3               |          | 0               |
| 4               |          | 1               |
| 5               |          | 2               |
| 6               |          | 3               |
| 7               |          | 4               |
| 8               |          | 5               |
| 9               |          | 6               |

In this example, each number between 0 and 9 corresponds to a number three digits behind it. By the way, the numbers cycle through: For example, the number 0 goes three steps back, starting at 0, to 9, 8, and then 7 in an "around-the-bend" fashion. This is an example of cryptographic substitution.

**NOTE** This is based on the *Caesar Cipher* (more accurately the Caesar Shift Cipher), where messages sent in ancient Rome would have each letter shifted by one or more places.

Let's analogize. Each of the components in the table can be likened to today's computer-based encryption concepts:

- The original number is like to original file data.
- The modifier is like to an encryption key.
- The modified number is like to encrypted file data.

I call this the "Black Book Example," but I would guess that others have used similar analogies. Of course, this is a basic example; however, it should serve to help you to associate actual computer-based encryption techniques with this more tangible idea.

Now, for other people to figure out the original phone numbers in the black book, they would have to do the following:

- Step 1.** Gain access to the black book. This is just like gaining access to data. Depending on how well the black book is secured, this by itself could be difficult.
- Step 2.** Break the code. This would be known as decrypting the data. Of course, if the owner of the black book was silly enough to put the phone number encryption table in the book, well, then game over; it would be easy to decode. But if the owner was smart enough to memorize the code (and tell it to no one), making it a secret code, it would be much more difficult for another person to crack. Plus, the person could make the code more advanced; for example, look at Table 13-2.

**Table 13-2** Advanced Black Book Phone Number Encryption

| Original Number | Modifier | Modified Number |
|-----------------|----------|-----------------|
| 0               | Minus 9  | 1               |
| 1               | Minus 8  | 3               |
| 2               | Minus 7  | 5               |
| 3               | Minus 6  | 7               |
| 4               | Minus 5  | 9               |
| 5               | Minus 4  | 1b              |

| Original Number | Modifier | Modified Number |
|-----------------|----------|-----------------|
| 6               | Minus 3  | 3b              |
| 7               | Minus 2  | 5b              |
| 8               | Minus 1  | 7b              |
| 9               | Minus 0  | 9b              |

In this example, there is a different modifier (or key) for each original number. Because the modified numbers have duplicates, we place a letter next to each of the various duplicates to differentiate. This is tougher to decrypt due to the increased level of variations, but on the flipside, it is that much harder to memorize. Likewise, computers have a harder time processing more advanced encryption codes, and hackers (or crackers) have a difficult time processing their decryption.

At this point, only one person has legitimate access to the encryption codes. However, what if the person wanted to share phone numbers with another person, but still keep the numbers secret from everyone else? This would be known as a secret key.

We refer to this basic concept as we go through this chapter and the next.

Now that we have given a basic example, let's define some terminology in a more technical way. We start with cryptography, encryption, ciphers, and keys. You might want to read through this list twice because each definition builds on the last.

- **Cryptography:** By definition, **cryptography** is the practice and study of hiding information, or more accurately, hiding the meaning of the information. It is used in e-commerce and with passwords. Most commonly, encryption is used to hide a message's meaning and make it secret.
- **Encryption:** **Encryption** is the process of changing information using an algorithm (or cipher) into another form that is unreadable by others—unless they possess the key to that data. Encryption is used to secure communications and to protect data as it is transferred from one place to another. The reverse, decryption, can be accomplished in two ways: First, by using the proper key to unlock the data, and second, by cracking the original encryption key. Encryption enforces confidentiality of data.
- **Cipher:** A **cipher** is an algorithm that can perform encryption or decryption. A basic example would be to take the *plaintext* word “code” and encrypt it as a *ciphertext* using a specific algorithm. The end result could be anything, depending on the algorithm used, but, for example, let's say the end result was the ciphertext “zlab.” I don't know about you, but “zlab” looks like gibberish to me. (Although if you Google it, I'm sure you'll find all kinds of endless fun.)

You've probably already guessed at my cipher—each letter of the plaintext word “code” was stepped back three letters in the alphabet. Historical ciphers use substitution methods such as this, and transposition methods as well. However, actual algorithms today are much more complex. **Algorithms** are well-defined instructions that describe computations from their initial state to their final state. IF-THEN statements are examples of computer algorithms. The entire set of instructions is the cipher. We cover the various types of ciphers (again, also known as algorithms) in the section “Encryption Algorithms” later in this chapter.

- **Key:** The **key** is the essential piece of information that determines the output of a cipher. It is indispensable; without it there would be no result to the cipher computation. In the previous bullet, the key was the act of stepping back three letters. In the first black book example, the key was stepping back three numbers (a modifier of minus 3). Just like a person can't unlock a lock without the proper key, a computer can't decrypt information without the proper key (using normal methods). The only way to provide security is if the key is kept secret—or in the case that there are multiple keys, if one of them is kept secret. The terms key and cipher are sometimes used interchangeably, but you should remember that the key is the vital portion of the cipher that determines its output. The length of the key determines its strength. Shorter, weaker keys are desirable to hackers attempting to access encrypted data. When two users exchange encrypted messages, it starts with a key exchange. The method of this exchange will vary depending on the type of cryptographic algorithm.

Keys can be private or public. A **private key** is only known to a specific user or users who keep the key a secret. A **public key** is known to all parties involved in encrypted transactions within a given group. An example of a private key would be the usage of an encrypted smart card for authentication. Smart cards, ExpressCard/PC Card technology, and USB flash drives are examples of devices that can store keys. When private keys are stored on these types of devices and delivered outside of a network, it is known as out-of-band key exchange. An example of a public key would be when two people want to communicate securely with each other over the Internet; they would require a public key that each of them knows. When this key transfer happens over a network, it is known as in-band key exchange.

Encryption types, such as AES or RSA, are known as ciphers, key algorithms, or simply as algorithms; we refer to them as algorithms during the rest of this chapter and the next. There are basically two classifications of key algorithms: symmetric and asymmetric.

## Symmetric Versus Asymmetric Key Algorithms

Some cryptographic systems use symmetric keys only, others use asymmetric keys only, and some use both symmetric and asymmetric. It is important to know the differences between the two, and how they can be used together.

### Symmetric Key Algorithms

The **symmetric key algorithm** is a class of cipher that uses a single key, identical keys, or closely related keys for both encryption and decryption. The term “symmetric key” is also referred to as the following: secret key, private key, single key, and shared key. Examples of symmetric key algorithms include DES, 3DES, RC, and AES, all of which we discuss later in this chapter. Another example of a technology that uses symmetric keys is Kerberos. By default, Kerberos makes use of a third party known as a key distribution center (KDC) for the secure transmission of symmetric keys, also referred to as tickets.

**NOTE** Kerberos can optionally use public key cryptography (covered later in this chapter) by making use of asymmetric keys. This is done during specific authentication stages. Kerberos is covered in more depth in Chapter 9, “Physical Security and Authentication Models.”

The private key is common in the workplace. Let’s say that a user encrypts a file with a private key. Generally, that same key (or a very similar private key) is needed to decrypt the data. Imagine that the user left the organization and that user’s account (and therefore the user’s key) was deleted. How would you get the data back? Well, if the system has a recovery agent, you could use that to decrypt the file; otherwise, the data will not be recoverable! It’s important to understand that private keys, and by extension, symmetric key systems, must be approached carefully or data could become lost.

Following are two types of symmetric key algorithms:

- A **stream cipher** is a type of algorithm that encrypts each binary digit in the data stream, one bit at a time.
- A **block cipher** is a type of algorithm that encrypts a group of bits collectively as individual units known as blocks. For example, the Advanced Encryption Standard (AES) algorithm can use 128-bit or 256-bit block ciphers.

Symmetric key algorithms require a secure initial exchange of one or more secret keys to both the sender and the receiver. In our black book example, we mentioned

that people might possibly want to share their cipher with someone else. To do so, they would need to make sure that they were alone and that no one was eavesdropping. It is also so with computers. The secure initial exchange of secret keys can be difficult depending on the circumstances. It is also possible to encrypt the initial exchange of the secret keys!

Symmetric ciphers can also be used for non-repudiation purposes by adding a message authentication code, which is a small algorithm that checks the integrity of the cipher and notifies the receiver if there were any modifications to the encrypted data. This way, the data cannot be denied (repudiated) when received.

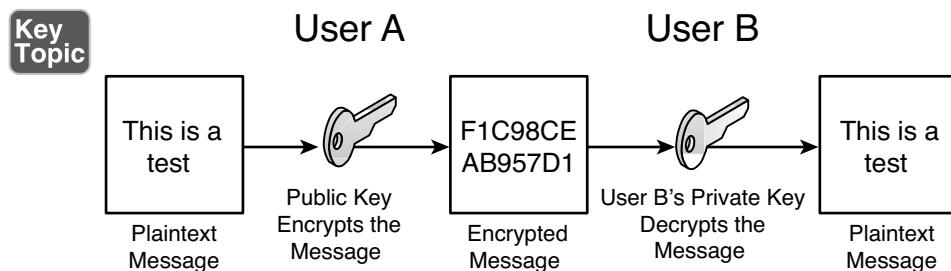
Symmetric encryption is the preferred option when encrypting and sending large amounts of data. This is in part because it usually takes far less time to encrypt and decrypt data than asymmetric encryption does.

## Asymmetric Key Algorithms

**Asymmetric key algorithms** use a pair of different keys to encrypt and decrypt data. The keys might be related, but they are not identical or even close to it in the way symmetric keys are. The two asymmetric keys are related mathematically. Imagine that you are the night shift security guard for a warehouse that stores CPUs. When your shift is over you are required to lock up. But the warehouse uses a special lock. Your key can only lock the warehouse door; it cannot unlock it. Conversely, the morning watchman has a key that can only unlock the door but not lock it. There are physical and electronic locks of this manner. This is analogous to asymmetric keys used in encryption. One key is used to encrypt data; the other, dissimilar key is used to decrypt the data. Because of the difference in keys, asymmetric key management schemes (such as PKI) are considered to be the most complicated. Examples of asymmetric key algorithms include RSA, the Diffie-Hellman system, and elliptic curve cryptography. SSL and TLS protocols use asymmetric key algorithms but generally do so in a public key cryptographic environment.

## Public Key Cryptography

**Public key cryptography** uses asymmetric keys alone or in addition to symmetric keys. It doesn't need the secure exchange of secret keys mentioned in the symmetric key section. Instead, the asymmetric key algorithm creates a secret private key and a published public key. The public key is well known, and anyone can use it to encrypt messages. However, only the owner(s) of the paired or corresponding private key can decrypt the message. The security of the system is based on the secrecy of the private key. If the private key is compromised, the entire system will lose its effectiveness. This is illustrated in Figure 13-1.



**Figure 13-1** Illustration of Public Key Cryptography

Public key cryptography can become more intense. In some schemes, the private key is used to sign a message, and anyone can check the signature with the public key. This signing is done with a digital signature. A **digital signature** authenticates a document through math, letting the recipient know that the document was created and sent by the actual sender, and not someone else. So, it ensures integrity and non-repudiation, and it protects against forgery and tampering. The basic order of functions for the usage of asymmetric keys in this case would be encrypt, sign, decrypt, and verify.

**NOTE** Digital signatures can also be hashed (more on hashing later) for comparison once the document gets to its final destination.

In the Diffie-Hellman scheme, each user generates a public/private key pair and distributes a public key to everyone else. After two or more users obtain a copy of the others' public keys, they can be used to create a shared secret used as the key for a symmetric cipher. Due to the varying methods of public key cryptography, the whole subject can become somewhat confusing. Remember that there will always be a private key and a public key involved, and that public key cryptography can use asymmetric keys alone or in addition to symmetric keys.

Internet standards, such as SSL/TLS and PGP, use public key cryptography. Don't confuse the term public key cryptography with public key infrastructure (PKI). Although they are related, they are not the same. PKI is an entire system of hardware, software, policies, and so on, that binds public keys with user identities by way of certificates and a certificate authority (server or other such device). A **certificate** is an electronic document that uses a digital signature to bind the key with the identity. We cover PKI more in Chapter 14, "PKI and Encryption Protocols."

## Key Management

Key management deals with the relationship between users and keys; it's important to manage the generation, exchange, storage, and usage of those keys. It is crucial technically, and organizationally, because issues can present themselves due to poorly designed key systems and poor management. Keys must be chosen and stored securely. The generation of strong keys is probably the most important concept. Some algorithms have weak keys that make cryptanalysis easy. For example, DES uses a considerably weaker key than AES; the stronger the key, the stronger the key management. We detail several methods for the exchange of keys later in this chapter, including encapsulating one key within another, using key indicators, and exchanging symmetric session keys with an asymmetric key algorithm—in effect, ciphering our cipher. (We'll talk more about session keys in Chapter 14.) Secure storage of keys often depends on users and passwords, or other authentication schemes. Proper storage of keys allows for availability, part of the CIA triad. Finally, keys should be replaced frequently. If a particular user uses a key for too long, it increases the chances of the key being cracked. Keys, like passwords, should be changed and/or recycled often.

## Steganography

Although I have placed steganography within the cryptography section, it actually isn't cryptography, although it might be used with cryptography. **Steganography** is the science (and art) of writing hidden messages; it is a form of security through obscurity. The goal is that no one aside from the sender and receiver should even suspect that the hidden message exists. The advantage of steganography is that the clearly visible messages look to be just that, regular old messages that wouldn't usually attract attention to themselves. Most people know when they come into contact with an encrypted message, but far fewer people identify when a steganographic message has crossed their path. The classic example of steganography is from ancient Greece. A messenger would shave his head, and a leader would write a message on the person's scalp with indelible ink. After the messenger's hair grew long enough to hide the message, he would then deliver the message (time was not of the essence). When the messenger arrived at his destination, he would shave his head and the recipient could read the message. In Greek, *steganos* means "covered," and this is one example of hiding a message by covering it.

Steganography can hide messages within encrypted documents by inserting extra encrypted information. The hidden messages can also be found in sound files, image files, slowed-down video files, and regular Word documents or Excel spreadsheets. Messages can also be concealed within VoIP conversations (known as Lost Audio Packets Steganography, or LACK), and within any streaming service as well. They can also be obscured on a compromised wireless network with the HICCUPS system (Hidden Communication System for Corrupted Networks).

A common example of steganography is when using graphic files to send hidden messages. In this scenario, the least significant bit of each byte is replaced. For example, we could shade the color of a pixel (or triad) just slightly. This slight change would change the binary number associated with the color, enabling us to insert information. The color blue is represented as three bytes of data numbered 0, 0, and 255. We could change the color blue slightly to 1, 0, 255. This would not make the graphic look any different to the naked eye, but the change would be there nonetheless. This would be done in several or more pixels of the graphic to form the message. For this to work, the recipient would first need to have possession of the original file. Then the sender would transmit the modified steganographic file to be compared with the original by the recipient.

## Encryption Algorithms

We mentioned previously that ciphers (or algorithms) can encrypt or decrypt data with the help of a key. We also pointed out that algorithms are well-defined instructions that describe computations from their initial state to their final state. In addition, we mentioned that there are symmetric and asymmetric algorithms. Now, let's talk about some of the actual algorithmic standards within both of those classifications. We start with symmetric types, including DES, 3DES, AES, and RC, and afterward move on to asymmetric types, including RSA, Diffie-Hellman, and the elliptic curve.

### DES and 3DES

The **Data Encryption Standard (DES)** is an older type of block cipher selected by the U.S. federal government back in the 1970s as its encryption standard. But due to its weak key, it is now considered deprecated and has been replaced by other standards. Being a block cipher, it groups 64 bits together into encryption units. Today, a 64-bit cipher is not considered powerful enough; also, and more important, the key size is 56-bit, which can be cracked fairly easily with a brute-force attack or linear cryptanalysis attack. In addition to this, there are some theoretical weaknesses to the cipher itself. DES was replaced by Triple DES (3DES) in 1999. The actual algorithm is sometimes referred to as the Data Encryption Algorithm (DEA). The algorithm is based on the Feistel cipher, which has very similar, if not identical, encryption and decryption processes, reducing the amount of code required.

**Triple DES**, also known as 3DES or the Triple Data Encryption Algorithm (TDEA), is similar to DES but applies the cipher algorithm three times to each cipher block. The cipher block size is still 64-bit, but the key size can now be as much as 168-bit (three times the size of DES). This was a smart approach to defeating brute-force attacks without having to completely redesign the DES protocol. However, both DES and 3DES have been overshadowed by AES, which became the preferred standard in late 2001.

## AES

In the late 1990s, the National Institute of Standards and Technology (NIST) started a competition to develop a more advanced type of encryption. There were 15 submissions, including Serpent, Twofish, RC6, and others, but the selected winner was Rijndael. This submission was then further developed into the **Advanced Encryption Standard (AES)** and became the U.S. federal government standard in 2002. AES is the successor to DES/3DES and is another symmetric key encryption standard composed of three different versions of block ciphers: AES-128, AES-192, and AES-256. Actually, each of these has the same 128-bit cipher block size, but the key sizes for each are 128-bit, 192-bit, and 256-bit, respectively.

AES is based on the substitution-permutation network, which takes plaintext and the key and applies  $x$  number of rounds to create the ciphertext. These rounds consist of substitution boxes and permutation boxes (usually in groups of 4X4 bytes) that convert the plaintext input bits to ciphertext output bits. AES specifies 10, 12, or 14 rounds for each of the respective versions.

AES is fast, uses minimal resources, and can be used on a variety of platforms. For example, it is the encryption algorithm of choice if you have a wireless network running the WPA2 protocol; the IEEE 802.11i standard specifies the usage of AES with WPA2, and in the process deprecates WEP. (See Chapter 8, “Securing Network Media and Devices,” for more about WEP and WPA.) You will also find AES as the encrypting protocol for remote control applications. These are examples of data in motion (also called data in transit). Any network session that uses AES would fall into this category. But memory encryption would fall into that category as well. For example, there are programs that can encrypt passwords and other personally identifiable information (PII) as it is passing through RAM. They often use AES or Twofish.

In addition, AES is a good choice for transferring encrypted data quickly to a USB flash drive. It is also used as the Windows Encrypting File System (EFS) algorithm and in whole disk encryption techniques such as BitLocker.

AES is purportedly susceptible to the related-key attack, if the attacker has some information about the mathematical relationship between several different keys. Side-channel attacks can also circumvent the AES cipher using malware to obtain privilege escalation. These are ways of attacking the implementation of the protocol, but not the protocol itself.

Generally, AES is considered the strongest type of symmetric encryption for many scenarios. As of now, AES is used worldwide and has not been outright compromised, and some industry experts think it never will be.

## RC

RC stands for different things depending on who you talk to. Officially, it is known as Rivest Cipher but is playfully known as Ron’s Code as well. There are multiple RC versions, most of which are not related aside from the fact that they are all encryption algorithms.

RC4 is a somewhat widely used stream cipher in protocols such as SSL, WEP, and RDP. It is known for its speed and simplicity. However, it is avoided when designing newer applications and technologies due to several vulnerabilities; when used with WEP on wireless networks, it can be cracked quickly with the use of aircrack-ptw. One way to avoid this to a certain extent is to use the Temporal Key Integrity Protocol (TKIP) with WEP. However, it still is recommended that AES and WPA2 be used in wireless networks. Some versions of Microsoft Remote Desktop Services use RC4 128-bit. However, Microsoft recommends disabling RC4 if at all possible, and using other encryption, such as FIPS-compliant encryption (IPsec and EFS) and TLS for authentication.

RC5 is a block cipher noted for its simplicity and for its variable size (32-, 64-, or 128-bit). The strongest block cipher that has been cracked via brute force as of the writing of this book is a 64-bit RC5 key, in 2001. This was done by distributed.net, a nonprofit organization which at the time had 30 TFLOPS of computational power. As of 2014, it is working on cracking the 72-bit version of RC5, with substantially higher throughput at its disposal. This is cause for concern for some—because Moore’s Law tells us of the effective doubling of CPU power every two years or so—but you must remember that stronger algorithms such as AES 256-bit are *exponentially* harder to crack.

RC6 is a block cipher entered into the AES competition and was one of the five finalists. Though it was not selected, it is a patented algorithm offered by RSA Security as an alternative to AES. It is similar to AES in block size and key size options but uses different mathematical methods than Rijndael.

## Blowfish and Twofish

Blowfish and Twofish are two ciphers designed by Bruce Schneier. The original Blowfish is a block cipher designed as an alternative to DES (the name also pertains to a suite of products). It has a 64-bit block size and variable key size between 1 and 448 bits. Bruce Schneier recommends the newer Twofish cipher, which has a block size of 128 bits and a key size up to 256 bits and is also based on Feistel. There is also a newer Threefish block cipher with key sizes up to 1024-bit. These symmetrical ciphers have not been compromised as of 2014.

## Summary of Symmetric Algorithms

Table 13-3 gives some comparisons of the algorithms up to this point and their key strength.

**Table 13-3** Summary of Symmetric Algorithms

**Key Topic**

| Algorithm Acronym | Full Name                    | Maximum/Typical Key Size |
|-------------------|------------------------------|--------------------------|
| DES               | Data Encryption Standard     | 56-bit                   |
| 3DES              | Triple DES                   | 168-bit                  |
| AES               | Advanced Encryption Standard | 256-bit                  |
| RC4               | Rivest Cipher version 4      | 128-bit typical          |
| RC5               | Rivest Cipher version 5      | 64-bit typical           |
| RC6               | Rivest Cipher version 6      | 256-bit typical          |
| Twofish           | Twofish                      | 128-, 192-, 256-bit      |

## RSA

Let's talk about some asymmetric key algorithms. The original and very common **RSA** (which stands for Rivest, Shamir, and Adleman, the creators) is a public key cryptography algorithm. As long as the proper size keys are used, it is considered to be a secure protocol and is used in many e-commerce scenarios. It is slower than symmetric key algorithms but has advantages being suitable for signing and for encryption. It works well with credit card security and TLS/SSL. Key lengths for RSA are much longer than in symmetric cryptosystems. For example, 512-bit RSA keys have proven to be breakable over a decade ago; however, 1024-bit keys are currently considered unbreakable by most known technologies, but RSA still recommends using the longer 2048-bit key, which should deter even the most powerful super hackers. It is important to note that asymmetric algorithm keys need to be much larger than their symmetric key counterparts to be as effective. For example, a 128-bit symmetric key is essentially equal to a 2304-bit asymmetric key in strength.

The RSA algorithm uses what is known as integer factorization cryptography. It works by first multiplying two distinct prime numbers that cannot be factored. Then it moves on to some more advanced math in order to derive a set of two numbers. Finally, from these two numbers, it creates a private and public key pair.

The private key is used to decrypt data that has been encrypted with the public key. For example, if Alice (User A) sends Bob (User B) a message, Alice can find out

Bob's public key from a central source and encrypt a message to Bob using Bob's public key. When Bob receives it, he decrypts it with his private key.

Bob can also authenticate himself to Alice, for example by using his private key to encrypt a digital certificate. When Alice receives it, she can use his public key to decrypt it. These concepts are summarized in Table 13-4.



**Table 13-4** Summary of RSA Public and Private Key Usage

| Task                           | Which person's key to use | What kind of key |
|--------------------------------|---------------------------|------------------|
| Send an encrypted message      | Receiver's                | Public key       |
| Decrypt an encrypted message   | Receiver's                | Private key      |
| Send an encrypted signature    | Sender's                  | Private key      |
| Decrypt an encrypted signature | Sender's                  | Public key       |

Other examples of RSA encryption include tokens in the form of SecurID USB dongles, and devices such as hardware security modules (HSMs) and trusted platform modules (TPMs). All these devices can store RSA asymmetric keys and can be used to assist in user authentication. RSA key distribution is vulnerable to man-in-the-middle attacks. However, these attacks are defensible through the use of digital certificates and other parts of a PKI system that we detail in the next chapter. It is also susceptible to timing attacks that can be defended against through the use of cryptographic blinding: This blind computation provides encryption without knowing actual input or output information. Due to other types of attacks, it is recommended that a secure padding scheme be used. Padding schemes work differently depending on the type of cryptography. In public key cryptography, padding is the addition of random material to a message to be sufficient, and incorporating a proof, making it more difficult to crack. A padding scheme is always involved, and algorithm makers such as RSA are always releasing improved versions.

In 2000, RSA Security released the RSA algorithm to the public. Therefore, no licensing fees are required if an organization decides to use or modify the algorithm. RSA published a group of standards known as PKCS (Public-Key Cryptography Standards) in an effort to promote its various public key techniques. For example, PKCS #1 defines the mathematical properties of RSA public and private keys. Another example is PKCS #11, which defines how HSMs utilize RSA. The entire list of standards can be found at the following link:

<http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm>

## Diffie-Hellman

The **Diffie-Hellman key exchange**, invented in the 1970s, was the first practical method for establishing a shared secret key over an unprotected communications channel. This asymmetric algorithm was developed shortly before the original RSA algorithm. It is also known as the Diffie-Hellman-Merkle key exchange due to Ralph Merkle's conceptual involvement.

Diffie-Hellman relies on secure key exchange before data can be transferred. This key exchange establishes a shared secret key that can be used for secret communications but over a public network. Originally, fictitious names were chosen for the “users”: Alice and Bob. Basically, Alice and Bob agree to initial prime and base numbers. Then, each of them selects secret integers and sends an equation based on those to each other. Each of them computes the other’s equation to complete the shared secret, which then allows for encrypted data to be transmitted. The secret integers are discarded at the end of the session. These were originally static keys, meaning that they were used for a long period of time.

Diffie-Hellman is considered secure against eavesdroppers due to the difficulty of mathematically solving the Diffie-Hellman problem. However, it is vulnerable to man-in-the-middle attacks. To prevent this, some method of authentication is used such as password authentication. This algorithm is used by the Transport Layer Security (TLS) protocol during encrypted web sessions. When used in this manner, it works in ephemeral mode, meaning that keys are generated during each portion of the key establishment process, and are used for shorter periods of time than with static keys. It is this ephemeral process that achieves *perfect forward secrecy* (PFS), which ensures that the compromise of one message will not lead to the compromise of another message. This ephemeral version of Diffie-Hellman is called DHE, or sometimes Ephemeral Diffie-Hellman (EDH). One of the drawbacks to DHE is that it requires more computational power; however, there is an elliptic curve alternative, which we talk about in the next section.

**NOTE** The Diffie-Hellman algorithm can also be used within a public key infrastructure (PKI), though the RSA algorithm is far more common.

## Elliptic Curve

**Elliptic curve cryptography (ECC)** is a type of public key cryptography based on the structure of an elliptic curve. It uses logarithms calculated against a finite field and is based on the difficulty of certain mathematical problems. It uses smaller keys than most other encryption methods. Keys are created by graphing specific points

on the curve, which were generated mathematically. All parties involved must agree on the elements that define the curve. This asymmetric algorithm has a compact design, leading to reduced computational power compared to other asymmetric algorithms, yet it creates keys that are difficult to crack.

Other algorithms have been adapted to work with elliptic curves, including Diffie-Hellman and the Digital Signature Algorithm (DSA). The Diffie-Hellman version (known as Elliptic Curve Diffie-Hellman, or ECDH) uses elliptic curve public/private key pairs to establish the secret key. Another variant, ECDHE, runs in ephemeral mode, which as previously stated makes sure that a compromised message won't start a chain reaction, and that other messages maintain their integrity. By its very design, the elliptic curve solves the problem of the extra computational power required by DHE. DSA is a U.S. federal government standard public key encryption algorithm used in digital signatures. The elliptic version is known as ECDSA. In general, the size of the public key in an elliptic curve-based algorithm can be 1/6 the size of the non-elliptic curve version. For example, ECDSA has a public key that is 160 bits, but regular DSA uses a public key that is 1024 bits. This is part of the reasoning behind the reduced amount of CPU power needed.

ECC cryptography is used with smart cards, wireless security, and other communications such as VoIP and IPsec (with DSA). It can be susceptible to side channel attacks (SCAs), which are attacks based on leaked information gained from the physical implementation (number and type of curves) of the cryptosystem, and fault attacks (a type of SCA), plus there are concerns about backdoors into the algorithm's random generator. Elliptic curve cryptography (as well as RSA and other algorithms) is also theoretically vulnerable to quantum cryptanalysis-based computing attacks.

### Quantum Cryptography

The quantum computer (as of the writing of this book) is highly theoretical, but quantum encryption is more of a reality. More accurately known as quantum cryptography, it builds on quantum mechanics, and in particular, quantum communications.

In the standard digital encryption scenario, the “key” is established between two parties: One person encodes bits of information, and the other decodes them. Standard bits of information are used (1s and 0s). But in a quantum encryption scenario, the bits of the key can be encoded as quantum data (in which bits can exist in multiple states). This allows information to be encoded in such a way that would otherwise be impossible in classical digital encryption schemes.

Currently, quantum cryptography is a reality only in the form of quantum key distribution (QKD), which does have various protocols based on it. It commonly uses

a fiber channel (fiber-optic matrix) to transmit quantum information, which can be very costly. In fact, the entire procedure is quite expensive and difficult to undertake, making it uncommon. But it is known to have flaws. Let's remember one general rule about security: There is no perfect, utopian, secure solution. Given time, every encryption technique is exploited and its vulnerabilities are exposed. It would follow that quantum encryption is no exception. And so continues the endless cycle of security control > hacking attempt > security control...

## More Encryption Types

We have a couple more encryption types to speak of. They don't quite fit into the other sections, so I figured I would place them here. The first is the one-time pad, and the second is the Pretty Good Privacy (PGP) application and encryption method.

### One-Time Pad

A **one-time pad** (also known as the Vernam cipher, named after the engineer Gilbert Vernam) is a stream cipher that encrypts plaintext with a secret random key that is the same length as the plaintext. It uses a string of bits that is generated at random (known as a keystream). Encryption is accomplished by combining the keystream with the plaintext message using the bitwise XOR operator to produce the ciphertext. Because the keystream is randomized, even an attacker with a plethora of computational resources on hand can only guess the plaintext if the attacker sees the ciphertext.

Unlike other encryption types, it can be computed by hand with a pencil and paper (thus the word “pad” in the name), although today computers will be used to create a one-time pad algorithm for use with technology. It has been proven as impossible to crack if used correctly and is known as being “information-theoretically secure”; it is the only cryptosystem with theoretically perfect secrecy. This means that it provides no information about the original message to a person trying to decrypt it illegitimately. However, issues with this type of encryption have stopped it from being widely used. Because of this, the acronym OTP is more commonly associated with “one-time passwords,” which we talk about later in this chapter.

One of the issues with a one-time pad is that it requires perfect randomness. The problem with computer-based random number generators is that they usually aren't truly random because high-quality random numbers are difficult to generate; instead, they are pseudorandom number generators. Another issue is that the exchange of the one-time pad data must be equal to the length of the message. It also requires proper disposal, which is difficult due to data remanence.

Regardless of these issues, the one-time pad can be useful in scenarios in which two users in a secure environment are required to also communicate with each other from two other separate secure environments. The one-time pad is also used in superencryption (or multiple encryption), which is encrypting an already encrypted message. In addition, it is commonly used in quantum cryptography, which uses quantum mechanics to guarantee secure communications. These last two concepts are far beyond the Security+ exam, but they show the actual purpose for this encryption type.

## PGP

**Pretty Good Privacy (PGP)** is an encryption program used primarily for signing, encrypting, and decrypting e-mails in an attempt to increase the security of e-mail communications. You might remember that we previously discussed weaknesses of e-mail client programs when sending via POP3 and SMTP servers. PGP uses (actually wrote) the encryption specifications as shown in the OpenPGP standard; other similar programs use this as well. Today, PGP has an entire suite of tools that can encrypt e-mail, accomplish whole disk encryption, and encrypt zip files and instant messages. PGP uses a symmetric session key (also referred to as a preshared key, or PSK), and as such, you might hear PGP referred to as a program that uses symmetric encryption, but it also uses asymmetric RSA for digital signatures and for sending the session key. Because of this it is known as a hybrid cryptosystem, combining the best of conventional systems and public key cryptography.

When encrypting data, PGP uses key sizes of at least 128 bits. Newer versions allow for RSA or DSA key sizes ranging from 512 bits to 2048 bits. The larger the key, the more secure the encryption is, but the longer it takes to generate the keys; although, this is done only once when establishing a connection with another user. The program uses a combination of hashing, data compression, symmetric key cryptography, and public key cryptography. New versions of the program are not fully compatible with older versions because the older versions cannot decrypt the data that was generated by a newer version. This is one of the issues when using PGP; users must be sure to work with the same version. Newer versions of PGP support OpenPGP and S/MIME, which allows for secure communications with just about everyone.

Because it works with RSA, the security of PGP is based on the key size. It is considered secure and uncrackable as long as a sufficient key size is used. As an example, it has been suggested that a 2048-bit key should be safe against the strongest of well-funded adversaries with knowledgeable people and the latest in supercomputers until at least the year 2020; 1024-bit keys are considered strong enough for all but the most sensitive data environments.

Around the turn of the millennium, the creator of PGP, and many other security-minded people that used PGP, sensed that an open source alternative would be beneficial to the cryptographic community. This was presented to, and accepted by, the IETF, and a new standard called OpenPGP was developed. With this open source code, others could write software that could easily integrate with PGP. One example of this is the GNU Privacy Guard (abbreviated as GNuPG, or simply GPG), which is compliant with the OpenPGP standard. Over time this has been developed for several platforms including various Linux GUIs, OS X, and Windows. GPG is a combination of symmetric key encryption and public key encryption.

PGP and its derivatives are used by many businesses and individuals worldwide so that files can be easily encrypted before transit. The original PGP (developed by Philip Zimmerman) has changed hands several times and, as of this writing, is owned by Symantec, which offers it as part of its products (for a fee). There are also several versions of PGP, as well as GNuPG, available for download for free. A good starting point for links to all of the latest packages is The International PGP Home Page: <http://www.pgpi.org/>.

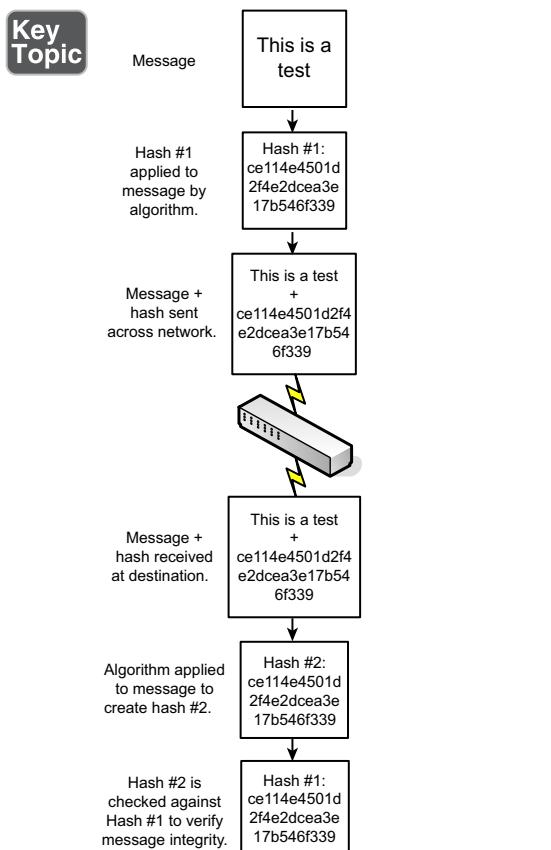
### AI and Genetic Algorithms

Algorithms are also used in the world of artificial intelligence, often by searching for particular information within a vast array of data. One example of this is the genetic algorithm, a type of evolutionary algorithm, which is inspired by natural, biological evolution. Algorithms such as this are programmed with languages like Python and C++.

A genetic algorithm can be used to identify a person from a very broad set of information. This could be based on a set of data gathered via data aggregation, or—and this is related to the book you are reading—it could involve stylometry. Stylometry is the study of linguistic style, music, and other forms of communication. It could be used to identify the author of this book without knowing any reference to the author, or to identify a songwriter. You know, name that tune in three notes!—except a computer does the naming. It's based on style and specific words (and their usage frequency) employed by the writer. A genetic algorithm used in stylometric analysis applies a set of rules (IF-THEN statements). It helps to know a key word that the writer uses somewhat frequently. For example, the word "known": In a chapter such as this, with 10,000 words, I might use that word 30 times. The rule could be "If the word *known* appears 3 or more times per every 1000 words, then the author is X." In this case, X would equal David L. Prowse, me, and possibly several other technical authors. Stylometry has its uses in identification, but can also be used to provide statistical analysis; for example, perhaps I should cut back on the word *known!* It might help to know overused words when a book such as this can commonly reach 2 million keystrokes. But more often than not it is used for identification of anonymous works. Stylometry is just one of many examples of applications that use genetic algorithms.

## Hashing Basics

A **hash** is a summary of a file or message, often in numeric format. Hashes are used in digital signatures, in file and message authentication, and as a way to protect the integrity of sensitive data; for example, data entered into databases, or perhaps entire hard drives. A hash is generated through the use of a hash function to verify the integrity of the file or message, most commonly after transit over a network. A **hash function** is a mathematical procedure that converts a variable-sized amount of data into a smaller block of data. The hash function is designed to take an arbitrary data block from the file or message, use that as an input, and from that block produce a fixed-length hash value. Basically, the hash is created at the source and is recalculated and compared with the original hash at the destination. Figure 13-2 illustrates this process. Note the hash that was created starting with ce114e and so on. This is the summary, or message digest, of the file to be sent. It is an actual representation of an MD5 hash (covered shortly) of a plaintext file with the words “This is a test,” as shown in the message portion of Figure 13-2.



**Figure 13-2** Illustration of the Hashing Process

Because the hash is a condensed version of the file/message, or a portion of it, it is also known as a message digest. It provides integrity to data so that a user knows that the message is intact, hasn't been modified during transit, and comes from the source the user expects. A hash can fall into the category of a **one-way function**. This means it is easy to compute when generated but difficult (or impossible) to compute in reverse. In the case of a hash, a condensed version of the message, initial computation is relatively easy (compared to other algorithms), but the original message should not be re-created from the hash. Contrast this concept to encryption methods that indeed can be reversed. A hash can be created without the use of an algorithm, but generally, the ones used in the field require some kind of cryptographic algorithm.

## Cryptographic Hash Functions

**Cryptographic hash functions** are hash functions based on block ciphers. The methods used resemble that of cipher modes used in encryption. Examples of cryptographic hash functions include MD5 and SHA.

### MD5

The **Message-Digest algorithm 5 (MD5)** is the newest of a series of algorithms designed by Ron Rivest. It uses a 128-bit key. This is a widely used hashing algorithm; at some point you have probably seen MD5 hashes when downloading files. This is an example of the attempt at providing integrity. By checking the hash produced by the downloaded file against the original hash, you can verify the file's integrity with a level of certainty. However, MD5 hashes are susceptible to collisions. A collision occurs when two different files end up using the same hash. Due to this low collision resistance, MD5 is considered to be harmful today. MD5 is also vulnerable to threats such as rainbow tables and pre-image attacks. The best solution to protect against these attacks is to use a stronger type of hashing function such as SHA-2 or higher.

### SHA

The **Secure Hash Algorithm (SHA)** is one of a number of hash functions designed by the U.S. National Security Agency (NSA) and published by the NIST. They are used widely in the United States government. SHA-1 is the most commonly used version, which employs a 160-bit hash, which is reasonably secure but uses a lot of resources on the computer generating the hash. SHA-2 is more secure; it has 256-bit and 512-bit block sizes but uses even more resources and is less widely accepted. Keccak was selected from a group of algorithms in 2012 as the SHA-3 winner, but

is not meant as a replacement for SHA-2, because no compromise of SHA-2 has yet been demonstrated.

It is important that a hashing algorithm be collision-resistant. If it has the capability to avoid the same output from two guessed inputs (by a hacker attempting a collision attack), it is collision-resistant. When it comes to cryptography, “perfect hashing” is not possible because usually unknowns are involved, such as the data to be used to create the hash, and what hash values have been created in the past. Though perfect is not possible, it is possible to increase collision resistance by using a more powerful hashing algorithm.

Because MD5 and SHA-1 have vulnerabilities, some government agencies started using SHA-2 in 2011 (and most likely will use SHA-3 at some point).

## RIPEMD and HMAC

RIPEMD stands for the RACE Integrity Primitives Evaluation Message Digest. The original RIPEMD (128-bit) had a collision reported, and therefore it is recommended to use RIPEMD-160 (160-bit), RIPEMD-256, or RIPEMD-320. The commonly used RIPEMD-160 is a 160-bit message digest algorithm used in cryptographic hashing. It is used less commonly than SHA-1 and was designed as an open source hashing algorithm.

HMAC stands for Hash-based Message Authentication Code. Let’s step back for a moment: Message Authentication Code (MAC) is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. Building on this concept, HMAC is a calculation of a MAC through the use of a cryptographic hash function such as MD5 or SHA-1. If for example SHA-1 is used, the corresponding MAC would be known as HMAC-SHA1.

## Happy Birthday!

Not when a birthday attack is involved. A **birthday attack** is an attack on a hashing system that attempts to send two different messages with the same hash function, causing a collision. It is based on the birthday problem in probability theory (also known as the birthday paradox). This can be summed up simply as the following: A randomly chosen group of people will have a pair of persons with the same calendar date birthday. Given a standard calendar year of 365 days, the probability of this occurring with 366 people is 100% (367 people on a leap year). So far, this makes sense and sounds logical.

The paradox (thoughtfully and mathematically) comes into play when fewer people are involved. With only 57 people, there is a 99% probability of a match (a much

higher percentage than one would think), and with only 23 people, there is a 50% probability. Imagine that and blow out your candles! And by this, I mean use hashing functions with strong collision resistance. Because if attackers can find any two messages that digest the same way (use the same hash value), they can deceive a user into receiving the wrong message. To protect against a birthday attack, use a secure transmission medium, such as SSH, or encrypt the entire message that has been hashed.

## LANMAN, NTLM, and NTLMv2

Passwords can also be hashed using algorithms. Some password hashes are more secure than others, whereas older ones have been cracked and are therefore compromised. This section details the Windows-based LANMAN, NTLM, and NTLMv2 hashes starting from the oldest. These three types of authentication are what attempts to make your login to the computer secure, unless you log in to a domain where Kerberos is used by default.

### LANMAN

The **LANMAN hash**, also known as the LAN Manager hash or simply LM hash, was the original hash used to store Windows passwords. It was used in Windows operating systems before Windows NT but is supported by some versions of Windows as a legacy backward in the attempt to be backward compatible. This backward compatibility can be a security risk because the LM hash has several weaknesses and can be cracked easily.

Its function is based on the deprecated DES algorithm and can only be a maximum of 14 characters. These weaknesses are compounded by the fact that the ASCII password is broken into two pieces, one of which is converted to uppercase, essentially removing a large portion of the character set. Plus, it can store a maximum of only seven uppercase characters. Due to this, brute-force attacks can crack alphanumeric LM hashes in a matter of hours.

Due to all these weaknesses, it is highly recommended that the LANMAN hash be disabled on operating systems that run it by default. It should also be checked on operating systems such as Windows Vista/Server 2008 and higher that are supposed to have it disabled by default, just in case the setting was modified.

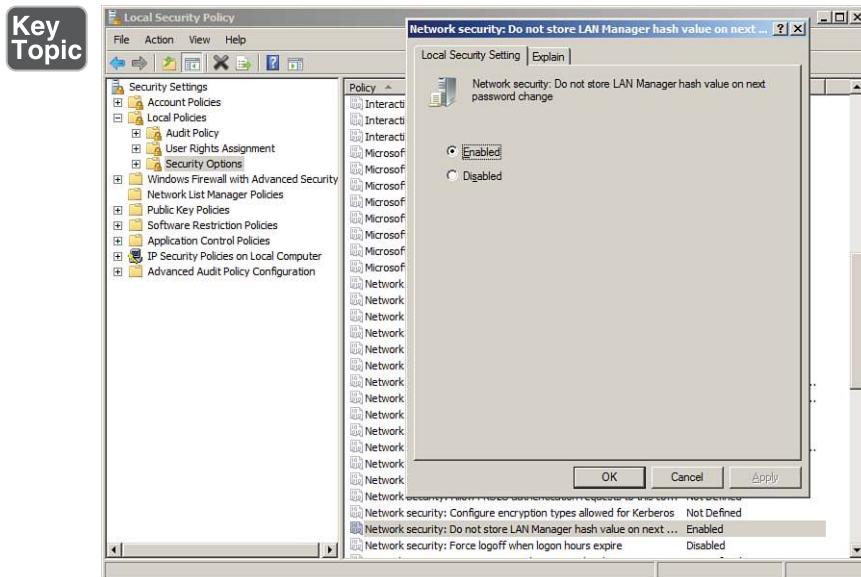
The following step-by-step procedure shows how to disable the storage of LM hashes in Windows:

- Step 1.** Open the Run prompt and type `secpol.msc` to display the Local Security Policy window.

**Step 2.** Navigate to Local Policies > Security Options.

**Step 3.** In the right pane, double-click the policy named Network Security: Do Not Store LAN Manager Hash Value on Next Password Change.

**Step 4.** Click Enabled (if it isn't already), as shown in Figure 13-3, and click OK.



**Figure 13-3** LM Hash in the Local Group Policy

**NOTE** For Windows Server domain controllers, you need to access the Group Policy Editor, not Local Group Policy. Generally, this would be done at the default domain policy, but it could also be accomplished at a single OU's policy, if necessary.

You can also disable the storage of LM hash passwords by modifying the Registry. This process is necessary for older versions of Windows. For more information, see the link to Microsoft's website in the "View Recommended Resources" document on the accompanying disc.

If, for whatever reason, the storing of LM hashes for passwords cannot be turned off, Microsoft recommends using a 15-character-minimum password. When this is done, an LM hash and an NTLM hash value are stored. In this situation, the LM hash cannot be used solely to authenticate the user; therefore, it cannot be solely cracked. The NTLM hash would have to be cracked as well. Because 15 characters

might be beyond some organizations' policies—or some users' ability, for that matter—it is highly recommended that the LM hash policy be disabled.

## NTLM and NTLMv2

Well, we talked a lot about why the LM hash is insufficient. Let's get into the replacements. The first is **NTLM hash**, also known as the NT LAN Manager hash. The NTLM algorithm was first supplied with Windows NT 3.1; it provides Unicode support and, more important to this conversation, the RC4 cipher. Although the RC4 cipher enables a more powerful hash known as NTLM for storing passwords, the systems it ran on were still configured to be backward compatible with the LM hash. So, as long as the LM hash was not disabled, those systems were still at the same risk as older systems that ran the LM hash only. Windows Vista and Windows 2008 operating systems (and higher) disable the older LM hash by default.

While NTLM uses cyclic redundancy checks (CRCs) and message digest algorithms for integrity, the main issue with NTLM is that it is based on the RC4 cipher, and not any recent cryptographic methods such as AES or SHA-256. RC4 has been compromised, and therefore the NTLM hash is compromised. Due to the weakness of NTLM, we need a stronger hashing algorithm: NTLMv2.

**NTLMv2** uses the MD5 hash, making it difficult to crack; it is a 128-bit system. NTLMv2 has been available since Windows NT 4.0 SP4 and is used by default on newer Windows operating systems. Even though NTLMv2 responds to the security issues of the LM hash and NTLM, most Microsoft domains use Kerberos as the logon authentication scheme because of its level of security when dealing with one computer logging in to another or in to an entire network.

## Additional Password Hashing Concepts

Remember that hashed passwords are one-way functions. The process of hashing takes the password and converts it into a fixed-length binary value that cannot be reversed. The converted number is usually represented in hexadecimal. Due to the nature of the conversion, even slightly different passwords will have completely different hashes.

Know that password hashes can be cracked. I know, I said the number cannot be reversed, and it can't, because it is a one-way function. But the hash can be cracked in a variety of ways. A person could try to guess the password, or use the dictionary attack method, or try the brute-force attack method. Hackers will also make use of lookup tables, reverse lookup tables, and rainbow tables. These vulnerabilities make your password policies—and the type of hash you use—very important. Of course, in some scenarios, you might be limited as to the length of password you can have

your users select. For example, let's say you are using a web server technology with a somewhat weak password methodology, and you are concerned about hash collisions. There are other ways to increase the security of the password.

One way is to use key stretching. A **key stretching** technique will take a weak key, process it, and output an enhanced and more powerful key. Often, this process will increase the size of the key to 128 bits, making attacks such as brute-force attacks much more difficult, if not impossible. Examples of key stretching software include PBKDF2 and bcrypt.

Bcrypt also incorporates salting to protect against dictionary attacks and rainbow table attacks. Salting is additional random data that is added to a one-way cryptographic hash. It is one character or more, but defined in bits. The person with the weaker web server password key, or perhaps the admin with the NTLM hash, would do well to consider key stretching or salting. Another technique used is the *nonce* (number used once). It can be added to password-based authentication schemes where a secure hash function (such as SHA) is used. It is a unique number (that is difficult for attackers to find) that can only be used once. As such, it helps to protect users from replay attacks.

Of course, an admin needs to remember that the primary line of defense when it comes to passwords is to use complexity *and* length; not just one or the other. There are a couple of myths connected with passwords in general. The first is that complexity is better than length. This isn't always true; it will depend on the type of attack (dictionary or brute-force), the level of complexity, and the length of the password. So again, if at all possible, define policies that specify complexity plus length. And if length cannot be incorporated into your password scheme, use key stretching, or salting, or strongly consider using a different hash altogether. Another myth is that password checkers ensure strong passwords. Password checkers can help you get an idea of whether a password is secure, but may interpret some weak passwords as strong.

Remember also to limit the number of times that a password can be tried via policy; for example, limiting password attempts to five or even as little as three (remember the three strikes and you're out rule?). Also, define delays between consecutive password attempts. This is especially important on websites. It can help to defend against exhaustive key searches. Better yet, use one-time passwords (OTPs), such as the HMAC-based OTP (HOTP). Extend that concept by supporting a time-based moving factor that must be changed each time a new password is generated, and you have the time-based OTP (TOTP).

It may seem like we've covered a dizzying array of password technologies and acronyms, but we can quickly get our bearings by creating a checklist and going through it every time we design a password scheme: Use a strong hash, and if not possible,

utilize key lengthening. Incorporate salting. Consider OTPs, and create meticulously defined policies governing passwords. Finally, if working on a website that accepts passwords (especially public passwords), implement secure programming techniques, particularly input validation.

## Chapter Summary

If there's one thing you should take away from this chapter it's that my phone number was probably never in any black books, either as plaintext or as ciphertext! (Just making sure you are reading the chapter summaries...be thankful I am not anthropomorphizing computers this time.) Seriously, though, it's amazing how many children can easily understand and design code with which to hide information. It's not surprising that there are so many cryptographers and cryptanalysts in this day and age, and a huge assortment of ciphers to work with.

The art of secret communication can basically be broken down into two categories: steganography and cryptography. Both have been used for millennia. But one is inherently insecure, and the other is inherently crackable. Steganography hides the entire message, but if the message is found, the message is instantly compromised. Remember the discussion of the Greek messenger who shaved his head, had a message written on his scalp, and re-grew his hair? If he had been asked by a guard at a border to shave his head (and had complied), the message would have been seen right away. That's why insecurity is built right into the scheme. Cryptography, on the other hand, is used to hide the *meaning* of the message. The message could be there for everyone to see, but they won't understand it unless they have the *key* to the message. Of course, all ciphers can be cracked; it's built into their DNA, so to speak. But, with the proper key size and appropriately designed ciphers, it can be very difficult, if not impossible, to crack the code. So encryption is the weapon of choice for most data transfers.

However, you will also see some scenarios where a message is encrypted and then hidden as well, effectively combining the two concepts of cryptography and steganography. For example, User A might e-mail User B with an attachment containing a photo of the Grand Canyon—a slightly altered Grand Canyon, where some of the pixels' colors have been changed, but the changes are not visible to the naked eye. User B already has an unaltered version of the original photo stored on the computer. User B compares the two, and locates all of the modified pixels (or has a program do it). The modified colors could translate to letters in the alphabet: for example, a certain shade of red's three-byte color would be written numerically as FF 00 66 (255 0 102 in decimal). It could have been decided earlier that the third number of the three bytes would be the modified color. Furthermore, 102 is equal to the letter *f* in ASCII, which might be the first letter of the first sentence of a message.

The process would continue until the complete message emerges from a group of modified colors. That's pretty hidden, wouldn't you say? But now, encryption could be employed based on a predetermined code. It could be as simple as a Caesar Cipher where the letters are shifted over three places, so instead of the ciphertext  $f$ , we get the plaintext  $c$ . So now, the message is hidden *and* the meaning of the message is hidden. And we can get as complex as we want with the cipher, either by utilizing a published algorithm or by designing our own.

Dating back to ancient times, cryptographers would create a code, and cryptanalysts would attempt to crack it. Every time a code was cracked, it was then considered compromised, and a new code would be created. This concept has been even more pronounced during the computer age. That's why there are so many algorithms in this chapter—the cyclic mousetrap effect has been in play for decades.

Symmetric algorithms use a single key, or more than one identical key (or very similar keys). One of the most powerful symmetric algorithms is the Advanced Encryption Standard (AES), which can have a maximum key length of 256 bits. That is considered uncrackable, so instead of trying to crack the code, attackers will usually attempt to maneuver around it and assault the implementation of the algorithm. Asymmetric algorithms, on the other hand, use a pair of different keys for encryption and decryption. For instance, take public key cryptography, where there will be a well-known public key that is used to encrypt messages, and a secret private key that is used to decrypt them. A common example of an asymmetric algorithm is RSA.

It is often desirable to create a summary of a message, known as a hash. Hashes are used in digital downloads to allow users to verify the integrity of a message or file. They are also used to protect passwords. A common hash used on the Internet is SHA-2. A common hash used to protect passwords in Windows is NTLMv2.

By combining all of these techniques and technologies, you can provide a decent amount of security for your files and passwords—essentially protecting your data *and* the access to that data.

## 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 13-5 lists a reference of these key topics and the page number on which each is found.

**Table 13-5** Key Topics for Chapter 13

| Key Topic Element | Description                                 | Page Number |
|-------------------|---------------------------------------------|-------------|
| Table 13-1        | Black book phone number encryption          | 508         |
| Figure 13-1       | Illustration of public key cryptography     | 514         |
| Table 13-3        | Summary of symmetric algorithms             | 519         |
| Table 13-4        | Summary of RSA Public and Private Key Usage | 520         |
| Figure 13-2       | Illustration of the hashing process         | 526         |
| Figure 13-3       | LM hash in the Local Group Policy           | 530         |

## Define Key Terms

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

cryptography, encryption, cipher, algorithms, key, private key, public key, symmetric key algorithm, stream cipher, block cipher, asymmetric key algorithm, public key cryptography, digital signature, certificate, steganography, Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), RSA, Diffie-Hellman key exchange, elliptic curve cryptography (ECC), one-time pad, Pretty Good Privacy (PGP), hash, hash function, one-way function, cryptographic hash functions, Message-Digest algorithm 5 (MD5), Secure Hash Algorithm (SHA), birthday attack, LANMAN hash, NTLM hash, NTLMv2 hash, key stretching

## Review Questions

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

- Which of the following is the proper order of functions for asymmetric keys?
  - Decrypt, validate, and code and verify
  - Sign, encrypt, decrypt, and verify
  - Encrypt, sign, decrypt, and verify
  - Decrypt, decipher, and code and encrypt
- Which type of encryption technology is used with the BitLocker application?
  - Symmetric
  - Asymmetric

- C.** Hashing
  - D.** WPA2
3. Which of the following will provide an integrity check?
- A.** Public key
  - B.** Private key
  - C.** WEP
  - D.** Hash
4. Why would a hacker use steganography?
- A.** To hide information
  - B.** For data integrity
  - C.** To encrypt information
  - D.** For wireless access
5. You need to encrypt and send a large amount of data. Which of the following would be the best option?
- A.** Symmetric encryption
  - B.** Hashing algorithm
  - C.** Asymmetric encryption
  - D.** PKI
6. Imagine that you are a hacker. Which would be most desirable when attempting to compromise encrypted data?
- A.** A weak key
  - B.** The algorithm used by the encryption protocol
  - C.** Captured traffic
  - D.** A block cipher
7. An SHA algorithm will have how many bits?
- A.** 64
  - B.** 128
  - C.** 512
  - D.** 1024

8. What is another term for secret key encryption?
  - A. PKI
  - B. Asymmetrical
  - C. Symmetrical
  - D. Public key
9. Your boss wants you to set up an authentication scheme in which employees will use smart cards to log in to the company network. What kind of key should be used to accomplish this?
  - A. Private key
  - B. Public key
  - C. Cipher key
  - D. Shared key
10. The IT director wants you to use a cryptographic algorithm that cannot be decoded by being reversed. Which of the following would be the best option?
  - A. Asymmetric
  - B. Symmetric
  - C. PKI
  - D. One-way function
11. Which of the following concepts does the Diffie-Hellman algorithm rely on?
  - A. Usernames and passwords
  - B. VPN tunneling
  - C. Biometrics
  - D. Key exchange
12. What does steganography replace in graphic files?
  - A. The least significant bit of each byte
  - B. The most significant bit of each byte
  - C. The least significant byte of each bit
  - D. The most significant byte of each bit

- 13.** What does it mean if a hashing algorithm creates the same hash for two different downloads?
  - A.** A hash is not encrypted.
  - B.** A hashing chain has occurred.
  - C.** A one-way hash has occurred.
  - D.** A collision has occurred.
- 14.** Which of the following methods will best verify that a download from the Internet has not been modified since the manufacturer released it?
  - A.** Compare the final LANMAN hash with the original.
  - B.** Download the patch file over an AES encrypted VPN connection.
  - C.** Download the patch file through an SSL connection.
  - D.** Compare the final MD5 hash with the original.
- 15.** Which of the following encryption methods deals with two distinct, large prime numbers and the inability to factor those prime numbers?
  - A.** SHA-1
  - B.** RSA
  - C.** WPA
  - D.** Symmetric
- 16.** Which of the following is not a symmetric key algorithm?
  - A.** RC4
  - B.** ECC
  - C.** 3DES
  - D.** Rijndael
- 17.** You are attempting to move data to a USB flash drive. Which of the following enables a rapid and secure connection?
  - A.** SHA-1
  - B.** 3DES
  - C.** AES-256
  - D.** MD5

- 18.** Which of the following is used by PGP to encrypt the session key before it is sent?
- A.** Asymmetric key distribution system
  - B.** Asymmetric scheme
  - C.** Symmetric key distribution system
  - D.** Symmetric scheme
- 19.** Which of the following encryption algorithms is used to encrypt and decrypt data?
- A.** SHA-1
  - B.** RC5
  - C.** MD5
  - D.** NTLM
- 20.** Of the following, which statement correctly describes the difference between a secure cipher and a secure hash?
- A.** A hash produces a variable output for any input size; a cipher does not.
  - B.** A cipher produces the same size output for any input size; a hash does not.
  - C.** A hash can be reversed; a cipher cannot.
  - D.** A cipher can be reversed; a hash cannot.
- 21.** When encrypting credit card data, which would be the most secure algorithm with the least CPU utilization?
- A.** AES
  - B.** 3DES
  - C.** SHA-1
  - D.** MD5
- 22.** A hash algorithm has the capability to avoid the same output from two guessed inputs. What is this known as?
- A.** Collision resistance
  - B.** Collision strength
  - C.** Collision cipher
  - D.** Collision metric

- 23.** Which of the following is the weakest encryption type?
- A.** DES
  - B.** RSA
  - C.** AES
  - D.** SHA
- 24.** Give two examples of hardware devices that can store keys. (Select the two best answers.)
- A.** Smart card
  - B.** Network adapter
  - C.** PCI Express card
  - D.** USB flash drive
- 25.** What type of attack sends two different messages using the same hash function, which end up causing a collision?
- A.** Birthday attack
  - B.** Bluesnarfing
  - C.** Man-in-the-middle attack
  - D.** Logic bomb
- 26.** Why would a hacker use steganography?
- A.** To hide information
  - B.** For data integrity
  - C.** To encrypt information
  - D.** For wireless access
- 27.** Which of the following might a public key be used to accomplish?
- A.** To decrypt the hash of a digital signature
  - B.** To encrypt web browser traffic
  - C.** To digitally sign a message
  - D.** To decrypt wireless messages

- 28.** You scan a computer for weak passwords and discover that you can figure out the password by cracking the first seven characters and then cracking the second part of the password separately. What type of hash is being used on the computer?
- A.** MD5
  - B.** SHA-1
  - C.** LANMAN
  - D.** NTLMv2
- 29.** WEP improperly uses an encryption protocol and because of this is considered to be insecure. What encryption protocol does it use?
- A.** AES
  - B.** RSA
  - C.** RC6
  - D.** RC4
- 30.** The fundamental difference between symmetric key systems and asymmetric key systems is that the symmetric key system will:
- A.** Use the same key on each end
  - B.** Use different keys on each end
  - C.** Use multiple keys for non-repudiation purposes
  - D.** Use public key cryptography
- 31.** Last week, one of the users in your organization encrypted a file with a private key. This week the user left the organization, and unfortunately the systems administrator deleted the user's account. What are the most probable outcomes of this situation? (Select the two best answers.)
- A.** The data is not recoverable.
  - B.** The former user's account can be re-created to access the file.
  - C.** The file can be decrypted with a PKI.
  - D.** The data can be decrypted using the recovery agent.
  - E.** The data can be decrypted using the root user account.

- 32.** You are tasked with ensuring that messages being sent and received between two systems are both encrypted and authenticated. Which of the following protocols accomplishes this?
- A.** Diffie-Hellman
  - B.** BitLocker
  - C.** RSA
  - D.** SHA-1
- 33.** Which of the following is not a valid cryptographic hash function?
- A.** RC4
  - B.** SHA-512
  - C.** MD5
  - D.** RIPEMD
- 34.** A network stream of data needs to be encrypted. Jason, a security administrator, selects a cipher that will encrypt 128 bits at a time before sending the data across the network. Which of the following has Jason chosen?
- A.** Stream cipher
  - B.** Block cipher
  - C.** Hashing algorithm
  - D.** RC4
- 35.** You are tasked with selecting an asymmetric encryption method that allows for the same level of encryption strength, but with a lesser key length than is typically necessary. Which encryption method fulfills your requirement?
- A.** RSA
  - B.** ECC
  - C.** DHE
  - D.** Twofish

## Answers and Explanations

- 1. C.** The proper order of functions for asymmetric keys is as follows: encrypt, sign, decrypt, and verify. This is the case when a digital signature is used to authenticate an asymmetrically encrypted document.

2. **A.** BitLocker uses symmetric encryption technology based on AES. Hashing is the process of summarizing a file for integrity purposes. WPA2 is a wireless encryption protocol.
3. **D.** A hash provides integrity checks, for example, MD5 hash algorithms. Public and private keys are the element of a cipher that allows for output of encrypted information. WEP (Wired Equivalent Privacy) is a deprecated wireless encryption protocol.
4. **A.** Steganography is the act of writing hidden messages so that only the intended recipients know of the existence of the message. This is a form of security through obscurity. Steganographers are not as concerned with data integrity or encryption because the average person shouldn't even know that a message exists. Although steganography can be accomplished by using compromised wireless networks, it is not used to gain wireless access.
5. **A.** Symmetric encryption is the best option for sending large amounts of data. It is superior to asymmetric encryption. PKI is considered an asymmetric encryption type, and hashing algorithms don't play into sending large amounts of data.
6. **A.** The easiest way for a hacker to get at encrypted data is if that encrypted data has a weak encryption key. The algorithm isn't of much use to a hacker unless it has been broken, which is a far more difficult process than trying to crack an individual key. Captured traffic, if encrypted, still needs to be decrypted, and a weak key will aid in this process. The block cipher is a type of algorithm.
7. **C.** SHA-2 algorithm blocks have 512 bits. SHA-1 is 160-bit. MD5 is 128-bit; 1024-bit keys are common in asymmetric encryption.
8. **C.** Symmetric key encryption uses a secret key. The term symmetric key is also referred to as the following: private key, single key, and shared key (and sometimes as session key). PKI and public keys at their core are asymmetrical.
9. **A.** A private key should be used by users when logging in to the network with their smart card. The key should certainly not be public. A key actually determines the function of a cipher. Shared key is another term for symmetric key encryption but does not imply privacy.
10. **D.** In cryptography, the one-way function is one option of an algorithm that cannot be reversed, or is difficult to reverse, in an attempt to decode data. An example of this would be a hash such as SHA-2, which creates only a small hashing number from a portion of the file or message. There are ways to crack asymmetric and symmetric encryptions, which enable complete decryption (decoding) of the file.

11. **D.** The Diffie-Hellman algorithm relies on key exchange before data can be sent. Usernames and passwords are considered a type of authentication. VPN tunneling is done to connect a remote client to a network. Biometrics is the science of identifying people by one of their physical attributes.
12. **A.** Steganography replaces the least significant bit of each byte. It would be impossible to replace a byte of each bit, because a byte is larger than a bit; a byte is eight bits.
13. **D.** If a hashing algorithm generates the same hash for two different messages within two different downloads, a collision has occurred and the implementation of the hashing algorithm should be investigated.
14. **D.** The purpose of the MD5 hash is to verify the integrity of a download. SHA is another example of a hash that will verify the integrity of downloads. LANMAN hashes are older, deprecated hashes used by Microsoft LAN Manager for passwords. Encrypted AES and SSL connections are great for encrypting the data transfer but do not verify integrity.
15. **B.** The RSA encryption algorithm uses two prime numbers. If used properly they will be large prime numbers that are difficult or impossible to factor. SHA-1 is an example of a Secure Hash Algorithm. WPA is the Wi-Fi Protected Access protocol, and RSA is an example of an asymmetric method of encryption.
16. **B.** ECC (elliptic curve cryptography) is an example of public key cryptography that uses an asymmetric key algorithm. All the other answers are symmetric key algorithms.
17. **C.** AES-256 enables a quick and secure encrypted connection for use with a USB flash drive. It might even be used with a whole disk encryption technology, such as BitLocker. SHA-1 and MD5 are examples of hashes. 3DES is an example of an encryption algorithm but would not be effective for sending encrypted information in a highly secure manner and quickly to a USB flash drive.
18. **D.** Pretty Good Privacy (PGP) encryption uses a symmetric key scheme for the session key data, and asymmetric RSA for the *sending* of the session key, plus a combination of hashing and data compression. Key distribution systems are part of an entire encryption scheme, which typically includes a technology such as Kerberos (key distribution center) or quantum cryptography.
19. **B.** RC5 (Rivest Cipher version 5) can encrypt and decrypt data. SHA-1 and MD5 are used as hashing algorithms, and NTLM (NT LAN Manager) is used by Microsoft as an authentication protocol and a password hash.

- 20.** **D.** Ciphers can be reverse engineered but hashes cannot when attempting to re-create a data file. Hashing is not the same as encryption; hashing is the digital fingerprint, so to speak, of a group of data. Hashes are not reversible.
- 21.** **A.** AES (Advanced Encryption Standard) is fast and secure, more so than 3DES. SHA-1 and MD5 are hashing algorithms. Not listed is RSA, which is commonly implemented to secure credit card transactions.
- 22.** **A.** A hash is collision resistant if it is difficult to guess two inputs that hash to the same output.
- 23.** **A.** DES (Data Encryption Standard) was developed in the 1970s; its 56-bit key has been superseded by 3DES (max 168-bit key) and AES (max 256-bit key). DES is now considered to be insecure for many applications. RSA is definitely stronger than DES even when you compare its asymmetric strength to a relative symmetric strength. SHA is a hashing algorithm.
- 24.** **A. and D.** Smart cards and USB flash drives can be used as devices that carry a token and store keys; this means that they can be used for authentication to systems, often in a multifactor authentication scenario. Network adapters and PCI Express cards are internal to a PC and would not make for good key storage devices.
- 25.** **A.** A birthday attack exploits the mathematics behind the birthday problem in probability theory. It deals with two different messages using the same hash function, generating the same message digest. Bluesnarfing deals with Bluetooth devices. The man-in-the-middle attack is when a person or computer intercepts information between a sender and the receiver. A logic bomb is a malicious attack set to go off at a particular time; often it is stored on a zombie computer.
- 26.** **A.** Steganography is the act of writing hidden messages so that only the intended recipients will know of the existence of the message. This is a form of security through obscurity. Data integrity is accomplished through the use of hashing. Steganography is not the same as cryptography in that it doesn't care whether a person sees the original message.
- 27.** **A.** Public keys can be used to decrypt the hash of a digital signature. Session keys are used to encrypt web browser traffic. Private keys are used to digitally sign a message and decrypt wireless messages.
- 28.** **C.** The LANMAN hash is a deprecated cryptographic hash function that breaks the password into two parts, the first of which is only seven characters. Due to the LANMAN hash's weakness, NTLMv2 is recommended. MD5 and SHA-1 are more powerful cryptographic hash functions that do not have this problem.

- 29. D.** RC4 has several vulnerabilities when used incorrectly by protocols such as WEP. WEP does not use AES, RSA, or RC6, all of which are secure protocols if used correctly.
- 30. A.** Symmetric key systems use the same key on each end during transport of data. Asymmetric key systems (such as public key cryptography systems) use different keys.
- 31. A. and D.** Many systems have a recovery agent that is designed just for this purpose. If the account that encrypted the file is deleted, it cannot be re-created (without different IDs and therefore no access to the file), and the recovery agent will have to be used. If there is no recovery agent (which in some cases needs to be configured manually), then the file will be unrecoverable. This file was encrypted with a private key and needs to be decrypted with a private key—PKI is a system that uses asymmetric key pairs (private and public). The root user account does not have the ability to recover files that were encrypted by other users.
- 32. C.** RSA can both encrypt and authenticate messages. Diffie-Hellman encrypts only. BitLocker is a type of whole disk encryption (WDE), which deals with encrypting entire hard drives but is not used to send and receive messages. SHA-1 is a cryptographic hash function used to preserve the integrity of files.
- 33. A.** RC4 is a symmetric encryption algorithm that uses a stream cipher. It is the only listed answer that is not a valid cryptographic hash function.
- 34. B.** Jason chose a block cipher; for example, the 128-bit version of AES. Don't let the phrase "network stream" fool you; stream ciphers will encrypt each bit in the stream. Hashing algorithms are not used to encrypt network streams of data. RC4 is a stream cipher.
- 35. B.** The ECC (elliptic curve cryptography) method allows for lesser key lengths but at the same level of strength as other asymmetric methods. This reduces the computational power needed. RSA and Diffie-Hellman require more computational power due to the increased key length. DHE especially uses more CPU power because of the ephemeral aspect. (ECDHE would be the solution in that respect.) Twofish is a symmetric algorithm.

## Case Studies for Chapter 13

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

### Case Study 13-1: Understanding Symmetric and Asymmetric Algorithms

**Scenario:** You have been tasked with selecting cryptographic algorithms for internal storage and for Internet-based transmissions. Select the strongest symmetric and asymmetric algorithms possible for each situation.

What algorithm should you select for encrypting an entire hard drive on a laptop?

What asymmetric algorithm should you select for the key exchange during a login to a secure website (using HTTPS)?

What symmetric algorithm should you select for the data exchange during a secure web session?

### Case Study 13-2: Disabling the LM Hash

**Scenario:** Your organization is concerned with the current level of password security. Your task is to make sure that a strong cryptographic hash is used.

If you find that the organization is currently using the LANMAN hash, what should you upgrade to?

In what two ways can you disable the LM Hash?

## Case Study Solutions

### Case Study 13-1 Solution

It's a fact—there are lots of cryptographic algorithms to choose from, but the ones that are the most secure make up a pretty short list. The key here (pun intended) is to select algorithms that will secure data as best possible, while working quickly to do so. The answers below are examples. You might find other answers that better suit your needs, and of course, new algorithms are released periodically.

The most common algorithm used for whole disk encryption (such as BitLocker) is AES. AES 256-bit is preferred. This is a symmetric algorithm that uses a block cipher.

There are three excellent answers for secure key exchange over the Internet; they are all asymmetric. First is RSA 2048-bit. It is commonly used by websites, but it has a massive key length, so elliptic curve technologies are also used: The Diffie-Hellman version ECDH (or ephemeral version ECDHE), and the DSA version (ECDSA). These use less computational power because the elliptic curve method uses a shorter key length.

The best symmetric algorithm for data exchange during a secure web session is AES. However, you might also see RC4 used. In fact, some websites will offer AES connections, until too many users are connected simultaneously; at that point, the additional users will receive RC4-based certificates.

**Video Solution:** Watch the video solution “13-1: Understanding Symmetric and Asymmetric Algorithms” on the accompanying disc.

**Simulation:** Complete the simulation “13-1: Understanding Symmetric and Asymmetric Algorithms” on the accompanying disc.

### Case Study 13-2 Solution

You should upgrade to the NTLMv2 cryptographic hash. Make sure that is running and that the LM hash has been disabled. This can be done by turning it off in the local security policy—OU or domain policy if configuring it for a Microsoft domain—and by disabling it in the Registry.

**Video Solution:** Watch the video solution “13-2: Disabling the LM Hash” on the accompanying disc.

*This page intentionally left blank*



### This chapter covers the following subjects:

- **Public Key Infrastructure:** In this section, we discuss PKI and its components, including private and public keys, certificates, certificate authorities, and the web of trust model.
- **Security Protocols:** Here, we define more security protocols such as S/MIME, SSL, TLS, SSH, and VPN-related protocols such as PPTP, L2TP, and IPsec. And three cheers if you want—these are the last of the TCP/IP security protocols in the book!

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 1.4, 6.2, and 6.3.

# PKI and Encryption Protocols

This short chapter wraps up the rest of the encryption concepts you need to know for the Security+ exam. You are required to understand public key infrastructures and should have the ability to explain what is entailed when a secure connection is made, for example, to a secure e-commerce web server. There is an entire system involved with public key infrastructures, from the users to servers, encryption methods, and much more. It's a big topic that can be confusing due to how many and what variety of keys are used. Take it slow, and reread the section if necessary. Several protocols use public key infrastructures as well, many of which you have probably heard of, such as S/MIME, SSL, SSH, and so on. Keep in mind that the security protocols discussed in this section are intertwined with the concepts of a public key infrastructure.

## Foundation Topics

### Public Key Infrastructure

A **public key infrastructure (PKI)** is an entire system of hardware and software, policies and procedures, and people. It is used to create, distribute, manage, store, and revoke digital certificates. If you have connected to a secure website in the past, you have been a part of a PKI! But a PKI can be used for other things as well, such as secure e-mail transmissions and secure connections to remote computers and remote networks. The PKI is all encompassing: It includes users, client computers, servers, services, and most of all, encryption. Don't confuse PKI with public key encryption. Though they are related, PKI is a way of accomplishing public key encryption, but not all public key encryption schemes are PKI. PKI creates asymmetric key pairs, a public key and a private key: The private key is kept secret, whereas the public key can be distributed. If the key pair is generated at a server, it is considered to be centralized, and the public key is distributed as needed. If the key pair is generated at a local computer, it is considered to be decentralized, and the keys are not distributed; instead, they are used by that local system. An example of public key usage would be a certificate obtained by a web browser during an encrypted session with an e-commerce website. An example of private key usage would be when a user

needs to encrypt the digital signature of a private e-mail. The difference is the level of confidentiality. The public key certificate obtained by the web browser is public and might be obtained by thousands of individuals. The private key used to encrypt the e-mail is not to be shared with anyone.

In a nutshell, public key infrastructures are set up in such a way so as to bind public keys with user identities. This is usually done through the use of certificates distributed by a certificate authority. Less commonly it is done by means of a web of trust.

Let's go ahead and describe these concepts in a little more detail.

## Certificates

**Certificates** are digitally signed electronic documents that bind a public key with a user identity. The identity information might include a person's name and organization, or other details relevant to the user to whom the certificate is to be issued.

Most certificates are based on the **X.509** standard, which is a common PKI standard developed by the ITU-T that often incorporates the single sign-on (SSO) authentication method. This way, a recipient of a single X.509 certificate has access to multiple resources, possibly in multiple locations. Although difficult, X.509 certificates that use MD5 and SHA1 hashes can be compromised. For organizations worried about extremely resourceful hackers, a more powerful hashing algorithm such as SHA2 should be implemented with the certificate. X.509 is the core of the PKIX, which is the IETF's Public Key Infrastructure (X.509) working group. Components of an X.509 certificate include the following:

- Owner (user) information, including their public key
- Certificate authority information, including their name, digital signature, serial number, issue and expiration date, and version

## Certificate Authorities

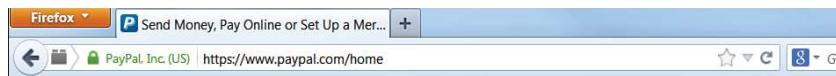
A **certificate authority (CA)** is the entity (usually a server) that issues certificates to users. In a PKI system that uses a CA, the CA is known as a trusted third party. Most PKI systems use a CA. The CA is also responsible for verifying the identity of the recipient of the certificate. An example of a technology that uses certificates would be secure websites. If you opened your browser and connected to a secure site, the browser would first check the certificate that comes from VeriSign or another similar company; it would *validate* the certificate. You (the user) and the website are the two parties attempting to communicate. The CA is a third party that negotiates the security of the connection between you and the website. For a user to obtain a digital identity certificate from a CA, the user's computer must initiate a *certificate signing request* (CSR) and present two items of information: The

first is proof of the user's identity; the second is a public key. This public key is then matched to the CA's private key, and if successful the certificate is granted to the user.

A basic example of this would be if you connect to [www.paypal.com](https://www.paypal.com). When connecting to this website, it automatically redirects you to <https://www.paypal.com>, which is secured by way of a VeriSign-issued certificate. You know you have been redirected to a secure site because the browser has various indicators. For instance, Internet Explorer shows a padlock in the locked position and the address field has a green background. The Firefox browser displays a similar padlock. These examples are shown in Figures 14-1 and 14-2, respectively. The certificate information is shown in the address field, so only the top areas of the browser windows are shown.

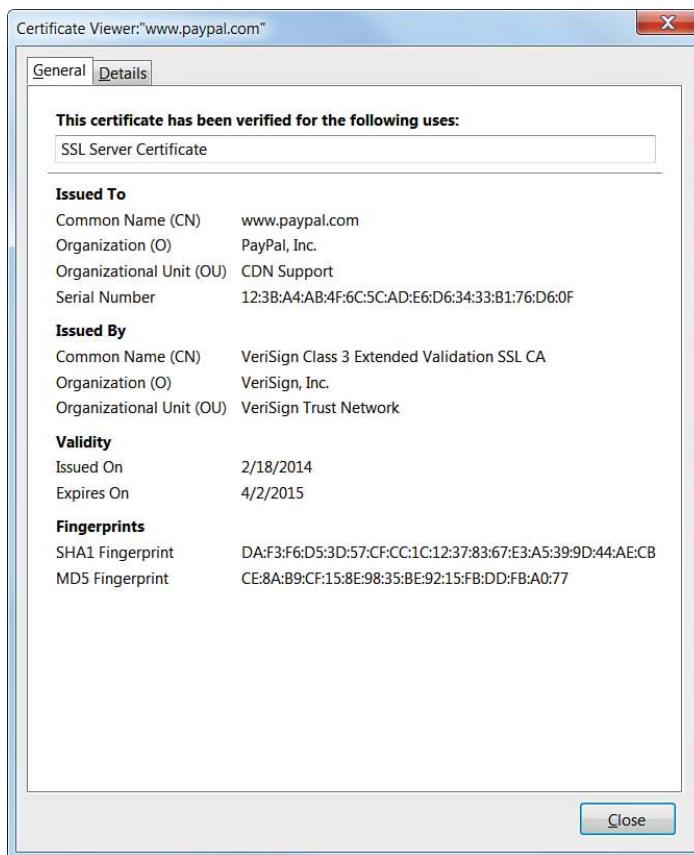


**Figure 14-1** Example of a Secure Connection, Shown in Internet Explorer



**Figure 14-2** Example of a Secure Connection, Shown in Firefox

These are examples of certificates. If you were to click on the green area of the address field in Firefox, it would display a drop-down information window that shows the name of the website and the issuer of the certificate. From there, you could click the More Information button, which tells you additional privacy and historical information, plus technical details. Finally, if you were to click the View Certificate button, the default General tab and the Details tab would show more details of the certificate, as shown in Figure 14-3.



**Figure 14-3** Details of a Typical VeriSign Certificate

The General tab shows that the certificate gets a super-long hexadecimal serial number, and shows when the certificate was originally issued and when it expires, among other information. You can also note that the certificate has been finger-printed with a SHA1 and an MD5 hash, enabling you or the website (or issuer) to verify the integrity of the certificate. If for some reason the certificate cannot be verified by any of the parties, and the issuer confirms this, then the issuer would need to revoke it and place it in the certificate revocation list (CRL).

Recipients can use one or more certificates. Certificate mapping defines how many certificates are associated with a particular recipient. If an individual certificate is mapped to a recipient, it is known as a **one-to-one mapping**. If multiple certificates are mapped to a recipient, it is known as **many-to-one mapping**. Multiple certificates might be used if the recipient requires multiple secure (and separate) communications channels.

In some cases, a **registration authority (RA)** is used to verify requests for certificates. If the request is deemed valid, the RA informs the CA to issue the certificate. An RA might also be used if the organization deals with several CAs. In this case, the RA is at the top of a hierarchical structure and verifies the identity of the user. An RA isn't necessary in a PKI, but if you are centrally storing certificates, a CA is necessary.

Certificate authorities aren't just for the rich and famous (for example, PayPal using VeriSign as the issuer). You can have a CA, too! If you are running a Windows Server, you can install your own CA—for example, one that utilizes L2TP; more on L2TP later in this chapter. Of course, a server's built-in certificates are not necessarily secure. If you were to implement this technology in a secure environment in your organization, you would probably want to obtain proper certificates from a trusted source to use with the Windows Server.

Certificate authorities can be subverted through the use of social engineering. If a person posing as a legitimate company managed to obtain certificates from a trusted source, those certificates would appear to be valid certificates and could cause widespread damage due to connections made by unsuspecting users. That is, until the certificates were revoked. This happens sometimes, but the CA issuer usually finds out quickly and takes steps to mitigate the problem, including revoking the certificate(s) and notifying any involved parties of the incident.

The **certificate revocation list (CRL)** is a list of certificates that are no longer valid or that have been revoked by the issuer. There are two possible states of revocation: revoked, which is when a certificate has been irreversibly revoked and cannot be used again, and hold, which is used to temporarily invalidate a certificate. Reasons for revoking a certificate include the compromising or theft of a certificate or entire CA, unspecified certificates, superseded certificates, held certificates, and key or encryption compromise. The CRL is published periodically, usually every 24 hours. This enables users of an issuer's certificates to find out whether a certificate is valid. CRLs, like the certificates themselves, carry digital signatures to prevent DoS and spoofing attacks; the CRL is digitally signed by the CA.

An alternative to the CRL is the **Online Certificate Status Protocol (OCSP)**. It contains less information than a CRL does, and the client side of the communication is less complex. However, OCSP does not require encryption, making it less secure than CRL.

Certificate keys can also be held in escrow. **Key escrow** is when a secure copy of a user's private key is held in case the key is lost. This may be necessary so that third parties such as government or other organizations can ultimately gain access to communications and data encrypted with that key. If data loss is unacceptable, you should implement key escrow in your PKI.

When installing a certificate authority to a Windows Server, you can set up a recovery agent for lost or corrupted keys. To do this, you need Windows Server and need to set up an Enterprise-level CA. In this configuration, the certificates (or private keys) are archived at the CA. If a **key recovery agent** has been configured, lost, or corrupted, keys can be restored. It's important to use some type of software that can archive and restore keys in case of an incident or disaster.

Another way to avoid single points of failure, such as a single CA, is to organize certificate authorities in a hierarchical manner. At the top of the tree is a root CA; underneath are subordinate CAs that offer redundancy. Though CA exclusivity is common, it is not the only type of architecture used to bind public keys to users. In some cases, a centralized model for certificates is not required or desired.

### **Single-Sided and Dual-Sided Certificates**

Most communication sessions, such as secure web sessions, use single-sided certificates. This is when the server validates itself to recipients of the certificate, such as users who are accessing the website. In these types of scenarios, users do not need to validate their own identity. This would be resource-intensive, especially for a secure web server that might have thousands of concurrent connections.

Sometimes, an organization might choose to have the server *and* the user validate their identities. This would be using a dual-sided certificate; it works well when a limited number of computers and sessions are involved. When more computers are added to the mix, the amount of resources necessary might be a strain on the issuing CA.

### **Web of Trust**

A **web of trust** is a decentralized trust model that addresses issues associated with the public authentication of public keys common to CA-based PKIs. It is considered peer-to-peer in that there is no root CA; instead, self-signed certificates are created and used that have been attested to by the creator. Users can decide what certificates they want to trust and can share those trusted certificates with others, making the web of trust grow larger. Of course, one of the most common reasons that a certificate issuer is not recognized by a web browser is due to unknown self-signed certificates. This model can also interoperate with standard CA architectures inherent to PKI. The more people that show trust of a certificate, the higher the chance that it is legitimate. This model is used by PGP, which enables users to start their own web of trust, self-publishing their own public key information.

## Security Protocols

You can use a variety of security protocols to allow for more secure connections to other systems and networks. But the question is: What should be secured when connecting to other computers? I like to break it down into four categories:

- **E-mail and other communications:** This can be accomplished with the use of S/MIME or PGP.
- **E-commerce and web logins:** This can be brought about with the aid of protocols such as SSL and TLS.
- **Direct connections to other computers:** This can be done with a protocol such as SSH.
- **Virtual connections to remote networks:** This can be achieved with virtual private networks and protocols such as PPTP and L2TP.

Each of these scenarios builds on the concepts we learned in the previous PKI section. Let's define each of these scenarios and the security protocols used in more depth.

### S/MIME

Originally developed by RSA Security, **Secure/Multipurpose Internet Mail Extensions (S/MIME)** is an IETF standard that provides cryptographic security for electronic messaging such as e-mail. It is used for authentication, message integrity, and non-repudiation of origin. Most e-mail clients have S/MIME functionality built-in. S/MIME uses a separate session key for each e-mail message.

S/MIME relies on PKI and the obtaining and validating of certificates from a CA, namely X.509v3 certificates. It also relies on digital signatures when attempting to establish non-repudiation. S/MIME enables users to send both encrypted and digitally signed e-mail messages.

S/MIME can be implemented in Outlook by first obtaining a certificate known as a Digital ID, publishing the certificate within Outlook, and then modifying the settings for Outlook, as shown in Figure 14-4.

One of the issues with S/MIME is that it encrypts not only messages but also any malware that found its way into the message. This could compromise systems between the sender and receiver. To defeat this, scan messages at a network gateway that has a copy of the private keys used with S/MIME. Do this after decryption. If an e-mail program stores an S/MIME encrypted message and the private key used for encryption/decryption is lost, deleted, or corrupted, the message cannot be decrypted.



**Figure 14-4** S/MIME Settings in Outlook

## SSL/TLS

**Secure Sockets Layer (SSL)** and its successor **Transport Layer Security (TLS)** are cryptographic protocols that provide secure Internet communications such as web browsing, instant messaging, e-mail, and VoIP. These protocols rely on a PKI for the obtaining and validating of certificates.

Many people refer to the secure connections they make to websites as SSL, but actually some of these will be TLS. The last version of SSL, version 3, was released in 1996. TLS is a more secure solution; version 1 of TLS supersedes SSLv3. As of the writing of this book, the latest version of TLS is 1.2 (defined in 2008). However, TLS and SSL work in much the same manner. Two types of keys are required when any two computers attempt to communicate with the SSL or TLS protocols: a public key and a session key. Asymmetric encryption is used to encrypt and share session keys, and symmetric encryption is used to encrypt the session data. Session keys used by protocol such as TLS are used only once—a separate session key is utilized for every connection. A recovery key will be necessary if any data is lost in an SSL/TLS session. SSL and TLS encrypt segments of network connections that start at the transport layer of the OSI model. The actual encryption occurs at the session layer. In general, SSL and TLS are known as application layer protocols.

HTTPS, which stands for Hypertext Transfer Protocol Secure, is a combination of HTTP and either SSL or TLS. Web servers that enable HTTPS inbound

connections must have inbound port 443 open. This is common for e-commerce. If you connect to an online shopping portal such as Amazon, your credit card transactions should be protected by HTTPS, and you should see the protocol within the address bar of your browser when you enter a secure area of the website.

HTTPS should not be confused with Secure HTTP (SHTTP). SHTTP is an alternative to HTTPS that works in much the same way. Because SHTTP was neglected by Microsoft, Netscape, and others in the 1990s, and because SHTTP encrypts only application layer messages, HTTPS became the widely used standard. HTTPS can encrypt all data passed between the client and the server, including data passing through layer 3.

SSL can be used by attackers as well. SSL-encrypted malware such as the Zeus or Gameover banking Trojans utilize the secure nature of SSL to exist undetected. Victims are often spammed a false update program that (if opened) downloads the Trojan payload through an SSL-encrypted connection from an infected website. The only way an individual user can protect from this is to have updated anti-malware running, and not open any unknown attachments. However, organizations can use *next-generation firewalls* (NGFWs) to filter out SSL-encrypted traffic. They might use these in addition to their regular firewalls, used for unencrypted traffic.

## SSH

**Secure Shell (SSH)** is a protocol that can create a secure channel between two computers or network devices, enabling one computer or device to remotely control the other. Designed as a replacement for Telnet, it is commonly used on Linux and Unix systems, and nowadays also has widespread use on Windows clients. It depends on public key cryptography to authenticate remote computers. One computer (the one to be controlled) runs the SSH daemon, while the other computer runs the SSH client and makes secure connections to the first computer (which is known as a server), as long as a certificate can be obtained and validated.

Computers that run the SSH daemon have inbound port 22 open. If a proper SSH connection is made, files can also be transferred securely using SFTP (Secure File Transfer Protocol) or SCP (Secure Copy Protocol). Tunneling is also supported.

Vulnerabilities to SSH 1 and 1.5, such as the unauthorized insertion of content, the forwarding of client authentications to other servers (daemons), and integer overflow, precipitated the development of SSH 2.0, which is incompatible with SSH version 1. Improvements to SSH 2.0 include usage of the Diffie-Hellman key exchange and integrity checking with message authentication codes (MACs).

## PPTP, L2TP, and IPsec

Virtual private networks (VPN) were developed to enable quick, secure, remote connections using the inherent capacity of the Internet. They were also developed to take advantage of faster Internet connections such as cable, DSL, and so on but still work with dial-up connections. The issue with VPNs is how to secure those connections. Basically, there are two common protocols used to do so: PPTP and L2TP (with the aid of IPsec).

### PPTP

The **Point-to-Point Tunneling Protocol (PPTP)** is a protocol used in VPNs. It encapsulates PPP packets, ultimately sending encrypted traffic. PPP by itself is useful for dial-up connections but is not suitable for a VPN by itself without a protocol such as PPTP. Servers and other devices running the PPTP protocol and accepting incoming VPN connections need to have inbound port 1723 open.

Because the authentication protocol MSCHAPv1 is considered inherently insecure, and MSCHAP-v2 is vulnerable to dictionary attacks, PPTP is deemed to be vulnerable. These authentication vulnerabilities can be dismissed if PPTP is used with an authentication method such as EAP-TLS. This relies on the existence of a PKI for the client and server computers. If this infrastructure is not readily available, PEAP can be used instead, as long as the computers are running the Windows Vista operating system or newer. Otherwise, L2TP with IPsec or other tunneling protocols is recommended for environments in which session and data security is of paramount importance.

### L2TP

The **Layer 2 Tunneling Protocol (L2TP)** is a tunneling protocol used to connect VPNs. In essence, it creates an unencrypted tunnel if used by itself (which would be unwise). It does not include confidentiality or encryption on its own, but when paired with a security protocol such as IPsec it is considered a formidable tunneling protocol.

Its starting point is based on the Layer 2 Forwarding Protocol (L2F) and PPTP. The latest version is L2TPv3, which has improved encapsulation and increased security features. Servers and other devices accepting incoming VPN connections need to have inbound port 1701 open.

When installed on a Windows Server, it uses a PKI. Valid certificates need to be downloaded to clients before they can make a VPN connection to the server. Security must be configured on the server side and the client side. Generally, the IPsec protocol is used to accomplish the secure connection within the L2TP tunnel.

## IPsec

**Internet Protocol Security (IPsec)** authenticates and encrypts IP packets, effectively securing communications between the computers and devices that use this protocol. IPsec operates at the network layer of the OSI model. It differs from SSH, SSL, and TLS in that it is the only protocol that does not operate within the upper layers of the OSI model. It can negotiate cryptographic keys and establish mutual authentication. IPsec is made up of three other protocols that perform its functions, including

**Key Topic**

- **Security association (SA):** This is the establishment of secure connections and shared security information, using either certificates or cryptographic keys. It is set up most often through the Internet Key Exchange (IKE) or via Kerberized Internet Negotiation of Keys. The IKE can select varying levels of security protocols for the computers in a connection, which can differ in a VPN due to the dissimilar computers (with disparate protocols) that might attempt to connect to it.
- **Authentication header (AH):** This offers integrity and authentication. The authentication information is a keyed hash based on all the bytes in the packet. It can be used with the Encapsulating Security Payload (ESP) protocol. It can protect against replay attacks by employing sliding window protocols, which put limits on the total amount of packets that can be transceived in a given timeframe but ultimately enables an unlimited number of packets to be communicated using fixed-size sequence numbers.
- **Encapsulating Security Payload (ESP):** This provides integrity, confidentiality, and authenticity of packets. Protected data is encapsulated and encrypted.

IPsec uses algorithms such as SHA1 for integrity and authenticity, which hashes the packets of data; afterward the hash is encrypted. It also uses Triple DES and AES for confidentiality.

## Chapter Summary

Because public keys are common knowledge, they must be protected from compromise. One way to do this is to implement a public key infrastructure (PKI). This is a complete environment for the public key, including hardware, software, and procedures.

Users who want to access a website securely are required to request a certificate; this will bind the user identity with the public key. The certificate is issued from a certificate authority (CA) such as VeriSign. To be validated, a user's computer initiates

a certificate signing request (CSR) with proof of the user's identity. If a certificate used by a website is no longer valid, or is suspected to be compromised, it needs to be revoked right away and placed on a public certificate revocation list (CRL).

PKI is used during secure web sessions (HTTPS, for example) that use SSL or TLS protocols, e-mail sessions that use S/MIME, and secure sessions between computers with SSH. Virtual private networks can also use a PKI; for example, a VPN that relies on L2TP and therefore certificates as well. To further secure an L2TP tunneled connection, IPsec is implemented.

However, PKI is most commonly used for secure web transactions. Within that system, a certificate will employ asymmetric encryption (such as RSA or ECC) and a cryptographic hash (such as SHA) for the key exchange. Afterward, the rest of the session's data will be encrypted in a symmetric format (such as AES or RC4), which uses less computational power than asymmetric encryption.

As you travel the Internet, check on the validity (and level of security) of the certificates used by websites. Any site that you can log into, or conduct any type of transaction regarding anything of value, should have an HTTPS connection, as well as SSL or TLS, RSA or ECC, SHA or MD5, and AES or RC4 cryptographic protocols.

## 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 14-1 lists a reference of these key topics and the page number on which each is found.

**Table 14-1** Key Topics for Chapter 14

| Key Topic Element | Description                                                | Page Number |
|-------------------|------------------------------------------------------------|-------------|
| Figure 14-1       | Example of a secure connection, shown in Internet Explorer | 553         |
| Figure 14-2       | Example of a secure connection, shown in Firefox           | 553         |
| Figure 14-3       | Details of a typical VeriSign certificate                  | 554         |
| Bulleted list     | IPsec protocols                                            | 561         |

## Define Key Terms

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

public key infrastructure (PKI), certificates, X.509, certificate authority (CA), one-to-one mapping, many-to-one mapping, registration authority (RA), certificate revocation list (CRL), Online Certificate Status Protocol (OCSP), key escrow, key recovery agent, web of trust, Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Protocol Security (IPsec)

## Review Questions

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

1. Which of the following does not apply to an X.509 certificate?
  - A. Certificate version
  - B. The issuer of the certificate
  - C. Public key information
  - D. Owner's symmetric key
2. What two items are included in a digital certificate? (Select the two best answers.)
  - A. User's private key
  - B. Certificate authority's digital signature
  - C. The user's public key
  - D. Certificate authority's IP address
3. Rick has a local computer that uses software to generate and store key pairs. What type of PKI implementation is this?
  - A. Distributed key
  - B. Centralized
  - C. Hub and spoke
  - D. Decentralized

4. Which of the following is usually used with L2TP?
  - A. IPsec
  - B. SSH
  - C. PHP
  - D. SHA
5. What ensures that a CRL is authentic and has not been modified?
  - A. The CRL can be accessed by anyone.
  - B. The CRL is digitally signed by the CA.
  - C. The CRL is always authentic.
  - D. The CRL is encrypted by the CA.
6. Which of the following encryption concepts is PKI based on?
  - A. Asymmetric
  - B. Symmetric
  - C. Elliptical curve
  - D. Quantum
7. You are in charge of PKI certificates. What should you implement so that stolen certificates cannot be used?
  - A. CRL
  - B. CAD
  - C. CA
  - D. CRT
8. Which of the following are certificate-based authentication mapping schemes? (Select the two best answers.)
  - A. One to-many mapping
  - B. One-to-one mapping
  - C. Many-to-many mapping
  - D. Many-to-one mapping
9. Which of the following network protocols sends data between two computers while using a secure channel?
  - A. SSH
  - B. SMTP

- C. SNMP
  - D. P2P
10. Which of the following protocols uses port 443?
- A. SFTP
  - B. HTTPS
  - C. SSHTP
  - D. SSLP
11. Which of the following protocols creates an unencrypted tunnel?
- A. L2TP
  - B. PPTP
  - C. IPsec
  - D. VPN
12. In a public key infrastructure setup, which of the following should be used to encrypt the signature of an e-mail?
- A. Private key
  - B. Public key
  - C. Shared key
  - D. Hash
13. Two computers are attempting to communicate with the SSL protocol. Which two types of keys will be used? (Select the two best answers.)
- A. Recovery key
  - B. Session key
  - C. Public key
  - D. Key card
14. Which layer of the OSI model does IPsec operate at?
- A. Data Link
  - B. Network
  - C. Transport
  - D. Application

- 15.** Which layer of the OSI model is where SSL provides encryption?
  - A.** Network
  - B.** Transport
  - C.** Session
  - D.** Application
  
- 16.** Which of the following details one of the primary benefits of using S/MIME?
  - A.** S/MIME expedites the delivery of e-mail messages.
  - B.** S/MIME enables users to send e-mail messages with a return receipt.
  - C.** S/MIME enables users to send both encrypted and digitally signed e-mail messages.
  - D.** S/MIME enables users to send anonymous e-mail messages.
  
- 17.** What should you do to make sure that a compromised PKI key cannot be used again?
  - A.** Renew the key.
  - B.** Reconfigure the key.
  - C.** Revoke the key.
  - D.** Create a new key.
  
- 18.** Which of the following statements is correct about IPsec authentication headers?
  - A.** The authentication information is a keyed hash based on half of the bytes in the packet.
  - B.** The authentication information is a keyed hash based on all the bytes in the packet.
  - C.** The authentication information hash will remain the same even if the bytes change on transfer.
  - D.** The authentication header cannot be used in combination with the IP Encapsulating Security Payload.
  
- 19.** Which of the following protocols is not used to create a VPN tunnel and not used to encrypt VPN tunnels?
  - A.** PPTP
  - B.** L2TP
  - C.** PPP
  - D.** IPsec

- 20.** Which of the following answers are not part of IPsec? (Select the two best answers.)
- A.** TKIP
  - B.** Key exchange
  - C.** AES
  - D.** Authentication header
- 21.** What should you publish a compromised certificate to?
- A.** CRL
  - B.** CA
  - C.** PKI
  - D.** AES
- 22.** You have been asked to set up authentication through PKI, and encryption of a database using a different cryptographic process to decrease latency. What encryption types should you use?
- A.** Public key encryption to authenticate users and public keys to encrypt the database
  - B.** Public key encryption to authenticate users and private keys to encrypt the database
  - C.** Private key encryption to authenticate users and private keys to encrypt the database
  - D.** Private key encryption to authenticate users and public keys to encrypt the database
- 23.** Which of the following uses an asymmetric key to open a session, and then establishes a symmetric key for the remainder of the session?
- A.** TLS
  - B.** SFTP
  - C.** HTTPS
  - D.** SSL
  - E.** TFTP

- 24.** Which of the following describes key escrow?
- A.** Maintains a secured copy of the user's private key for the purpose of recovering the CRL
  - B.** Maintains a secured copy of the user's private key for the purpose of recovering the key if it is lost
  - C.** Maintains a secured copy of the user's public key for the purpose of recovering messages if the key is lost
  - D.** Maintains a secured copy of the user's public key for the purpose of increasing network performance
- 25.** When a user's web browser communicates with a CA, what PKI element does the CA require from the browser?
- A.** Public key
  - B.** Private key
  - C.** Symmetric key
  - D.** Secret key

## Answers and Explanations

- 1.** **D.** In X.509, the owner does not use a symmetric key. All the other answers apply to X.509.
- 2.** **B.** and **C.** A digital certificate includes the certificate authority's (CA) digital signature and the user's public key. A user's private key should be kept private and should not be within the digital certificate. The IP address of the CA should have been known to the user's computer before obtaining the certificate.
- 3.** **D.** When creating key pairs, PKI has two methods: centralized and decentralized. Centralized is when keys are generated at a central server and are transmitted to hosts. Decentralized is when keys are generated and stored on a local computer system for use by that system.
- 4.** **A.** IPsec is usually used with L2TP. SSH is a more secure way of connecting to remote computers. PHP is a type of language commonly used on the web. SHA is a type of hashing algorithm.
- 5.** **B.** Certificate revocation lists (CRLs) are digitally signed by the certificate authority for security purposes. If a certificate is compromised, it will be revoked and placed on the CRL. CRLs are later generated and published periodically.

6. **A.** The public key infrastructure, or PKI, is based on the asymmetric encryption concept. Symmetric, elliptical curve, and quantum cryptography are all different encryption schemes that PKI is not associated with.
7. **A.** You should implement a CRL (certificate revocation list) so that stolen certificates, or otherwise revoked or held certificates, cannot be used.
8. **B.** and **D.** When dealing with certificate authentication, asymmetric systems use one-to-one mappings and many-to-one mappings.
9. **A.** SSH, or Secure Shell, enables two computers to send data via a secure channel. SMTP is the Simple Mail Transfer Protocol, which deals with e-mail. SNMP is the Simple Network Management Protocol, which enables the monitoring of remote systems. P2P is an abbreviation of peer-to-peer network.
10. **B.** Port 443 is used by HTTPS, which implements TLS/SSL for security. SFTP is the Secure File Transfer Protocol. There are no protocols named SSHTP and SSLP.
11. **A.** In VPNs (virtual private networks), Layer Two Tunneling Protocol (L2TP) creates an unencrypted tunnel between two IP addresses. It is usually used with IPsec to encrypt the data transfer. PPTP is the Point-to-Point Tunneling Protocol, which includes encryption.
12. **A.** A private key should be used to encrypt the signature of an e-mail in an asymmetric system such as PKI. Public keys and shared keys should never be used to encrypt this type of information. A hash is not used to encrypt in this fashion; it is used to verify the integrity of the message.
13. **B.** and **C.** In an SSL session, a session key and a public key are used. A recovery key is not necessary unless data has been lost. A key card would be used as a physical device to gain access to a building or server room.
14. **B.** IPsec is a dual-mode, end-to-end security scheme that operates at layer 3, the network layer of the OSI model, also known as the internet layer within the Internet Protocol suite. It is often used with L2TP for VPN tunneling, among other protocols.
15. **C.** SSL, or Secure Sockets Layer, and its successor Transport Layer Security (TLS) encrypt segments of network connections that start at the transport layer. The actual encryption is done at the session layer, and the protocol is known as an application layer protocol.
16. **C.** S/MIME (Secure/Multipurpose Internet Mail Extensions) enables users to send both encrypted and digitally signed e-mail messages, enabling a higher level of e-mail security. It does not make the delivery of e-mail any faster, nor

does it have anything to do with return receipts. Return receipts are usually controlled by the SMTP server. Anonymous e-mail messages would be considered spam, completely insecure, and something that a security administrator wants to reduce, and certainly does not want users to implement.

17. **C.** Key revocation is the proper way to approach the problem of a compromised PKI key. The revoked key will then be listed in the CRL (certificate revocation list).
18. **B.** The only statement that is true is that the authentication information is a keyed hash that is based on all the bytes in the packet. A hash will not remain the same if the bytes change on transfer; a new hash will be created for the authentication header (AH). The authentication header can be used in combination with the Encapsulating Security Payload (ESP).
19. **C.** PPP, or Point-to-Point Protocol, does not provide security and is not used to create VPN connections. You will see PPP used in dial-up connections, and it is an underlying protocol used by L2TP, PPTP, and IPsec, which are all used in VPN connections.
20. **A. and C.** IPsec contains (or uses) a key exchange (either Internet Key Exchange or Kerberized Internet Negotiation of Keys) and an authentication header (in addition to many other components). TKIP and AES are other encryption protocols.
21. **A.** A compromised certificate should be published to the CRL (certificate revocation list). The CA is the certificate authority that houses the CRL. PKI stands for public key infrastructure—the entire system that CRLs and CAs are just components of. AES is an encryption protocol.
22. **B.** PKI uses public keys to authenticate users. If you are looking for a cryptographic process that allows for decreased latency, then symmetrical keys (private) would be the way to go. So the PKI system uses public keys to authenticate the users, and the database uses private keys to encrypt the data.
23. **C.** HTTPS will govern the entire session when a person attempts to connect to a website securely (for example, [HTTPS://www.yourbanknamehere.com](https://www.yourbanknamehere.com)). It initiates a key exchange using SSL or TLS, riding on asymmetric encryption such as RSA or ECC. Then, it performs the rest of the session data transfer using symmetric encryption such as AES. SFTP is Secure FTP, based on SSH. TFTP is Trivial FTP, which has little security.
24. **B.** Key escrow is implemented to secure a copy of the user's private key (not the public key) in case it is lost. It has nothing to do with the CRL.
25. **A.** The browser must present the public key, which is matched against the CA's private key. Symmetric and secret keys are other names for private keys.

## Case Studies for Chapter 14

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book's disc.

### Case Study 14-1: Understanding PKI

**Scenario:** Your boss wants you to set up a new website for customers that will allow for a secure login directly on the home page. Your task is to locate two vendors of SSL certificates that have up to 256-bit AES encryption and also offer RSA encryption for key exchange.

Identify two SSL certificate vendors and describe their services.

Define what an SLA is.

Explain what happens if more than a certain level of users connect simultaneously.

### Case Study 14-2: Making an SSH Connection

**Scenario:** A company you consult for wants to make secure connections to two Linux systems so that they can be remotely controlled in the command-line. The company does not want to use the deprecated Telnet utility. You decide to recommend the SSH protocol because of its known security advantages over Telnet.

What is SSH?

What port does it use, and which computers should have that port open?

What kind of secure algorithm does it support?

What program(s) can you use to remotely control the Linux systems from the command-line?

## Case Study Solutions

### Case Study 14-1 Solution

There are plenty of Secure Sockets Layer (SSL) certificate providers. Examples include VeriSign, Comodo, GoDaddy, DigiCert, and Thwate. The more trusted providers (such as VeriSign) use that trust to increase the price of their products.

A typical SSL certificate from VeriSign will offer RSA 2048-bit asymmetric key exchange with SHA1 hashing, as well as variable symmetric session encryption. As of the writing of this book, it would be common to have 256-bit AES for a certain number of users, and any users that connect beyond that would get 128-bit AES or RC4 connections.

An SLA is a service-level agreement, which is effectively a contract defining the terms of service. We'll discuss this more later in the book.

It's important to note that this technology changes quickly. Encryption methods are often considered uncrackable—that is until they are cracked, and then there is a complete paradigm shift in the technology once again. It's unavoidable. For example, in 2009, a lot of websites used Triple DES (168-bit) for the session data. AES was still gaining traction, but now (as of the writing of this book), just five years later, AES is the standard, and Triple DES is all but extinct. Chances are, the algorithm of choice will be completely different every five years or so. Make sure you don't sign SLAs that have a span of more than two years. Keep the contracts short, review your technology (and the PKI used) often, and reconsider your options as time goes on.

**Video Solution:** Watch the video solution “14-1: Understanding PKI” on the accompanying disc.

### Case Study 14-2 Solution

SSH stands for Secure Shell, and is a cryptographic protocol used to secure communications and command-line-based remote login. It uses port 22 by default. The computer that will be logged in to needs to have SSH installed and inbound port 22 open. SSH2 (as of the writing of this book) is the more secure version of SSH. It supports public key authentication using certificates (X.509), RSA, and DSA. File transfer can be secured by using SFTP. The copying of files can also be secured using SCP. By default these use TCP as the transport mechanism, but can also use STCP. For these file transfers it supports the 3DES, AES, and Blowfish symmetric algorithms.

The most commonly used program to remotely control Linux systems in the command-line is the PuTTy program. It is an open source terminal emulator that allows control over the remote computer, and network file transfer. It has support for a wide variety of operating systems. Other SSH clients include Open SSH, Dropbear, and Tera Term, though their support for operating systems will vary.

**Video Solution:** Watch the video solution “14-2: Making an SSH Connection” on the accompanying disc.



### This chapter covers the following subjects:

- **Redundancy Planning:** This section is all about ensuring your network and servers are fault tolerant. By setting up redundant power, data, servers, and even ISPs, you can avoid many disasters that could threaten the security of your organization.
- **Disaster Recovery Planning and Procedures:** A disaster is when something happens to your network that your fault-tolerant methods cannot prevent. To help recover after a disaster, data should be backed up, and a proper disaster recovery plan should be designed, practiced, and implemented if necessary.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 1.1 and 2.8.

# Redundancy and Disaster Recovery

The typical definition of “redundant” means superfluous or uncalled for. However, it is not so in the IT field. Being redundant is a way of life. It is a way of enhancing your servers, network devices, and other equipment. It is a way of developing fault tolerance—the capability to continue functioning even if there is an error.

This chapter discusses how to prevent problems that might occur that could threaten the security of your servers, network equipment, and server room in general. A good network security administrator should have plenty of redundancy and fault-tolerant methods in place that can help combat threats and help avoid disaster.

However, no matter how much redundancy you implement, there is always a chance that a tragedy could arise—a disaster. A disaster could be the loss of data on a server, a fire in a server room, or the catastrophic loss of access to an organization’s building. To prepare for these events, a disaster recovery plan should be designed, but with the thought in mind that redundancy and fault tolerance can defend against most “disasters.” The best admin is the one that avoids disaster and, in the rare case that it does happen, has a plan in place to recover quickly from it. This chapter also covers how to plan for disasters and discusses a plan of action for recovering swiftly.

## Foundation Topics

### Redundancy Planning

Most networks could do with a little more redundancy. I know...a lot of you are probably wondering why I keep repeating myself! It’s because so many customers of mine in the past, and network admins that have worked for and with me, insist on avoiding the issue. Redundancy works—use it!

This section discusses redundant power in the form of power supplies, UPSs, and backup generators. It also talks about redundant data, servers, ISPs, and sites. All these things, when planned properly, create an environment that can withstand most failures barring total disaster.

The whole concept revolves around single points of failure. A **single point of failure** is an element, object, or part of a system that, if it fails, causes the whole system to fail. By implementing redundancy, you can bypass just about any single point of failure.

There are two methods to combating single points of failure. The first is to use redundancy. If employed properly, redundancy keeps a system running with no downtime. However, this can be pricey, and we all know there is only so much IT budget to go around. So, the alternative is to make sure you have plenty of spare parts lying around. This is a good method if your network and systems are not time-critical. Installing spare parts often requires you to shut down the server or a portion of a network. If this risk is not acceptable to an organization, you'll have to find the cheapest redundant solutions available. Research is key, and don't be fooled by the hype—sometimes the simplest sounding solutions are the best.

Here's the scenario (and we apply this to the rest of this "Redundancy Planning" section). Your server room has the following powered equipment:

- Nine servers
- Two Microsoft domain controllers
- One DNS server
- Two file servers
- One database server
- Two web servers (which second as FTP servers)
- One mail server
- Five 48-port switches
- One master switch
- Three routers
- Two CSU/DSUs
- One PBX
- Two client workstations (for remote server access without having to work directly at the server); these are within the server room as well.

It appears that there is already some redundancy in place in your server room. For example, there are two domain controllers. One of them has a copy of the Active Directory and acts as a secondary DC in the case that the first one fails. There are also two web servers, one ready to take over for the other if the primary one fails. This type of redundancy is known as failover redundancy. The secondary system is

inactive until the first one fails. Also, there are two client workstations used to remotely control the servers; if one fails, another one is available.

Otherwise, the rest of the servers and other pieces of equipment are one-offs—single instances in need of something to prevent failure. There are a lot of them, so we truly need to *redundacize*. Hey, it's a word if IT people use it! It's the detailed approach to preparing for problems that can arise in a system that will make for a good IT contingency plan. Try to envision the various upcoming redundancy methods used with each of the items listed previously in our fictitious server room.

But before we get into some hard-core redundancy, let's quickly discuss the terms fail-open and fail-closed. *Fail-open* means that if a portion of a system fails, the rest of the system will still be available or “open.” *Fail-closed* means that if a portion of a system fails, the entire system will become inaccessible or simply shut down.

Depending on the level of security your organization requires, you might have a mixture of fail-open and fail-closed systems. In the previous server room example, we have a DNS server and a database server. Let's say that the DNS server forwards information to several different zones, and that one of those zones fails for one reason or another. We might decide that it is more beneficial to the network to have the rest of the DNS server continue to operate and service the rest of the zones instead of shutting down completely, so we would want the DNS server to fail-open. However, our database server might have confidential information that we cannot afford to lose, so if one service or component of the database server fails, we might opt to have the database server stop servicing requests altogether, or in other words, to fail-closed. Another example would be a firewall/router. If the firewall portion of the device failed, we would probably want the device to fail-closed. Even though the network connectivity could still function, we probably wouldn't want it to since there is no firewall protection. It all depends on the level of security you require, and the risk that can be associated with devices that fail-open. It also depends on whether the server or device has a redundancy associated with it. If the DNS server mentioned previously has a secondary redundant DNS server that is always up and running and ready to take requests at a moment's notice, we might opt to instead configure the first DNS server to fail-closed and let the secondary DNS server take over entirely. This leads to clustering, which we discuss later in this chapter.

## Redundant Power

Let's begin with power because that is what all our devices and computers gain “sustenance” from. Power is so important—when planning for redundancy it should be at the top of your list. When considering power implications, think like an engineer; you might even need to enlist the help of a coworker who has an engineering background, or a third party, to help plan your electrical requirements and make them a reality.

We are most interested in the server room. Smart companies store most of their important data, settings, apps, and so on in that room. So power is critical here, whereas it is not as important for client computers and other client resources. If power fails in a server room or in any one component within the server room, it could cause the network to go down, or loss of access to resources. It could also cause damage to a server or other device.

When considering power, think about it from the inside out. For example, start with individual computers, servers, and networking components. How much power does each of these things require? Make a list and tally your results. Later, this plays into the total power needed by the server room. Remember that networking devices such as IP phones, cameras, and some wireless access points are powered over Ethernet cabling, which can require additional power requirements at the Ethernet switch (or switches) in the server room. Think about installing redundant power supplies in some of your servers and switches. Next, ponder using UPS devices as a way of defeating short-term power loss failures. Then, move on to how many circuits you need, total power, electrical panel requirements, and also the cleanliness of power coming in from your municipality. Finally, consider backup generators for longer term power failures.

Using proper power devices is part of a good preventative maintenance/security plan and helps to protect a computer. You need to protect against several things:

**Key Topic**

- **Surges:** A **surge** in electrical power means that there is an unexpected increase in the amount of voltage provided. This can be a small increase, or a larger increase known as a spike.
- **Spikes:** A **spike** is a short transient in voltage that can be due to a short circuit, tripped circuit breaker, power outage, or lightning strike.
- **Sags:** A **sag** is an unexpected decrease in the amount of voltage provided. Typically, sags are limited in time and in the decrease in voltage. However, when voltage reduces further, a brownout could ensue.
- **Brownouts:** A **brownout** is when the voltage drops to such an extent that it typically causes the lights to dim and causes computers to shut off.
- **Blackouts:** A **blackout** is when total loss of power for a prolonged period occurs. Another problem associated with blackouts is the spike that can occur when power is restored. In the New York area, it is common to have an increased amount of tech support calls during July; this is attributed to lightning storms! Often, damage to systems is due to improper protection.
- **Power supply failure:** Power supplies are like hard drives in two ways: One, they will fail: It's not a matter of if; it's a matter of when. Two, they can cause intermittent issues when they begin to fail, issues that are hard to trouble-

shoot. If you suspect a power supply failure, then you should replace the supply. Also consider using a redundant power supply.

Some devices have specific purposes, and others can protect against more than one of these electrical issues. Let's talk about three of them now: redundant power supplies, uninterruptible power supplies, and backup generators.

## Redundant Power Supplies

A proper **redundant power supply** is an enclosure that contains two (or more) complete power supplies. You make one main power connection from the AC outlet to the power supply, and there is one set of wires that connects to the motherboard and devices. However, if one of the power supplies in the enclosure fails, the other takes over immediately without computer failure. These are common on servers, especially RAID boxes. They are not practical for client computers, but you might see them installed in some powerful workstations. In our scenario, we should install redundant power supplies to as many servers as possible, starting with the file servers and domain controllers. If possible, we should implement redundant power supplies for any of our switches or routers that will accept them, or consider new routers and switches that are scalable for redundant power supplies.

In some cases (pun intended), it is possible to install two completely separate power supplies so that each has a connection to an AC outlet. This depends on your server configuration but is less common due to the amount of redundancy it requires of the devices inside the server. Either look at the specifications for your server's case or open it up during off-hours to see if redundant power supplies are an option.

Vendors such as HP and manufacturers such as Thermaltake and Enlight offer redundant power supply systems for servers, and vendors such as Cisco offer redundant AC power systems for its networking devices.

This technology is great in the case that a power supply failure occurs, but it does not protect from scenarios in which power to the computer is disrupted.

## Uninterruptible Power Supplies

It should go without saying, but surge protectors are not good enough to protect power issues that might occur in your server room. A UPS is the proper device to use. An **uninterruptible power supply (UPS)** takes the functionality of a surge suppressor and combines that with a battery backup. So now, our server is protected not only from surges and spikes, but also from sags, brownouts, and blackouts. Most UPS devices also act as line conditioners that serve to clean up dirty power. Noise and increases/decreases in power make up dirty power. Dirty power can also be

caused by too many devices using the same circuit, or because power coming from the electrical panel or from the municipal grid fluctuates, maybe because the panel or the entire grid is under/overloaded. If a line conditioning device such as a UPS doesn't fix the problem, a quick call to your company's electrician should result in an answer and possibly a long-term fix.

If you happen to be using a separate line conditioning device *in addition to* a UPS, it should be tested regularly. Line conditioning devices are always supplying power to your devices. A UPS backup battery will kick in only if a power loss occurs.

Battery backup is great, but the battery can't last indefinitely! It is considered emergency power and typically keeps your computer system running for 5 to 30 minutes depending on the model you purchase. UPS devices today have a USB connection so that your computer can communicate with the UPS. When there is a power outage, the UPS sends a signal to the computer telling it to shut down, suspend, or stand-by before the battery discharges completely. Most UPSs come with software that you can install that enables you to configure the computer with these options.

The more devices that connect to the UPS, the less time the battery can last if a power outage occurs; if too many devices are connected, there may be inconsistencies when the battery needs to take over. Thus many UPS manufacturers limit the amount of battery backup-protected receptacles. Connecting a laser printer to the UPS is *not* recommended due to the high current draw of the laser printer; and *never* connect a surge protector or power strip to one of the receptacles in the UPS, to protect the UPS from being overloaded.

The UPS normally has a lead-acid battery that, when discharged, requires 10 hours to 20 hours to recharge. This battery is usually shipped in a disconnected state. Before charging the device for use, you must first make sure that the leads connect. If the battery ever needs to be replaced, a red light usually appears accompanied by a beeping sound. Beeping can also occur if power is no longer supplied to the UPS by the AC outlet.

There are varying levels of UPS devices, which incorporate different technologies. For example, the cheaper standby UPS (known as an SPS) might have a slight delay when switching from AC to battery power, possibly causing errors in the computer operating system. If a UPS is rack mounted, it will usually be a full-blown UPS (perhaps not the best choice of words!); this would be known as an "online" or "continuous" UPS—these cost hundreds or even thousands of dollars. If it is a smaller device that plugs into the AC outlet and lies freely about, it is probably an SPS—these cost between \$25 and \$100. You should realize that some care should be taken when planning the type of UPS to be used. When data is crucial, you had better plan for a quality UPS!

Just about everything in the server room should be connected to a UPS (you will most likely need several) to protect from power outages. This includes servers,

monitors, switches, routers, CSU/DSUs, PBX equipment, security cameras, workstations, and monitors—really, everything in the server room!

## Backup Generators

What if power to the building does fail completely? Most would consider this a disaster, and over the long term it could possibly be. However, most power outages are 5 minutes or less on the average, and most of the time a UPS can pick up the slack for these short outages but not for the less common, longer outages that might last a few hours or days. And, a UPS powers only the devices you plug into it. If your organization is to keep functioning, it will need a backup generator to power lights, computers, phones, and security systems over short-term outages, or longer ones.

A **backup generator** is a part of an emergency power system used when there is an outage of regular electric grid power. Some emergency power systems might include special lighting and fuel cells, whereas larger, more commercial backup generators can power portions of a building, or an entire building, as long as fuel is available. For our scenario we should make sure that the backup generator powers the server room at the very least.

Backup generator fuel types include gasoline, diesel, natural gas, propane, and solar. Smaller backup generators often use gasoline, but these are not adequate for most companies. Instead, many organizations use larger natural gas generators. Some of these generators need to be started manually, but the majority of them are known as **standby generators**. These are systems that turn on automatically within seconds of a power outage. Transfer switches sense any power loss and instruct the generator to start. Standby generators may be required by code for certain types of buildings with standby lighting, or buildings with elevators, fire-suppression systems, and life-support equipment. You should always check company policy and your municipal guidelines before planning and implementing a backup generator system.

Backup generators can be broken into three types:

- **Portable gas-engine generator:** The least expensive and run on gasoline or possibly solar power. They are noisy, high maintenance, must be started manually, and usually require extension cords. They are a carbon monoxide risk and are only adequate for small operations and in mobile scenarios.  
Gas-powered inverters are quieter but often come with a higher price tag per watt generated.
- **Permanently installed generator:** Much more expensive, with a complex installation. These almost always run on either natural gas or propane. They are quieter and can be connected directly to the organization's electrical panel. Usually, these are standby generators and, as such, require little user interaction.

- **Battery-inverter generator:** These are based on lead-acid batteries, are quiet, and require little user interaction aside from an uncommon restart and change of batteries. They are well matched to environments that require a low amount of wattage or are the victims of short power outages only. Battery-inverter systems can be stored indoors, but because the batteries can release fumes, the area they are stored in should be well ventilated, such as an air conditioned server room with external exhaust. Uninterruptible power supplies fall into the battery-inverter generator category.

Some of the considerations you should take into account when selecting a backup generator include the following:

- **Price:** As with any organizational purchase, this will have to be budgeted.
- **How unit is started:** Does it start automatically? Most organizations require this.
- **Uptime:** How many hours will the generator stay on before needing to be re-fueled? This goes hand-in-hand with the next bullet.
- **Power output:** How many watts does the system offer? Before purchasing a backup generator, you should measure the total maximum load your organization might use by running all computers, servers, lights, and other devices simultaneously, and measure this at the main electrical panel. Alternatively, you could measure the total on paper by adding the estimated power requirements of all devices together.
- **Fuel source:** Does it run on natural gas, gasoline, and so on? If it is an automatically starting system, the options will probably be limited to natural gas and propane.

Some vendors that offer backup generators include Generac, Gillette, and Kohler. These devices should be monitored periodically; most companies attempt to obtain a service contract from you, which might be wise depending on the size of your organization. We discuss service contracts and service-level agreements in Chapter 16, “Policies, Procedures, and People.”

Remember that your mission-critical devices, such as servers, should constantly be drawing power from a line conditioning device. Then, if there is a power outage to the server, a UPS should kick in. (In some cases, the UPS also acts as the line conditioning device.) Finally, if necessary, a backup generator will come online and feed all your critical devices with power.

## Redundant Data

Now that we have power taken care of, we can move on to the heart of the matter—data. Data can fail due to file corruption and malicious intent, among other

things. Power failures, hard drive failures, and user error can all lead to data failure. As always, it's the data that we are most interested in securing, so it stands to reason that the data should be redundant as well. But which data? There is so much of it! Well, generally file servers should have redundant data sets of some sort. If an organization has the budgeting, next on the list would be databases and then web and file servers. However, in some instances these additional servers might be better off with failover systems as opposed to redundant data arrays. And certainly, the majority of client computers' data does not constitute a reason for RAID. So we concentrate on the file servers in our original scenario in the beginning of the chapter.

The best way to protect file servers' data is to use some type of redundant array of disks. This is referred to as RAID (an acronym for redundant array of independent disks, or inexpensive disks). RAID technologies are designed to either increase the speed of reading and writing data or to create one of several types of fault-tolerant volumes, or to do both. From a security viewpoint, we are most interested in the availability of data, the fault tolerance (the capability to withstand failure) of our disks. A RAID array can be internal or external to a computer. Historically, RAID arrays were configured as SCSI chains, but nowadays you also find SATA, eSATA, and Fibre Channel. Either way, the idea is that data is being stored on multiple disks that work with each other. The number of disks and the way they work together is dependent on the level of RAID. For the exam, you need to know several levels of RAID including RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10 (also known as RAID 1+0). Table 15-1 describes each of these. Note that RAID 0 is the only one listed that is *not* fault tolerant, so from a security perspective it is not a viable option. Nevertheless, you should know it for the exam.

**Table 15-1** RAID Descriptions

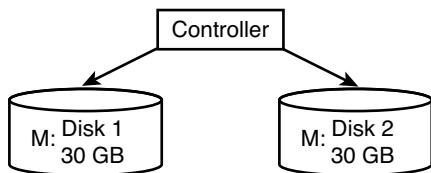
**Key Topic**

| RAID Level | Description                                                                                                                                                                                                                                                                                                                                                               | Fault Tolerant? | Minimum Number of Disks |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------------|
| RAID 0     | Striping<br><br>Data is striped across multiple disks to increase performance.                                                                                                                                                                                                                                                                                            | No              | Two                     |
| RAID 1     | Mirroring<br><br>Data is copied to two identical disks. If one disk fails, the other continues to operate. See Figure 15-1 for an illustration. This RAID version allows for the least amount of downtime because there is a complete copy of the data ready at a moment's notice. When each disk is connected to a separate controller, this is known as disk duplexing. | Yes             | Two (and two only)      |

| RAID Level                  | Description                                                                                                                                                                                                                                                                                                      | Fault Tolerant? | Minimum Number of Disks |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------------|
| <b>RAID 5</b>               | <p>Striping with Parity</p> <p>Data is striped across multiple disks; fault-tolerant parity data is also written to each disk. If one disk fails, the array can reconstruct the data from the parity information. See Figure 15-2 for an illustration.</p>                                                       | Yes             | Three                   |
| RAID 6                      | <p>Striping with Double Parity</p> <p>Data is striped across multiple disks as it is in <b>RAID 5</b>, but there are two stripes of parity information. This usually requires another disk in the array. This system can operate even with two failed drives and is more adequate for time-critical systems.</p> | Yes             | Four                    |
| RAID 0+1                    | <p>Combines the advantages of RAID 0 and <b>RAID 1</b>. Requires a minimum of four disks. This system contains two RAID 0 striped sets. Those two sets are mirrored.</p>                                                                                                                                         | Yes             | Four                    |
| RAID 10 (also known as 1+0) | <p>Combines the advantages of <b>RAID 1</b> and RAID 0. Requires a minimum of two disks but will usually have four or more. This system contains at least two mirrored disks that are then striped.</p>                                                                                                          | Yes             | Two (usually four)      |

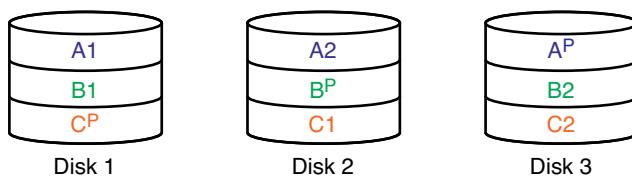
Figure 15-1 shows an illustration of **RAID 1**; you can see that data is written to both disks and that both disks collectively are known as the M: drive or M: *volume*. Figure 15-2 displays an illustration of **RAID 5**. In a **RAID 5** array, blocks of data are distributed to the disks (A1 and A2 are a block, B1 and B2 are a block, and so on), and parity information is written for each block of data. This is written to each disk in an alternating fashion (Ap, Bp, and such) so that the parity is also distributed. If one disk fails, the parity information from the other disks will reconstruct the data. It is important to make the distinction between fault tolerance and backup. *Fault tolerance* means that the hard drives can continue to function (with little or no downtime) even if there is a problem with one of the drives. *Backup* means that we are taking the data and copying it (and possibly compressing it) to another location for archival in the event of a disaster. An example of a disaster would be if *two* drives in a RAID

5 array were to fail. If an organization is worried that this disaster could happen, it should consider RAID 6, RAID 0+1, or the less common RAID 1+0.



**Key Topic**

**Figure 15-1** RAID 1 Illustration



**Key Topic**

**Figure 15-2** RAID 5 Illustration

Windows servers support RAID 0, 1, and 5 (and possibly 6 depending on the version) within the operating system. But most client operating systems cannot support RAID 1, 5, and 6. However, they *can* support hardware controllers that can create these arrays. Some motherboards have built-in RAID functionality as well.

Hardware is always the better way to go when it comes to RAID. Having a separate interface that controls the RAID configuration and handling is far superior to trying to control it with software within an operating system. The hardware could be an adapter card installed inside the computer, or an external box that connects to the computer or even to the network. When it comes to RAID in a network storage scenario, you are now dealing with network attached storage (NAS). These NAS points can be combined to form a storage area network (SAN), but any type of network attached storage will cost more money to an organization.

You can classify RAID in three different ways; these classifications can help when you plan which type of RAID system to implement.

- **Failure-resistant disk systems:** Protect against data loss due to disk failure. An example of this would be RAID 1 mirroring.
- **Failure-tolerant disk systems:** Protect against data loss due to any single component failure. An example of this would be RAID 1 mirroring with duplexing.
- **Disaster-tolerant disk systems:** Protect data by the creation of two independent zones, each of which provides access to stored data. An example of this would be RAID 0+1.

Of course, no matter how well you protect the data from failure, users still need to access the data, and to do so might require some redundant networking.

## Redundant Networking

Network connections can fail as well. And we all know how users need to have the network up and running—or there will be heck to pay. The security of an organization can be compromised if networking connections fail. Some types of connections you should consider include the following:

- Server network adapter connections
- Main connections to switches and routers
- The Internet connection

So basically, when I speak of redundant networking, I'm referring to any network connection of great importance that could fail. Generally, these connections will be located in the server room.

Redundant network adapters are commonly used to decrease or eliminate server downtime in the case that one network adapter fails. However, you must consider how they will be set up. Optimally, the second network adapter will take over immediately when the first one fails, but how will this be determined? There are applications that can control multiple network adapters, or the switch that they connect to can control where data is directed in the case of a failure. Also, multiple network adapters can be part of an individual collective interface. What you decide will be dictated by company policy, budgeting, and previously installed equipment. As a rule of thumb, you should use like network adapters when implementing redundancy; check the model and the version of the particular model to be exact. When installing multiple network adapters to a server, that computer then becomes known as a multihomed machine. It is important to consider how multiple adapters (and their operating systems) will behave normally and during a failure. Microsoft has some notes about this; I left a link in “View Recommended Resources” on the disc that accompanies this book. In some cases, you will install multiple physical network adapters, and in others you might opt for a single card that has multiple ports, such as the Intel PRO/1000 MT Dual Port Server Adapter. This is often a cheaper solution than installing multiple cards but provides a single point of failure in the form of one adapter card and one adapter card slot. In our original scenario we had domain controllers, database servers, web servers, and file servers; these would all do well with the addition of redundant network adapters.

Companies should always have at least one backup switch sitting on the shelf. If the company has only one switch, it is a desperate single point of failure. If a company has multiple switches stacked in a star-bus fashion, the whole stack can

be a single point of failure unless special backup ports are used (only available on certain switches). These special ports are often fiber-optic-based and are designed either for high-speed connections between switches or for redundancy. This concept should be employed at the master switch in a hierarchical star as well to avoid a complete network collapse. However, the hierarchical star is more secure than a star-bus configuration when it comes to network failure. In a hierarchical star, certain areas of the network still function even if one switch fails. This is a form of redundant topology.

Finally, your ISP is susceptible to failure as well—as I’m sure you are well aware. Most organizations rely on just one Internet connection for their entire network. This is another example of a single point of failure. Consider secondary connections to your ISP; known as a **redundant ISP**. If you have a T-1 line, perhaps a BRI connection will do. Or if you have a T-3, perhaps a PRI connection would be best. At the very least, a set of dial-up connections can be used for redundancy. Some companies install completely fault-tolerant, dual Internet connections, the second of which comes online immediately following a failure. If you use a web host for your website and/or e-mail, consider a mirror site or more than one. Basically, in a nutshell, it’s all about not being caught with your pants down. If an organization is without its Internet connection for more than a day (or hours in some cases), you know it will be the network admin and the security admin that will be the first on the chopping block, most likely followed by the ISP.

**NOTE** Network devices will fail. It’s just a matter of time. Earlier in the book we mentioned the concept of mean time between failure (MTBF)—a reliability term used to provide an average number of failures for a device per million hours of use. MTBF, along with mean time to repair (MTTR) and mean time to failure (MTTF), should be incorporated into your thought process when considering redundant networking.

## Redundant Servers

Let’s take it to the next level and discuss redundant servers. When redundant network adapters and disks are not enough, you might decide to cluster multiple servers together that act as a single entity. This will be more costly and require more administration but can provide a company with low downtime and a secure feeling. Two or more servers that work with each other are a **cluster**.

The clustering of servers can be broken down into two types:



- **Failover clusters:** Otherwise known as high-availability clusters, these are designed so that a secondary server can take over in the case that the primary one fails, with limited or no downtime. A failover cluster can reduce the chance of a single point of failure on a server, regardless of what failed on that server—hard disk, CPU, memory, and so on. An example of a failover cluster would be the usage of two Microsoft domain controllers. When the first domain controller fails, the secondary domain controller should be ready to go at a moment's notice. There can be tertiary and quaternary servers and beyond as well. It all depends on how many servers you think might fail concurrently. Another example would be the DNS server we talked about in the beginning of the chapter. If we wanted the DNS server to fail-closed, then we should set up a secondary DNS server as a failover, one that will be ready to go at a moment's notice.
- **Load-balancing clusters:** Load-balancing clusters are multiple computers connected together for the purpose of sharing resources such as CPU, RAM, and hard disks. In this way, the cluster can share CPU power, along with other resources, and balance the CPU load among all the servers. Microsoft's Cluster Server is an example of this (although it can also act in failover mode), enabling for parallel, high-performance computing. Several third-party vendors offer clustering software for operating systems and virtual operating systems as well. It is a common technique in web and FTP server farms, as well as in IRC servers, DNS servers, and NNTP servers.

Data can also be replicated back and forth between servers as it often is with database servers and web servers. This is actually a mixture of redundant data (data replication) and server clustering.

However, it doesn't matter how many servers you install in a cluster. If they are all local, they could all be affected by certain attacks or, worse yet, disasters. Enter the redundant site concept.

## Redundant Sites

Well, we have implemented redundant arrays of disks, redundant network adapters, redundant power, and even redundant servers. What is left? Devising a mirror of the entire network! That's right, a redundant site. Within the CIA triad, redundant sites fall into the category of *availability*. In the case of a disaster, a redundant site can act as a safe haven for your data and users. Redundant sites are sort of a gray area between redundancy and a disaster recovery method. If you have one and need to use it, a “disaster” has probably occurred. But, the better the redundant site, the less time the organization loses, and the less it seems like a disaster and more like a failure that you have prepared for. Of course, this all depends on the type of redundant site your organization decides on.

When it comes to the types of redundant sites, I like to refer to the story of Goldilocks and the three bears' three bowls of porridge. One was too hot, one too cold—and one just right. Most organizations opt for the warm redundant site as opposed to the hot or cold. Let's discuss these three now.

**Key Topic**

- **Hot site:** A near duplicate of the original site of the organization that can be up and running within minutes (maybe longer). Computers and phones are installed and ready to go, a simulated version of the server room stands ready, and the vast majority of the data is replicated to the site on a regular basis in the event that the original site is not accessible to users for whatever reason. Hot sites are used by companies that would face financial ruin in the case that a disaster makes their main site inaccessible for a few days or even a few hours. This is the only type of redundant site that can facilitate a full recovery.
- **Warm site:** Has computers, phones, and servers, but they might require some configuration before users can start working on them. The warm site will have backups of data that might need to be restored; they will probably be several days old. This is chosen the most often by organizations because it has a good amount of configuration yet remains less expensive than a hot site.
- **Cold site:** Has tables, chairs, bathrooms, and possibly some technical setup—for example, basic phone, data, and electric lines. Otherwise, a lot of configuration of computers and data restoration is necessary before the site can be properly utilized. This type of site is used only if a company can handle the stress of being nonproductive for a week or more.

Although they are redundant, these types of sites are generally known as backup sites because if they are required, a disaster has probably occurred. A good network security administrator tries to plan for, and rely on, redundancy and fault tolerance as much as possible before having to resort to disaster recovery methods.

## Redundant People

Well—not really redundant people (which I suppose would be clones), but rather the redundancy of a person's role in the organization. A person doesn't work for a company forever; in fact, the average length of employment for IT management persons is less than five years. This level of attrition is in part made up of persons who move to other departments, leave for another job, take leaves of absence, or retire. This leads to the important concept of *succession planning*: identifying *internal* people who understand the IT infrastructure and can take over in the event an important decision-maker departs; for example, IT directors, CIOs, CTOs, and other IT management persons. The concept trickles down to any IT person who works for the organization. That is where the concepts of job rotation and separation of

duties become very important. A high attrition rate requires cross-training of employees. In smaller companies, the loss of one smart IT person could be tantamount to a disaster if no one else understands (or has access to) the critical systems. That could truly be a disaster from a personnel standpoint, but much more lethal is a disaster concerning actual data.

## Disaster Recovery Planning and Procedures

Regardless of how much you planned out redundancy and fault tolerance, when disaster strikes, it can be devastating. There are three things that you should be concerned with as a network security administrator when it comes to disasters—your data, your server room, and the site in general. You need to have a powerful backup plan for your data and a comprehensive disaster recovery plan as well.

### Data Backup

Disaster recovery (or DR for short) is pretty simple in the case of data. If disaster strikes, you better have a good data backup plan; one that fits your organization's needs and budget. Your company might have a written policy as to what should be backed up, or you might need to decide what is best. Data can be backed up to a lot of different types of media (or to other computers, SANs, NAS devices, and to the cloud), but generally, one of the best local mediums is tape backup.

There are three tape backup types you should be aware of for the exam. Keep in mind that this list is not the end-all of backup types, but it gives a basic idea of the main types of backups used in the field. When performing any of these types of backups, the person must select what to back up. It could be a folder or an entire volume. For the sake of simplicity we call these folders.



- **Full backup:** Backs up all the contents of a folder. The full backup can be stored on one or more tapes. If more than one is used, the restore process would require starting with the oldest tape and moving through the tapes chronologically one by one. Full backups can use a lot of space, causing a backup operator to use a lot of backup tapes, which can be expensive. Full backups can also be time-consuming if there is a lot of data. So, often, incremental and differential backups are used with full backups as part of a backup plan.
- **Incremental backup:** Backs up only the contents of a folder that has changed since the last full backup or the last incremental backup. An incremental backup must be preceded by a full backup. Restoring the contents of a folder or volume would require a person to start with the full backup tape and then move on to each of the incremental backup tapes chronologically, ending with the latest incremental backup tape. Incremental backups started in the time of

floppy disks when storage space and backup speed were limited. Some operating systems and backup systems associate an archive bit (or archive flag) to any file that has been modified; this indicates to the backup program that it should be backed up during the next backup phase. If this is the case, the incremental backup resets the bit after backup is complete.

- **Differential backup:** Backs up only the contents of a folder that has changed since the last full backup. A differential backup must be preceded by a full backup. To restore data, a person would start with the full backup tape and then move on to the differential tape. Differential backups do not reset the archive bit when backing up. This means that incremental backups will not see or know that a differential backup has occurred.

Table 15-2 shows an example of a basic one-week backup schedule using the full and incremental backup types. A full backup is done on Monday, and incremental backups are done Tuesday through Friday.

**Table 15-2** Example Incremental Backup Schedule

**Key Topic**

| Day       | Backup Type        | Time   |
|-----------|--------------------|--------|
| Monday    | Full backup        | 6 p.m. |
| Tuesday   | Incremental backup | 6 p.m. |
| Wednesday | Incremental backup | 6 p.m. |
| Thursday  | Incremental backup | 6 p.m. |
| Friday    | Incremental backup | 6 p.m. |

In this schedule, five backup tapes are required, one for each day. Let's say that the backups are done at 6 p.m. daily. Often an organization might employ a sixth tape, which is a dummy tape. This tape is put in the tape drive every morning by the backup operator and is replaced with the proper daily tape at 5:30 p.m. when everyone has left the building. This prevents data theft during the day. The real tapes are kept locked up until needed. Tapes might be reused when the cycle is complete, or an organization might opt to archive certain tapes each week, for example, the full backup tapes, and use new tapes every Monday. Another option is to run a complete full backup (which might be time-consuming) over the weekend and archive that tape every Monday. As long as no data loss is reported, this is a feasible option.

Let's say that this backup procedure was used to back up a server. Now, let's say that the server crashed on Wednesday at 9 p.m., and the hard drive data was lost. A backup operator arriving on the scene Thursday morning would need to review any logs available to find out when the server crashed. Then, after an admin fixes

the server, the backup operator would need to restore the data. This would require starting with the Monday full backup tape and continuing on to the Tuesday and Wednesday incremental backup tapes. So three tapes in total would be needed to complete the restore.

Table 15-3 shows another possible backup schedule where a full backup is done on Monday and differential backups are done on Wednesday and Friday.

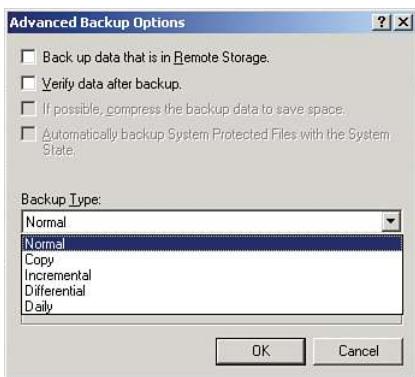


**Table 15-3** Example Differential Backup Schedule

| Day       | Backup Type         | Time   |
|-----------|---------------------|--------|
| Monday    | Full backup         | 6 p.m. |
| Tuesday   | None                |        |
| Wednesday | Differential backup | 6 p.m. |
| Thursday  | None                |        |
| Friday    | Differential backup | 6 p.m. |

Let's say the backup operator needed to restore data on Monday morning due to a failure over the weekend. The backup operator would need two backup tapes, the previous Monday full backup and the Friday differential backup, because the differential backup would have backed up everything since the last full backup. The Wednesday differential backup would not be necessary for recovery; contrast this with the incremental backup schedule from Table 15-2 where each tape would be needed for restoration. In a differential backup scenario the "clear archive bit" is not selected, so a differential backup will back up things that may have already been backed up by a previous differential backup. In an incremental backup scenario, the "clear archive bit" option *is* selected, and so items that are backed up by an incremental are not backed up by a subsequent incremental.

Windows Server operating systems have the capability to do full backups, incremental backups, and differential backups, as shown in Figure 15-3. Windows refers to a full backup as "normal." You will note that Windows also enables copy backups and daily backups.



**Figure 15-3** Windows Server Backup Types

Now, the schedules we just showed in Tables 15-2 and 15-3 are basic backup methods, also known as backup rotation schemes. Organizations might also do something similar over a 2-week period. However, you should also be aware of a couple of other backup schemes used in the field. These might use one or more of the backup types mentioned previously.

- **10 tape rotation:** This method is simple and provides easy access to data that has been backed up. It can be accomplished during a 2-week backup period; each tape is used once per day for 2 weeks. Then the entire set is recycled. Generally, this is similar to the one-week schedule shown previously; however, the second Monday might be a differential backup instead of a full backup. And the second Friday might be a full backup, which is archived. There are several options; you would need to run some backups and see which is best for you given the amount of tapes required and time spent running the backups.
- **Grandfather-father-son:** This backup rotation scheme is probably the most common backup method used. When attempting to use this scheme, three sets of backup tapes must be defined—usually they are daily, weekly, and monthly, which correspond to son, father, and grandfather. Backups are rotated on a daily basis; normally the last one of the week will be graduated to father status. Weekly (father) backups are rotated on a weekly basis, with the last one of the month being graduated to grandfather status. Often, monthly (grandfather) backups, or a copy of them, are archived offsite.
- **Towers of Hanoi:** This backup rotation scheme is based on the mathematics of the Towers of Hanoi puzzle. This also uses three backup sets, but they are rotated differently. Without getting into the mathematics behind it, the basic idea is that the first tape is used every second day, the second tape is used every fourth day, and the third tape is used every eighth day. Table 15-4 shows an

**Key Topic**

example of this. Keep in mind that this can go further; a fourth tape can be used every 16th day, and a fifth tape every 32nd day, and so on, although it gets much more complex to remember what tapes to use to back up and which order to go by when restoring. The table shows an example with three tape sets represented as sets A, B, and C.

**Table 15-4** Example of Towers of Hanoi Three-Tape Schedule

| <b>Day of the Cycle</b> |   |   |   |   |   |   |   |   |
|-------------------------|---|---|---|---|---|---|---|---|
|                         | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| <b>Tape</b>             | A |   | A |   | A |   | A |   |
|                         |   | B |   |   |   | B |   |   |
|                         |   |   |   | C |   |   |   | C |

To avoid the rewriting of data, start on the fourth day of the cycle with tape C. This rotation scheme should be written out and perhaps calculated during the planning stage before it is implemented. Also, due to the complexity of the scheme, a restore sequence should be tested as well.

Tapes should be stored in a cool, dry area, away from sunlight, power lines, and other power sources. Most tape backup vendors have specific guidelines as to the temperature and humidity ranges for storage, along with other storage guidelines.

Tape backup methods and tape integrity should always be tested by restoring all or part of a backup.

It's also possible to archive data to a third party. This could be for backup purposes or for complete file replication. Several companies offer this type of service, and you can usually select to archive data over the Internet or by courier.

Many organizations back up to tape. But many other organizations are far too large for tape backup, and don't have the personnel or equipment necessary to archive properly. In these "big data" scenarios, data might be stored on the cloud, or archived with a third-party such as Iron Mountain. Whatever your data backup method, make sure that there is some kind of archival offsite in the case of a true disaster. Optimally, this will be in a sister site in another city but regardless should be geographically distant from the main site. It is an integral part of disaster recovery planning.

## DR Planning

Before we can plan for disasters, we need to define exactly what disasters are possible and list them in order starting with the most probable. Sounds a bit morbid, but it's necessary to ensure the long-term welfare of your organization.

What could go wrong? Let's focus in on the server room in the beginning of the chapter as our scenario. As you remember, we have nine servers, networking equipment, a PBX, and a few workstations—a pretty typical server room for a midsized company. Keep in mind that larger organizations will have more equipment, bigger server rooms, and more to consider when it comes to DR planning.

Disasters can be divided into two categories: natural and manmade. Some of the disasters that could render your server room inoperable include the following:

- **Fire:** Fire is probably the number one planned for disaster. This is partially because most municipalities require some sort of fire suppression system, as well as the fact that most organizations' policies define the usage of a proper fire suppression system. You probably recall the three main types of fire extinguishers: A (for ash fires), B (for gas and other flammable liquid fires), and C (for electrical fires). Unfortunately, these and the standard sprinkler system in the rest of the building are not adequate for a server room. If there were a fire, the material from the fire extinguisher or the water from the sprinkler system would damage the equipment, making the disaster even worse! Instead, a server room should be equipped with a proper system of its own such as DuPont FM-200. This uses a large tank that stores a clean agent fire extinguisher that is sprayed from one or more nozzles in the ceiling of the server room. It can put out fires of all types in seconds. A product such as this can be used safely when people are present; however, most systems also employ a *very* loud alarm that tells all personnel to leave the server room. It is wise to run through several fire suppression alarm tests and fire drills, ensuring that the alarm will sound when necessary and that personnel know what do to when the alarm sounds. For example, escape plans should be posted, and battery-backup exit signs should be installed in various locations throughout the building so that employees know the quickest escape route in the case of a fire. Fire drills (and other safety drills) should be performed periodically so that the organization can analyze the security posture of their safety plan.
- **Flood:** The best way to avoid server room damage in the case of a flood is to locate the server room on the first floor or higher, not in a basement. There's not much you can do about the location of a building, but if it is in a flood zone, it makes the use of a warm or hot site that much more imperative. And a server room could also be flooded by other things such as boilers. The room should not be adjacent to, or on the same floor as, a boiler room. It should also be located away from other water sources such as bathrooms and any sprinkler systems. The server room should be thought of three-dimensionally; the floors, walls, and ceiling should be analyzed and protected. Some server rooms are designed to be a room within a room and might have drainage installed as well.

- **Long-term power loss:** Short-term power loss should be countered by the UPS, but long-term power loss requires a backup generator and possibly a redundant site.
- **Theft and malicious attack:** Theft and malicious attack can also cause a disaster, if the right data is stolen. Physical security such as door locks/access systems and video cameras should be implemented to avoid this. Servers should be cable-locked to their server racks, and removable hard drives (if any are used) should have key access. Not only does a security administrator have the task of writing policies and procedures that govern the security of server rooms and data centers, but that person will often have the task of *enforcing* those policies—meaning muscle in the form of security guards, and dual-class technician/guards—or by otherwise having the right to terminate employees as needed, contact and work with the authorities, and so on. Physical security is covered in more depth in Chapter 9, “Physical Security and Authentication Models.” Malicious network attacks also need to be warded off; these are covered in depth in Chapter 6, “Networking Protocols and Threats.”
- **Loss of building:** Temporary loss of the building due to gas leak, malicious attack, inaccessibility due to crime scene investigation, or natural event will require personnel to access a redundant site. Your server room should have as much data archived as possible, and the redundant site should be warm enough to keep business running. A plan should be in place as to how data will be restored at the redundant site and how the network will be made functional.

**Disaster recovery plans** should include information regarding redundancy, such as sites and backup, but should not include information that deals with the day-to-day operations of an organization, such as updating computers, patch management, monitoring and audits, and so on. It is important to include only what is necessary in a disaster recovery plan. Too much information can make it difficult to use when a disaster does strike.

Although not an exhaustive set, the following written disaster recovery policies, procedures, and information should be part of your disaster recovery plan:

- **Contact information:** Who you should contact if a disaster occurs and how employees will contact the organization.
- **Impact determination:** A procedure to determine a disaster’s full impact on the organization. This includes an evaluation of assets lost and the cost to replace those assets.
- **Recovery plan:** This will be based on the determination of disaster impact. This will have many permutations depending on the type of disaster. Although it is impossible to foresee every possible event, the previous list gives a good

starting point. The recovery plan includes an estimated time to complete recovery and a set of steps defining the order of what will be recovered and when.

- **Business continuity plan:** A BCP defines how the business will continue to operate if a disaster occurs; this plan is often carried out by a team of individuals. BCPs are also referred to as continuity of operations plans. Over the years, BCPs have become much more important, and depending on the organization, the BCP might actually encompass the entire DRP. It also comprises **business impact analysis**—the examination of critical versus noncritical functions. These functions are assigned two different values or metrics: **recovery time objective (RTO)**, the acceptable amount of time to restore a function (for example, the time required for a service to be restored after a disaster), and **recovery point objective (RPO)**, the acceptable latency of data, or the maximum tolerable time that data can remain inaccessible after a disaster. It's impossible to foresee exactly how long it will take to restore service after a disaster, but with the use of proper archival, hot/warm/cold sites, and redundant systems, a general timeframe can be laid out, and an organization will be able to decide on a maximum timeframe to get data back online.

Some organizations will have a crisis management group that meets every so often to discuss the BCP. Instead of running full-scale drills, they might run through tabletop exercises, where a talk-through of simulated disasters (in real time) is performed—a sort of role-playing, if you will. This can save time and be less disruptive to employees, but it is more than just a read-through of the BCP.

- **Copies of agreements:** Copies of any agreements with vendors of redundant sites, ISPs, building management, and so on should be stored with the DR plan.
- **Disaster recovery drills and exercises:** Employees should be drilled on what to do if a disaster occurs. These exercises should be written out step-by-step and should conform to safety standards.
- **Hierarchical list of critical systems:** This is a list of all systems necessary for business operations: domain controllers, firewalls, switches, DNS servers, file servers, web servers, and so on. They should be listed by priority. Systems such as client computers, test computers, and training systems would be last on the list or not listed at all.

This information should be accessible at the company site, and a copy should be stored offsite as well. It might be that your organization conforms to special compliance rules; these should be consulted when designing a DR plan. Depending on the type of organization, there might be other items that go into your DR plan. We cover some of these in more depth in Chapter 16.

## Chapter Summary

This chapter defined in the strictest sense how to protect against potential failures, and how to recover from would-be disasters. Redundancy of data, services, and power is your best bet when it comes to the failure of equipment and servers. Data archiving and procedural planning are vitally important considerations when you are preparing for the unlikely scenario of disaster.

Any single point of failure is a bad thing. In a system of parts, that single point will cause the entire system to fail. It's common knowledge that hard drives will fail, power supplies will fail, power will fail, networking connections will fail, and so on. If you run your systems long enough, a failure will occur—over enough time the probability becomes 100%.

It's the redundancy that can save you: RAID systems and clustered servers for data; multiple power supplies, UPS devices, and generators for power; multihomed servers and multiple Internet connections for the networking of data; even entire secondary worksites and people waiting in the wings to take over when necessary. All these things can provide for a redundant IT infrastructure. But be wary, too much redundancy might blow your IT budget, leaving you little for maintenance, future planning, and disaster planning.

Although the chances of a disaster are slim, they do happen. The list of possible disasters in this chapter is not a complete one either, but it shows the more common tragedies you might encounter. The prepared organization will have a well-defined archival plan that should include a minimum of tape backup that is stored offsite. That protects the bulk of the data, but a DR plan is necessary to protect the employees, servers, and other equipment as well. And in the case of a loss of building, a backup worksite becomes imperative.

Many companies will have one person who spearheads the development of a DR plan, but it should be reviewed and mocked up by a group of people, with one person always ready to succeed the DR plan developer in the case that person leaves the organization.

## 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 15-5 lists a reference of these key topics and the page number on which each is found.

**Table 15-5** Key Topics for Chapter 15

| Key Topic Element | Description                          | Page Number |
|-------------------|--------------------------------------|-------------|
| Bulleted list     | Power failures                       | 578         |
| Table 15-1        | RAID descriptions                    | 583         |
| Figure 15-1       | RAID 1 illustration                  | 585         |
| Figure 15-2       | RAID 5 illustration                  | 585         |
| Bulleted list     | Server cluster types                 | 588         |
| Bulleted list     | Types of redundant sites             | 589         |
| Bulleted list     | Backup types                         | 590         |
| Table 15-2        | Example incremental backup schedule  | 591         |
| Table 15-3        | Example differential backup schedule | 592         |
| Bulleted list     | Backup rotation schemes              | 593         |

## Define Key Terms

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

single point of failure, surge, spike, sag, brownout, blackout, redundant power supply, uninterruptible power supply (UPS), backup generator, standby generator, RAID 1, disk duplexing, RAID 5, redundant ISP, cluster, failover clusters, load-balancing clusters, hot site, warm site, cold site, full backup, incremental backup, differential backup, 10 tape rotation, grandfather-father-son, Towers of Hanoi, disaster recovery plan, business impact analysis, recovery time objective (RTO), recovery point objective (RPO)

## Review Questions

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

- Which of the following RAID versions offers the least amount of performance degradation when a disk in the array fails?
  - RAID 0
  - RAID 1
  - RAID 4
  - RAID 5

- 2.** Which of the following can facilitate a full recovery within minutes?
  - A.** Warm site
  - B.** Cold site
  - C.** Reestablishing a mirror
  - D.** Hot site
  
- 3.** What device should be used to ensure that a server does not shut down when there is a power outage?
  - A.** RAID 1 box
  - B.** UPS
  - C.** Redundant NIC
  - D.** Hot site
  
- 4.** Which of the following tape backup methods enables daily backups, weekly full backups, and monthly full backups?
  - A.** Towers of Hanoi
  - B.** Incremental
  - C.** Grandfather-father-son
  - D.** Differential
  
- 5.** To prevent electrical damage to a computer and its peripherals, the computer should be connected to what?
  - A.** Power strip
  - B.** Power inverter
  - C.** AC to DC converter
  - D.** UPS
  
- 6.** Which of the following would not be considered part of a disaster recovery plan?
  - A.** Hot site
  - B.** Patch management software
  - C.** Backing up computers
  - D.** Tape backup

7. Which of the following factors should you consider when evaluating assets to a company? (Select the two best answers.)
  - A. Their value to the company
  - B. Their replacement cost
  - C. Where they were purchased from
  - D. Their salvage value
8. You are using the following backup scheme: A full backup is made every Friday night at 6 p.m., and differential backups are made every other night at 6 p.m. Your database server fails on a Thursday afternoon at 4 p.m. How many tapes will you need to restore the database server?
  - A. One
  - B. Two
  - C. Three
  - D. Four
9. Of the following, what is the worst place to store a backup tape?
  - A. Near a bundle of fiber-optic cables
  - B. Near a power line
  - C. Near a server
  - D. Near an LCD screen
10. Critical equipment should always be able to get power. What is the correct order of devices that your critical equipment should draw power from?
  - A. Generator, line conditioner, UPS battery
  - B. Line conditioner, UPS battery, generator
  - C. Generator, UPS battery, line conditioner
  - D. Line conditioner, generator, UPS battery
11. What is the best way to test the integrity of a company's backed up data?
  - A. Conduct another backup
  - B. Use software to recover deleted files
  - C. Review written procedures
  - D. Restore part of the backup

- 12.** Your company has six web servers. You are implementing load balancing. What is this an example of?
- A.** UPS
  - B.** Redundant servers
  - C.** RAID
  - D.** Warm site
- 13.** Your company has a T-1 connection to the Internet. Which of the following can enable your network to remain operational even if the T-1 fails?
- A.** Redundant network adapters
  - B.** RAID 5
  - C.** Redundant ISP
  - D.** UPS
- 14.** Which action should be taken to protect against a complete disaster in the case that a primary company's site is permanently lost?
- A.** Back up all data to tape, and store those tapes at a sister site in another city.
  - B.** Back up all data to tape, and store those tapes at a sister site across the street.
  - C.** Back up all data to disk, and store the disk in a safe deposit box at the administrator's home.
  - D.** Back up all data to disk, and store the disk in a safe in the building's basement.
- 15.** Of the following backup types, which describes the backup of files that have changed since the last full or incremental backup?
- A.** Incremental
  - B.** Differential
  - C.** Full
  - D.** Copy
- 16.** Michael's company has a single web server that is connected to three other distribution servers. What is the greatest risk involved in this scenario?
- A.** Fraggle attack
  - B.** Single point of failure

- C. Denial-of-service attack
  - D. Man-in-the-middle attack
17. Which of the following defines a business goal for system restoration and *acceptable* data loss?
- A. RPO
  - B. Warm site
  - C. MTBF
  - D. MTTR
18. Which of the following uses multiple computers to share work?
- A. RAID
  - B. VPN concentrator
  - C. Load balancing
  - D. Switching
19. You have been tasked with increasing the level of server fault tolerance, but you have been given no budget to perform the task. Which of the following should you implement to ensure that servers' data can withstand hardware failure?
- A. RAID
  - B. Hardware load balancing
  - C. A cold site
  - D. Towers of Hanoi
20. Which of the following provides for the best application availability and can be easily expanded as an organization's demand grows?
- A. RAID 6
  - B. Server virtualization
  - C. Multi-CPU motherboards
  - D. Load balancing

## Answers and Explanations

1. **B.** RAID 1 is known as mirroring. If one drive fails, the other will still function and there will be no downtime and no degraded performance. All the rest of the answers are striping-based and therefore have either downtime or degraded performance associated with them. RAID 5 is the second best option because in many scenarios it will have zero downtime and little degraded performance. RAID 0 will not recover from a failure; it is not fault tolerant.
2. **D.** A hot site can facilitate a full recovery of communications software and equipment within minutes. Warm and cold sites cannot facilitate a full recovery but may have some of the options necessary to continue business. Reestablishing a mirror will not necessarily implement a full recovery of data communications or equipment.
3. **B.** A UPS (uninterruptible power supply) ensures that a computer will keep running even if a power outage occurs. The number of minutes the computer can continue in this fashion depends on the type of UPS and battery it contains. A backup generator can also be used, but it does not guarantee 100% uptime, because there might be a delay between when the power outage occurs and when the generator comes online. RAID 1 has to do with the fault tolerance of data. Redundant NICs (network interface cards aka network adapters) are used on servers in the case that one of them fails. Hot sites are completely different places that a company can inhabit. Although the hot site can be ready in minutes, and although it may have a mirror of the server in question, it does not ensure that the original server will not shut down during a power outage.
4. **C.** The grandfather-father-son (GFS) backup scheme generally uses daily backups (the son), weekly backups (the father), and monthly backups (the grandfather). The Towers of Hanoi is a more complex strategy based on a puzzle. Incremental backups are simply one-time backups that back up all data that has changed since the last incremental backup. These might be used as the son in a GFS scheme. Differential backups back up everything since the last full backup.
5. **D.** A UPS (uninterruptible power supply) protects computer equipment against surges, spikes, sags, brownouts, and blackouts. Power strips, unlike surge protectors, do not protect against surges.
6. **B.** Patching a system is part of the normal maintenance of a computer. In the case of a disaster to a particular computer, the computer's OS and latest service pack would have to be reinstalled. The same would be true in the case of a disaster to a larger area, like the building. Hot sites, backing up computers, and tape backup are all components of a disaster recovery plan.

7. **A.** and **B.** When evaluating assets to a company, it is important to know the replacement cost of those assets and the value of the assets to the company. If the assets were lost or stolen, the salvage value is not important, and although you may want to know where the assets were purchased from, it is not one of the best answers.
8. **B.** You need two tapes to restore the database server—the full backup tape made on Friday and the differential backup tape made on the following Wednesday. Only the last differential tape is needed. When restoring the database server, the technician must remember to start with the full backup tape.
9. **B.** Backup tapes should be kept away from power sources, including power lines, CRT monitors, speakers, and so on. And the admin should keep backup tapes away from sources that might emit EMI. LCD screens, servers, and fiber-optic cables have low EMI emissions.
10. **B.** The line conditioner is constantly serving critical equipment with clean power. It should be first and should always be on. The UPS battery should kick in only if there is a power outage. Finally, the generator should kick in only when the UPS battery is about to run out of power. Often, the line conditioner and UPS battery will be the same device. However, the line conditioner function will always be used, but the battery comes into play only when there is a power outage, or brownout.
11. **D.** The best way to test the integrity of backed up data is to restore part of that backup. Conducting another backup will tell you if the backup procedure is working properly, and if isn't, after testing the integrity of the backup and after the restore, a person might need to use software to recover deleted files. It's always important to review written procedures and amend them if need be.
12. **B.** Load balancing is a method used when you have redundant servers. In this case, the six web servers will serve data equally to users. The UPS is an uninterruptible power supply, and RAID is the redundant array of inexpensive disks. A warm site is a secondary site that a company can use if a disaster occurs; a warm site can be up and running within a few hours or a day.
13. **C.** A secondary ISP enables the network to remain operational and still gain Internet access even if the T-1 connection fails. This generally means that there will be a second ISP and a secondary physical connection to the Internet. Redundant network adapters are used on servers so that the server can have a higher percentage of uptime. **RAID 5** is used for redundancy of data and spreads the data over three or more disks. A UPS is used in the case of a power outage.
14. **A.** In the case that a building's primary site is lost, data should be backed up to tape stored at a sister site in another city. Storing information across the

street might not be good enough, especially if the area has to be evacuated. Company information should never be stored at an employee's home. And of course if the data were stored in the primary building's basement and there were a complete disaster at the primary site, that data would also be lost.

15. **A.** An incremental backup backs up only the files that have changed since the last incremental or full backup. Generally it is used as a daily backup. Differential backups are meant to be used to back up files that have changed since the last full backup. A full backup backs up all files in a particular folder or drive, depending on what has been selected; this is regardless of any previous differential or incremental backups. Copies of data can be made, but they will not affect backup rotations that include incremental, differential, and full backups. Technically, this question could be answered "Incremental" or "Differential," but "Incremental" is the accepted (and therefore best) answer. The CompTIA objectives expect a person to understand that an incremental backup will back up anything that was created/changed since the last incremental backup, or the last full backup if that was the last one completed.
16. **B.** The greatest risk involved in this scenario is that the single web server is a single point of failure regardless that it is connected to three other distribution servers. If the web server goes down or is compromised, no one can access the company's website. A Fraggle is a type of denial-of-service attack. Although denial-of-service attacks are a risk to web servers, they are not the greatest risk in this particular scenario. A company should implement as much redundancy as possible.
17. **A.** An RPO (recovery point objective) defines acceptable data loss. A warm site is a secondary site that will have computers and phones ready for users, but data and services need to be configured and loaded before work can commence. MTBF is the mean time between failure, which defines the average number of failures per million hours, and is usually a number derived from multiple customers of a product. MTTR is the mean time to repair. Both of these are more similar to RTO as opposed to RPO.
18. **C.** Load balancing uses multiple computers to share work, for example, in a load-balancing cluster configuration. RAID uses multiple hard drives to increase speed or create fault tolerance. VPN concentrators allow for remote access of multiple employees over the Internet. Switching (in its simplest form) is the moving of data across the LAN.
19. **A.** RAID should be employed; specifically a fault-tolerant version of RAID (1, 5, 6, and so on). This will ensure that data will still be accessible if one drive fails. Load balancing uses multiple computers to share the load of processing data—often in the form of CPU and RAM collectives—but it does not ensure

that data will be accessible in the case of a failure. A cold site is not fault tolerant because it takes at least a day or two to get it up and running. Towers of Hanoi is a tape backup schedule, and as such is not fault tolerant either.

- 20. D.** Load balancing is the best option for application availability and expansion. You can cluster multiple servers together to make a more powerful super-computer of sorts—one that can handle more and more simultaneous access requests. RAID 6 is meant more for data files, not applications. It may or may not be expandable depending on the system used. Multi-CPU motherboards are used in servers and power workstations, but are internal to one system. The CPUs are indeed used together, but will not help with expandability, unless used in a load-balancing scenario.

## Case Study for Chapter 15

The case study in this chapter offers a generic scenario for you to read through and answer according to your own technology and experiences. At the end of the section is the example solution. Your solution will vary in comparison to the book, but both can certainly be valid. The case study solution also points to a hands-on video and simulation, which can be found on the book's disc.

### Case Study 15-1: Configuring RAID

**Scenario:** You have a mission-critical server that cannot be allowed to fail completely. And this time you have some IT budget to work with. You must make sure that the operating system, applications, *and* the data does not fail.

What type of RAID should you use to make sure the OS and applications are available all of the time?

What type of RAID should you implement to ensure that data will be accessible, even in the event of a failure? For the fault tolerance of the data, should you opt for a hardware solution or a software solution? Should it be internal or external?

## Case Study Solution

### Case Study 15-1 Solution

You should strongly consider **RAID 1** (mirroring) with disk duplexing to protect the OS and the applications. This is the type of solution that will mirror the C: drive. If one drive fails, the other will continue to work with no downtime. You can replace the drive during off-hours.

For the data, **RAID 5**, 6, and possibly 10, are highly recommended. With **RAID 5**, if one drive fails, the data remains accessible. In RAID 6, two drives can fail and the data remains accessible. And of course, the data can be rebuilt from the parity data when you are ready. If you have the budget backing you, the best option is to use external hard drive boxes with hot-swappable capabilities.

**Video Solution:** Watch the video solution “15-1: Configuring RAID” on the accompanying disc.

**Simulation:** Complete the simulation “15-1: Configuring RAID” on the accompanying disc.

*This page intentionally left blank*



### This chapter covers the following subjects:

- **Environmental Controls:** When dealing with the environment, it is important for a security person to consider fire suppression methods, heating, cooling, ventilation, shielding, and how to protect the server room. This section covers fire suppression methods, such as fire extinguishers, sprinkler systems, and special hazard protection, and HVAC, shielding, and the Faraday cage concept.
- **Social Engineering:** This section delves into the methods and techniques that social engineers can employ to gain access to buildings and systems and obtain company data and personal information. It also covers the various ways that these social engineers can be defeated.
- **Legislative and Organizational Policies:** In this section, you learn about ways to classify data, laws that protect individual privacy, personnel security policies and how to implement them, service-level agreements, the safe disposal of computers, and incident response procedures.

This chapter covers a portion of the CompTIA Security+ SY0-401 objectives 2.1 through 2.7, 2.9, 3.2, 3.3, 4.2, 4.3, 4.4, and 4.5.

# Policies, Procedures, and People

The idea behind this chapter is to examine the people who work for an organization, and how to protect their privacy, while still protecting your infrastructure from *them!* Environmental controls, policies, and procedures can help to protect legitimate individuals and help protect the infrastructure from malicious individuals and social engineers.

This is the last chapter of actual objective content for the Security+ exam, but you will no doubt see several questions on the exam about these topics. The concepts covered in this chapter are a bit of a hodge-podge, covering concepts less about computers, and more on the periphery of technology security, but I have tried to line them up in a way that will make for easy reading and recall. We start with fire suppression and social engineering, which are the first and second sections. That's not to say that policies and procedures are not important, and we do indeed move on to those in the third section.

When going through this chapter, try to keep an open mind as to the different roles a security person might be placed in. Imagine branching out beyond computers, servers, and networks, and developing security for the entire organization and its personnel.

## Foundation Topics

### Environmental Controls

Although it is usually the duty of the IT director and building management to take care of the installation, maintenance, and repair of environmental controls, you also should have a basic knowledge of how these systems function. Significant concepts include fire suppression, HVAC, and shielding of equipment. By far, the concept a person would spend the most time dealing with when planning a server room is fire suppression.

#### Fire Suppression

We talked about fire suppression somewhat in Chapter 15, “Redundancy and Disaster Recovery,” but we need to dig a bit deeper into the types you can

employ, and some of the policies and procedures involved with fire suppression. **Fire suppression** is the process of controlling and/or extinguishing fires to protect an organization's employees, its data, and its equipment. There are basically three types of fire suppression you need to know for the CompTIA Security+ exam: handheld fire extinguisher solutions, sprinkler systems, and special hazard protection systems such as those used in server rooms.

## Fire Extinguishers

Be careful when selecting a handheld fire extinguisher. There are several types to choose from; they vary depending on what type of environment you work in. Keep in mind that any one of these will probably cause damage to computers, phones, and other electronics. With only a couple exceptions, these solutions should not be used in a server room or other critical areas of your organization. Here are some of the classifications of fires and their indicators on corresponding fire extinguishers:



- **Fire Class A:** Denoted by a green triangle, this class defines use for ordinary fires consuming solid combustibles such as wood. Think A for “ash” to help remember this type. Water-based extinguishers are suitable for Class A fires only and should not be used in a server room.
- **Fire Class B:** Represented by a red square, this type defines use for flammable liquid and gas fires. I like to remember this by associating B with “butane” because butane is a highly flammable gas.
- **Fire Class C:** Indicated with a blue circle, this type defines use for electrical fires—for example, when an outlet is overloaded. Think C for “copper” as in copper electrical wiring to aid in memorizing this type. If a fire occurs in a server room, and you don’t have a special hazard system (not wise), the multi-purpose BC extinguisher (CO<sub>2</sub>) is the best handheld extinguisher to use. Electrical fires are the most likely type of fire in a server room.
- **Fire Class D:** Designated with a yellow decagon, this type defines use for combustible metal fires such as magnesium, titanium, and lithium. A Class D extinguisher is effective in case a laptop’s batteries spontaneously ignite. Chemical laboratories and PC repair labs should definitely have one of these available. Metal fires can easily and quickly spread to become ordinary fires. These fire extinguishers are usually yellow; it is one of only a couple that deviate from the standard red color. Also, this is the only other exception when it comes to the use of extinguishers in a critical area of your organization. Because of those two reasons, I like to remember it by associating D with “deviate.”
- **Fire Class K:** Symbolized as a black hexagon, this type is for cooking oil fires. This is one type of extinguisher that should be in any kitchen. This is

important if your organization has a cafeteria with cooking equipment. Think K for “kitchen” when remembering this type.

The previous bulleted list is not an official standard but is used by most manufacturers of fire extinguishers in the United States. Other countries might have a slightly different system.

In general, the most common type of fire extinguisher used in a building is the multipurpose dry-chemical ABC extinguisher. However, this is extremely messy—it gets into everything! Plus, it can cause corrosion to computer components over time. For server rooms, BC extinguishers are sometimes employed; the most common is the carbon dioxide (CO<sub>2</sub>) extinguisher. The CO<sub>2</sub> extinguisher displaces oxygen, which is needed for a fire to burn, in addition to heat and fuel, which collectively make up the fire triangle. CO<sub>2</sub> extinguishers are relatively safe for computer components, especially compared to ABC extinguishers. However, the CO<sub>2</sub> extinguisher can possibly cause damage to computer components from electrostatic discharge (ESD), although this is rare. Also, if carbon dioxide is released in an enclosed space where people are present, there is a risk of suffocation. If the organization has the money, it is far more preferable to use an ABC-rated Halotron extinguisher in the server room—or better yet, a special hazard protection system.

Older extinguishants, such as Halon, are not used anymore because they are harmful to the environment. Less-developed countries might still use them, but most governments have banned the use of Halon. If you see one of these, it should be replaced with a newer extinguisher that uses environment-safe halocarbon agents such as Halotron or FE-36. These are known as gaseous clean agents that are not only safe on humans and safe for IT equipment, but are better for the environment as well. Gaseous fire suppression systems are the best for server rooms.

## Sprinkler Systems

The most common type of fire sprinkler system consists of a pressurized water supply system that can deliver a high quantity of water to an entire building via a piping distribution system. This is known as a **wet pipe sprinkler system**. Typical to these systems are sprinkler heads with glass bulbs (often red) or two-part metal links.

When a certain amount of predetermined heat reaches the bulb or link, it causes it to shatter or break, applying pressure to the sprinkler cap and initiating the flow of water from that sprinkler and perhaps others in the same zone. The entire system is usually controlled by a valve assembly, often located in the building’s basement. Some organizations might have a need for a dry pipe system, which is necessary in spaces where the temperature of that area of the building can be cold enough to freeze the water in a wet pipe system. In this type of system, the pipes are pressurized with air, and water is sent through the system only if necessary; for example, during a fire.

Regardless of the system, an organization should conduct periodic fire drills to simulate a real fire and sprinkler system activation. Afterward, the security administrator should simulate disaster recovery procedures, as detailed in Chapter 15.

Most local municipalities require that organizations possess a sprinkler system that covers all the building's floor space. However, the standard wet pipe or dry pipe systems are not acceptable in server rooms because if set off, they will most likely damage the equipment within. If a person were working in the server room and somehow damaged a pipe, it could discharge; possibly sending a few servers to the scrap heap. Instead, another option for a server room would be a pre-action sprinkler system (and possibly a special hazard protection system in addition to that). A **pre-action sprinkler system** is similar to a dry pipe system, but there are requirements for it to be set off such as heat or smoke. So, even if a person were to damage one of the pipes in the sprinkler system, the pre-action system would not be set off.

## Special Hazard Protection Systems

I've mentioned several times that your server room contains the livelihood of your organization—its data. If you don't protect the data, you'll be out of a job. One way to protect the server room is by installing a clean agent fire suppression system. Special clean agent fire extinguishers, such as Halotron and FE-36, are recommended for server rooms because they leave no residue after the fire is extinguished, reducing the likelihood of damage to computer systems and networking equipment. Also, they are rated as ABC, so not only can they put out electrical fires, but they can also put out the ash fire that will most likely ensue. All the other systems mentioned up to this point can easily cause computer failure if they are discharged.

The ultimate solution would be to equip the server room with a **special hazard protection system**, a clean agent system, such as FM-200. This gaseous system would be installed in addition to the pre-action system (or other dry pipe system) if the organization can afford it. This system uses a large tank that stores a clean agent fire extinguishant in the form of a liquid. It is sprayed from one or more nozzles in the ceiling of the server room in gas form. A system such as this can put out most classes of fires in seconds. This type of product does not do damage to equipment and can be used safely when people are present. However, most of these systems also employ a *very* loud alarm that tells all personnel to leave the server room; it's usually so loud and abrasive that you are compelled to leave! It is wise to run through fire suppression alarm tests and fire drills, ensuring that the alarm will sound when necessary and that IT personnel know what to do when the alarm sounds, namely, leave. In some cases, these systems will shut the door automatically after a certain timeout. In these cases, procedures should be written out specifying what to do if a fire occurs. Drilling is of utmost importance in these environments to make certain

that everyone knows to leave the server room quickly if a fire occurs. Again, after drills have been completed, the appropriate IT personnel should simulate disaster recovery procedures, if necessary. If the system was installed properly and does its job, this simulation should be minimal.

## HVAC

HVAC, or heating, ventilating, and air conditioning, is important for server rooms, data centers, and other technology-oriented areas of your building. Servers run hot—their CPUs can make the temperature inside the case skyrocket. This heat needs to be dissipated and exhausted outside the case. All the heat from servers and other networking equipment is enough to make your server room fry!

To alleviate the situation, organizations install a heavy-duty air-conditioning system used solely for the server room. Often, the system also includes a humidity control. As we know, static electricity is our enemy. By increasing humidity, we decrease the buildup of static electricity and the chance of ESD. Also, this can enable us to keep our equipment from getting too humid, which can also cause failure. It is important to have this system on its own dedicated circuit that is rated properly.

Because most AC systems use refrigerant, it is important to locate the device and any pipes away from where servers and other equipment will be situated, or use a pipeless system. The controls for this system should be within the server room, perhaps protected by a key code. This way, only authorized IT personnel (who have access to the server room) can change the temperature or humidity. This control can also be hooked up to the door access system or other monitoring systems to log who made changes and when.

Another way to improve the heat situation is to circulate the air, and one smart way to do this is to install **hot and cold aisles**. To illustrate this concept, imagine that you had several rows of servers inside cabinets, all of which are resting on a raised floor. You would set up the fronts of the cabinets of each row to face each other, forming a cold aisle (the row you would normally walk down to access the servers). The cold air is pumped into this aisle from the raised floor. Since most servers and other IT equipment use front-to-back heat dissipation, the heat should be exhausted out behind the row. That's where the hot aisle is, along with network cables, power cables, and so on. The hot air is exhausted through the raised floor or through exhaust ducts in the ceiling.

A heating system is rarely needed in a server room, unless the organization's building is in the coldest of environments. This is due to the amount of heat that all the servers give off, and the fact that they usually run 24/7.

If there is a power failure that cannot be alleviated by use of a UPS and/or backup generator, you might opt to shut down all but the most necessary of systems

temporarily. Some organizations enforce this by way of a written policy. To help monitor HVAC systems and their power consumption, industrial control systems (ICSs) such as the **supervisory control and data acquisition (SCADA)** computer-controlled system will be used. A system such as SCADA combines hardware monitoring devices (pressure gauges, electrodes, remote terminal units that connect to sensors) with software that is run on an admin's (or building management employee's) workstation, allowing the admin to monitor the HVAC system in real time. There could also be a human-machine interface (HMI) that displays SCADA animations on a separate screen in a strategic place in the building. SCADA systems are vulnerable to viruses (such as Stuxnet) that can be used to access design files. To protect against this, the workstation that runs the software portion of SCADA should have its AV software updated, and any separate physical interfaces, displays, and sensors should be secured and perhaps be placed within view of a CCTV system.

Aside from monitoring HVAC, heating and ventilation systems are usually beyond the knowledge of the IT people, and any maintenance or repair of such systems should be directed to qualified professionals. Sometimes, the building management is responsible for such systems, but more than likely the organization is responsible for the installation, repair, and maintenance. What's important to know for the exam is that HVAC systems address the need for *availability* of data.

## Shielding

We have already established that EMI and RFI can corrupt legitimate signals and can possibly create unwelcome emanations. Shielding can help to prevent these problems. Although these have been briefly discussed previously, let's get into a little more detail with a few examples:

- **Shielded twisted-pair (STP) cable:** By using STP cable, you employ a shield around the wires inside the cable, reducing the levels of interference on the cable segment. This can help with computers suffering from intermittent data loss.
- **HVAC shielding:** By installing a shield around air conditioners and other similar equipment, you end up shielding them, and thereby keep EMI generated by that equipment inside the shield.
- **Faraday cage:** There are several types of Faraday cages. Screened cables such as coaxial cables for TV are basic examples. Booster bags lined with aluminum foil would be another example. But the term Faraday cage is usually applied to an entire room. If an entire room is shielded, electromagnetic energy cannot pass through the walls in either direction. So, if a person attempts to use a cell phone inside the cage, it will not function properly, because the signal cannot go beyond the cage walls; the cell phone cannot acquire a signal from a cell

phone tower. More important, devices such as cell phones, motors, and wireless access points that create electromagnetic fields and are outside the cage cannot disrupt electromagnetic-sensitive devices that reside inside the cage.

By using shielding effectively, you can limit just about any type of interference. Some server rooms are shielded entirely to stop any type of wireless transmissions from entering or exiting the room. This can be an expensive proposition and is more common in data centers and advanced technology computer rooms. The pinnacle of shielding technology and research is TEMPEST, which, according to some organizations, stands for Transient ElectroMagnetic Pulse Emanations Standard, though the U.S. government has denied that the word is an acronym at all. The TEMPEST standards (as defined by the U.S. government) deal with the studies into compromising emissions, which are broken down into different levels according to particular environments and strictness of shielding necessary to those environments. Because computers and monitors give off electromagnetic radiation, there is a chance, if a hacker uses the proper antenna, that information could be recorded. The TEMPEST standards govern the limiting of EM radiation, reducing the chance of the leakage of data. A TEMPEST-certified building can prevent wireless devices from being hacked by war-driving attacks and other similar wireless attacks.

If only it were so easy to shield people from the con: from what we call social engineering.

## Social Engineering

Let's discuss a low note in our society. Because that is what social engineering is—a low form of behavior, but an effective one. It is estimated that 1 out of 10 people is conned every year through social engineering, and as many as half of them don't even know it has occurred.

We mentioned in Chapter 1, "Introduction to Security," that *social engineering* is the act of manipulating users into revealing confidential information or performing other actions detrimental to the user. Examples of social engineering are common in everyday life. A basic example would be a person asking for your username and password over the phone; often the person uses flattery to gain information. Malicious people use various forms of social engineering in an attempt to steal whatever you have of value: your money, information, identity, confidential company data, or IT equipment. Social engineering experts use techniques and principles such as the following:

- Authority
- Intimidation
- Bold impersonation

- Urgency, scarcity, and even emergency
- The grooming of trust/familiarity/liking
- Persistence and patience
- Relating to the user: using company jargon, consensus, and social facts and proof
- Embedding of questions within conversations

They also use tools such as social networking sites and P2P software to obtain information disclosure either directly or through data aggregation. The main reason that social engineering succeeds is due to a lack of user awareness. But social engineering can also be effective in environments in which the IT personnel have little training, and in public areas, for example, public buildings with shared office space. Let's discuss some of the more common types of social engineering.

## Pretexting

**Pretexting** is when a person invents a scenario, or pretext, in the hope of persuading a victim to divulge information. Preparation and some prior information are often needed before attempting a pretext; impersonation is often a key element. By impersonating the appropriate personnel or third-party entities, a person performing a pretext hopes to obtain records about an organization, its data, and its personnel. IT people and employees should always be on the lookout for impersonators and always ask for identification. If there is any doubt, the issue should be escalated to your supervisor and/or a call should be made to the authorities.

## Malicious Insider

The malicious insider is one of the most insidious threats. Instead of impersonating personnel as is done in pretexting, the person actually *becomes* personnel! This attack is often used as part of a corporate espionage plan. Think that all IT techs are 100% honorable? In high-tech, you will find an assortment of atrocities, including the malicious insider threat. The insider might have been sent by a competing organization to obtain a job/consulting position with a certain company, or perhaps is approached by the competing organization while already working for the company that is the target. It is often initiated by organizations from another country. Once the insider is situated, that person can easily get access to secure data, PII, financials, engineering plans, and so on, and pass them on to the infiltrating organization. Of course, the penalties for this are high, but the potential rewards can be quite enticing to the properly “motivated” individual. Companies will therefore often run thorough background checks and credit checks and have human resources

go through an entire set of psychological questions. Then, when a person is hired, there is a sort of trial period where the person is allowed very little access to secure data and secure environments.

Now, a malicious insider doesn't necessarily have to be a person. It could be a device or bug that was inserted into the organization by a person using social engineering skills. For example, rogue PIN pad devices, audio and video sensors (bugs), keyloggers, and so on. This requires physical access to the building in one way or another, so identification and authentication become of paramount importance.

Warning! As of the writing of this book, malicious insider threats are severely underappreciated by many organizations. They shouldn't be, because the malicious insider has the best chance of obtaining a desired result; a far better chance than the outsider. Think about it, if you wanted to steal 100,000 credit card numbers so that you could charge \$1 to each—making a fortune, but causing no great stress to the credit card holders—how would you do it? Would you attempt a whole lot of MITM attacks? Would you try to hack through the bank's firewall and IDS/IPS, tip-toe around the honeypot, and so on? Or would you attempt to get *inside*. The risk is greater, of course, for the person. It is much easier to get caught. But the potential for success outweighs the risk in comparison to trying to hack the system from the outside. The number of compromises to banks and chains of stores done in this manner is staggering. It really could be the number one thing to watch out for as of the writing of this book.

## Diversion Theft

**Diversion theft** is when a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location. This happens more often than you would think, and millions of dollars' worth of IT equipment is stolen in this manner every day. It is important that couriers and other shippers know exactly where they are supposed to be delivering items, and that they are given an organization contact name, number, and possibly security code in case there is any confusion.

## Phishing

**Phishing** is the attempt at fraudulently obtaining private information. A phisher usually masquerades as someone else, perhaps another entity. There are two main differences between phishing and pretexting. First, phishing is usually done by electronic communication, not in person. Second, little information about the target is necessary. A phisher may target thousands of individuals without much concern as to their background. An example of phishing would be an e-mail that requests verification of private information. The e-mail probably leads to a malicious website designed to lure people into a false sense of security to fraudulently obtain

information. The website often looks like a legitimate website. A common phishing technique is to pose as a vendor (such as an online retailer or domain registrar) and send the target e-mail confirmations of orders that they supposedly placed.

This is a triple-whammy. First, the orders are obviously fake; a person might say “Hey, wait! I didn’t place these orders!” and perhaps click the link(s) in the e-mail, leading the person to the false web page. Second, if a person thinks it’s a legitimate order (perhaps the person does many orders, and the fraudulent one looks like another legitimate one), the person might click a link to track the order, again leading to the bogus web page. Third, once at the web page, the person is asked to enter her credentials for her account (which then leads to credit card fraud and ID theft), and in addition to that the page might have Trojans and other malicious scripts that are delivered to the unsuspecting person on exit. Sheesh, talk about cyber-bullying!

Generally, no information about the target is necessary for a phishing attack. However, some “fishermen” actually target specific groups of people or even specific individuals. This is known as **spear phishing**. And when an attacker targets senior executives (CEOs, CFOs, etc.) it is known as **whaling**. Whaling attacks are much more detailed and require that the attacker know a good deal of information about the target (much of which is freely available on the Internet).

The concept of phishing is also accomplished by telephone. Phone phishing, known as **vishing**, works in the same manner as phishing but is initiated by a phone call (often using VoIP systems). The phone call often sounds like a prerecorded message from a legitimate institution (bank, online retailer, donation collector, and so on). The message asks the unsuspecting person for confidential information such as name, bank account numbers, codes, and so on; all under the guise of needing to verify information for the person’s protection. It’s really the opposite, of course, and many people are caught unawares by these types of scams every day. By using automated systems (such as the ones telemarketers use), vishing can be perpetuated on large groups of people with little effort.

**NOTE** A similar technique using automated systems is known as *war-dialing*. This is when a device (modem or other system) is used to scan a list of telephone numbers and dial them in search of computer systems and fax machines. The technique sifts out the phone numbers associated with voice lines, and the numbers associated with computers. It results in a list that can later be used by other attackers for various purposes.

Many different types of social engineering are often lumped into what is referred to as phishing, but actual phishing for private information is normally limited to e-mail and websites. To defend against this, a phishing filter or add-on should be installed and enabled on the web browser. Also, a person should be trained to realize that institutions will *not* call or e-mail requesting private information. If people are not sure, they should hang up the phone or simply delete the e-mail. A quick way to find out whether an e-mail is phishing for information is to hover over a link. You will see a URL domain name that is far different from that of the institution that the phisher is claiming to be, probably a URL located in a distant country. Many of these phishers are also probably engaging in spy-phishing: a combination of spyware and phishing that effectively makes use of spyware applications. A spyware application of this sort is downloaded to the target, which then enables additional phishing attempts that go beyond the initial phishing website.

## Hoaxes

A **hoax** is the attempt at deceiving people into believing something that is false. The differences between hoaxes and phishing can be quite gray. However, hoaxes can come in person, or through other means of communication, whereas phishing is generally relegated to e-communication and phone. Although phishing can occur at any time, and with the specific goal of obtaining private information, a hoax can often be perpetuated on holidays or other special days and could be carried out simply for fun. Regardless, they can use up valuable organization resources: e-mail replies, Internet bandwidth used, time spent, and so on. An example of a “harmless” hoax was Google’s supposed name change to “Topeka” on April Fools’ Day 2010. An example of a financially harmful hoax was the supposed assassination of Bill Gates on April Fools’ Day 2003. This hoax led to stock market fluctuations and loss of profit in Asia. Some companies place a time limit on jokes and hoaxes indicating that the affected person has become nonproductive; for example, 3% of the workday.

Pretexting, malicious insider attempts, diversion theft, phishing, and hoaxes are all known as *confidence tricks*, thus the term *con*, and are committed by “bunko” artists. However, there are even lower ways to get access to people’s information; these often are used with the previous methods. These include shoulder surfing, eavesdropping, dumpster diving, baiting, and piggybacking.

## Shoulder Surfing

**Shoulder surfing** is when a person uses direct observation to find out a target’s password, PIN, or other such authentication information. The simple resolution for this is for the user to shield the screen, keypad, or other authentication-requesting devices. A more aggressive approach is to courteously ask the assumed shoulder surfer to move along. Also, private information should never be left on a desk or out

in the open. Computers should be locked or logged off when the user is not in the immediate area. Shoulder surfing and the following two sections are examples of no-tech hacking.

### Eavesdropping

**Eavesdropping** is when a person uses direct observation to “listen” in to a conversation. This could be a person hiding around the corner or a person tapping into a phone conversation. Soundproof rooms are often employed to stop eavesdropping, and encrypted phone sessions can also be implemented.

### Dumpster Diving

**Dumpster diving** is when a person literally scavenges for private information in garbage and recycling containers. Any sensitive documents should be stored in a safe place as long as possible. When they are no longer necessary, they should be shredded. (Some organizations incinerate their documents.) Information might be found not only on paper, but also on hard drives or removable media. Proper recycling and/or destruction of hard drives is covered later in this chapter.

### Baiting

**Baiting** is when a malicious individual leaves malware-infected removable media such as a USB drive or optical disc lying around in plain view. It might have an interesting logo or distinctive look about it. When a person takes it and connects it to his computer, the malware infects the computer and attempts to take control of it and/or the network the computer is a member of.

### Piggybacking/Tailgating

**Piggybacking** is when an unauthorized person tags along with an authorized person to gain entry to a restricted area—usually with the person’s consent. **Tailgating** is essentially the same with one difference: it is usually without the authorized person’s consent. Both of these can be defeated through the use of mantraps. A **mantrap** is a small space that can usually only fit one person. It has two sets of interlocking doors; the first set must be closed before the other will open, creating a sort of waiting room where people are identified (and cannot escape!). This technique is often used in server rooms and data centers. Multifactor authentication is often used in conjunction with a mantrap. For example, using a proximity card and PIN at the first door, and biometric scan at the second. A mantrap is an example of a preventive security control. Turnstiles, double entry doors, and employing security guards are other less expensive (and less effective) solutions to the problem of piggybacking and tailgating and help address confidentiality in general.

## Summary of Social Engineering Types

Table 16-1 summarizes the various types of social engineering we have discussed in this section.

**Table 16-1** Summary of Social Engineering Types

**Key Topic**

| Type                     | Description                                                                                                                                                                                                               |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Pretexting</b>        | When a person invents a scenario, or pretext, in the hope of persuading a victim to divulge information.                                                                                                                  |
| Malicious insider threat | When a person works at an organization with the secret purpose of obtaining secret information, financial information, design work, and PII.                                                                              |
| <b>Diversion theft</b>   | When a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location.                                                                                                               |
| Phishing                 | The attempt at fraudulently obtaining private information, usually done electronically.<br><br>Vishing is done by phone.<br><br>Spear phishing targets specific individuals.<br><br>Whaling targets senior executives.    |
| <b>Hoax</b>              | The attempt at deceiving people into believing something that is false.                                                                                                                                                   |
| <b>Shoulder surfing</b>  | When a person uses direct observation to find out a target's password, PIN, or other such authentication information.                                                                                                     |
| <b>Eavesdropping</b>     | When a person uses direct observation to "listen" in to a conversation. This could be a person hiding around the corner or a person tapping into a phone conversation.                                                    |
| <b>Dumpster diving</b>   | When a person literally scavenges for private information in garbage and recycling containers.                                                                                                                            |
| <b>Baiting</b>           | When a malicious individual leaves malware-infected removable media such as a USB drive or optical disc lying around in plain view in the hopes that unknowing people will bring it back to their computer and access it. |
| Piggybacking/Tailgating  | When an unauthorized person tags along with an authorized person to gain entry to a restricted area.                                                                                                                      |

In some cases, social engineering is easier than other, more technical ways of hacking information. For example, if a malicious individual wanted a person's password, it might be a lot easier to trick the person into giving her password than to try to crack it.

## User Education and Awareness

User education and awareness training are the keys to helping reduce social engineering success. The following is a basic list of rules you can use when training employees:

- Never, under any circumstances, give out any authentication details such as passwords, PINs, company ID, and so on.
- Always shield keypads and screens when entering authentication information.
- Adhere to the organization's *clean desk policy*, which states that all documents, electronics, personally owned devices, and other items be put away (or locked away) when the user is not at his or her desk, or other work area.
- Always screen your e-mail and phone calls carefully and keep a log of events.
- Use encryption when possible to protect e-mails and phone calls.
- If there is any doubt as to the legitimacy of a person, e-mail, or phone call, document the situation and escalate it to your supervisor, security, or the authorities.
- Never pick up, and make use of, any unknown removable media.
- Always shred any sensitive information destined for the garbage or recycling.
- Always comply with company policy when it comes to data handling and disposal. For example, if a hard drive, USB flash drive, memory stick, or optical disc is no longer being used, make sure it is disposed of properly. If the user is not sure, contact the IT department or facilities department of the organization to find out if it should be recycled, or destroyed.
- Always track and expedite shipments.

When training employees, try to keep them interested; infuse some fun and examples. Use examples of social engineering so that your trainees can make the connection between actual social engineering methods and their defenses. Make them understand that social engineers don't care how powerful an organization's firewall is or how many armed guards the company has. They get past technology and other types of security by exploiting the weaknesses inherent in human nature.

The previous lists of social engineering methods and defenses are in no way finite. There are so many ways to con a person and so many ways to defend against the con. However, some of the best weapons against social engineering, aside from user education and awareness, are policies and procedures, and their constant analysis. The next two sections detail some policies and procedures designed to protect sensitive information.

## Legislative and Organizational Policies

There are myriad legislative laws and policies. For the Security+ exam, we are concerned only with a few that affect, and protect, the privacy of individuals. In this section, we cover those and some associated security standards.

More important for the Security+ exam are organizational policies. Organizations usually define policies that concern how data is classified, expected employee behavior, and how to dispose of IT equipment that is no longer needed. These policies begin with a statement or goal that is usually short, to the point, and open-ended. They are normally written in clear language that can be understood by most everyone. They are followed by procedures (or guidelines) that detail how the policy will be implemented.

Table 16-2 shows an example of a basic policy and corresponding procedure.

**Table 16-2** Example of a Company Policy

| Policy                                                                                 | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Employees will identify themselves in a minimum of two ways when entering the complex. | <ol style="list-style-type: none"> <li>When employees enter the complex, they will first enter a guard room. This will begin the authentication process.</li> <li>In the guard room, they must prove their identification in two ways:           <ul style="list-style-type: none"> <li>By showing their ID badge to the on-duty guard.</li> <li>By being visible to the guard so that the guard can compare their likeness to the ID badge's photo. The head of the employee should not be obstructed by hats, sunglasses, and so on. In essence, the employee should look similar to the ID photo. If the employee's appearance changes for any reason, that person should contact human resources for a new ID badge.</li> </ul> <small>* If guards cannot identify the "employee," they will contact the employee's supervisor, human resources, or security in an attempt to confirm the person's identity. If the employee is not confirmed, they will be escorted out of the building by security.</small> </li> <li>After the guard has acknowledged the identification, employees will swipe their ID badge against the door scanner to complete the authentication process and gain access to the complex.</li> </ol> |

Keep in mind that this is just a basic example; technical documentation specialists will tailor the wording to fit the feel of the organization. Plus, the procedure will be different depending on the

size and resources of the organization and the type of authentication scheme used, which could be more or less complex. However, the *policy* (which is fairly common) is written in such a way as to be open-ended, allowing for the *procedure* to change over time. We talk about many different policies as they relate to the Security+ exam in this section.

## Data Sensitivity and Classification of Information

Sensitive data is information that can result in a loss of security, or loss of advantage to a company, if accessed by unauthorized persons. Often, information is broken down into two groups: classified (which requires some level of security clearance) and nonclassified.

ISO/IEC 27002:2005 (which revises the older ISO/IEC 17799:2005) is a security standard that among other things can aid companies in classifying their data. Although you don't need to know the contents of that document for the Security+ exam, you should have a basic idea of how to classify information. For example, classification of data can be broken down, as shown in Table 16-3.

**Table 16-3** Example of Data Sensitivity Classifications

| Class                    | Description                                                                                                                                                           |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Public information       | Information available to anyone. Also referred to as unclassified or nonclassified.                                                                                   |
| Internal information     | Used internally by a company, but if it becomes public, no critical consequences result. This, and the next three levels, is known as <i>private</i> information.     |
| Confidential information | Information that can cause financial and operational loss to the company.                                                                                             |
| Secret information       | Data that should never become public and is critical to the company.                                                                                                  |
| Top secret information   | The highest sensitivity of data; few people should have access, and security clearance may be necessary. Information is broken into sections on a need-to-know basis. |

In this example, loss of public and internal information probably won't affect the company very much. However, unauthorized access, misuse, modification, or loss of confidential, secret, or top secret data can affect users' privacy, trade secrets, financials, and the general security of the company. By classifying data and enforcing policies that govern who has access to what information, a company can limit its exposure to security threats.

Different organizations will classify data in various ways, but they will usually be similar to Table 16-3. For example, you might also see the high, medium, and low

classifications. Or, for instance, Red Hat Linux uses the Top Secret, Secret, and Confidential classifications (just as in Table 16-3), but considers everything else simply unclassified. All of these types of interpretations of data classifications are implementations of mandatory access control (MAC) discussed in Chapter 10, “Access Control Methods and Models.” It’s the incorporation of these types of classifications that is a key element in the multilevel security of Trusted Operating Systems (TOSs). Trusted Operating Systems such as Red Hat, OS X 10.6 and higher, and HP-UX utilize multilevel security concepts such as these to meet government requirements.

Moving beyond government classification requirements, many companies need to be in compliance with specific *laws* when it comes to the disclosure of information. In the United States there are a few acts you should know about, as shown in Table 16-4. In addition, there are several bills in process that could be passed in the near future regarding data breach notification.

**Table 16-4** Acts Passed Concerning the Disclosure of Data and Personally Identifiable Information (PII)

**Key Topic**

| Act                                                 | Acronym | Description                                                                                                                                                                                                                                      |
|-----------------------------------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Privacy act of 1974                                 | n/a     | Establishes a code of fair information practice.<br>Governs the collection, use, and dissemination of personally identifiable information about persons’ records maintained by federal agencies.                                                 |
| Sarbanes-Oxley                                      | SOX     | Governs the disclosure of financial and accounting information. Enacted in 2002.                                                                                                                                                                 |
| Health Insurance Portability and Accountability Act | HIPAA   | Governs the disclosure and protection of health information. Enacted in 1996.                                                                                                                                                                    |
| Gramm-Leach-Bliley Act                              | GLB     | Enables commercial banks, investment banks, securities firms, and insurance companies to consolidate.<br>Protects against pretexting. Individuals need proper authority to gain access to nonpublic information such as Social Security numbers. |
| Help America Vote Act of 2002                       | HAVA    | Main goal was to replace punchcard and lever-based voting systems.<br>Governs the security, confidentiality, and integrity of personal information collected, stored, or otherwise used by various electronic and computer-based voting systems. |
| California SB 1386                                  | SB 1386 | Requires California businesses that store computerized personal information to immediately disclose breaches of security.<br>Enacted in 2003.                                                                                                    |

Many computer technicians have to deal with SOX and HIPAA at some point in their careers, and although these types of acts create a lot of paperwork and protocol, the expected result is that, in the long run, they will help companies protect their data and keep sensitive information private.

**NOTE** SOX sparked another concept known as governance, risk, and compliance (GRC), which deals with the continuous security monitoring of: overall management of information systems and control structures; risk management processes; and compliance with stated requirements, be they government related or otherwise. CA and IBM provide GRC software solutions.

## Personnel Security Policies

Most organizations have policies governing employees. The breadth and scope of these policies vary from organization to organization. For example, a small company might have a few pages defining how employees should behave (a code of ethics) and what to do in an emergency. Other larger organizations might go so far as to certify to a particular standard such as ISO 9001:2000 or ISO 9001:2008. This means that the organization will comply with a set of quality standards that is all-encompassing, covering all facets of the business. An organization would have to be examined and finally accredited by an accrediting certification body to state that it is ISO 9001:2000-certified. This is a rigorous process and is not for the average organization. For many companies, this would create too much documentation and would bog the company down in details and minutia.

We as IT people are more interested in policies that deal with the security of the infrastructure and its employees. As a security administrator, you might deal with procedural documentation specialists, technical documentation specialists, and even outside consultants. You should become familiar with policies and as many procedures as possible, focusing on policies that take security into account, but remember that actual work must take precedence!

Let's define a few types of policies that are common to organizations. We focus on the security aspect of these policies.

## Privacy Policies

The Privacy act of 1974 sets many standards when it comes to the security of personally identifiable information (PII). However, most organizations will go further and define their own privacy policy, which explains how users' identities and other

similar information will be secured. For example, if an organization has an Internet-based application that internal and external users access, the application will probably retain some of their information—possibly details of their identity. Not only should this information be secured, but the privacy policy should state in clear terms what data is allowed to be accessed, and by whom, as well as how the data will be retained and distributed (if at all). An organization might also enact a policy that governs the labeling of data to ensure that all employees understand what data they are handling, and to prevent the mishandling of confidential information. Before any systems administrators or other personnel gather information about these users, they should consult the privacy policy.

### Acceptable Use

Acceptable usage policies (AUPs) define the rules that restrict how a computer, network, or other system may be used. They state what users are, and are not, allowed to do when it comes to the technology infrastructure of an organization. Often, an AUP must be signed by the employees before they begin working on any systems. This protects the organization, but it also defines to employees exactly what they should, and should not, be working on. If a director asks a particular employee to repair a particular system that was outside the AUP parameters, the employee would know to refuse. If employees are found working on a system that is outside the scope of their work, and they signed an AUP, it is grounds for termination. As part of an AUP, employees enter into an agreement acknowledging they understand that the unauthorized sharing of data is prohibited. Also, employees should understand that they are not to take any information or equipment home without express permission from the various parties listed in the policy. This can sometimes be in conflict with a BYOD policy where users are permitted to bring their own devices into work and use them for work purposes. At that point, strong policies for data ownership need to be developed, identifying what portion of the data on a mobile device is owned by the organization, and what portion is owned by the employee. Any organizational data on a mobile device should be backed up.

### Change Management

**Change management** is a structured way of changing the state of a computer system, network, or IT procedure. The idea behind this is that change is necessary, but that an organization should adapt with change, and be knowledgeable of it. Any change that a person wants to make must be introduced to each of the heads of various departments that it might affect. They must approve the change before it goes into effect. Before this happens, department managers will most likely make recommendations and/or give stipulations. When the necessary people have signed off on

the change, it should be tested and then implemented. During implementation, it should be monitored and documented carefully.

Because there are so many interrelated parts and people in an IT infrastructure, it is sometimes difficult for the left hand to know what the right hand is doing, or has done in the past. For example, after a network analysis, a network engineer might think that an unused interface on a firewall doesn't necessarily need to exist anymore. But does he know this for sure? Who installed and configured the interface? When was it enabled? Was it ever used? Perhaps it is used only rarely by special customers making a connection to a DMZ; perhaps it is used with a honeynet; or maybe it is for future use or for testing purposes. It would be negligent for the network engineer to simply modify the firewall without at least asking around to find out whether the interface is necessary. More likely, there will be forms involved that require the network engineer to state the reason for change and have it signed by several other people before making the change. In general this will slow down progress, but in the long run it will help to cover the network engineer. People were warned, and as long as the correct people involved have signed off on the procedure or technical change, the network engineer shouldn't have to worry. In a larger organization that complies with various certifications such as ISO 9001:2000, it can be a complex task. IT people should have charts of personnel and department heads. There should also be current procedures in place that show who needs to be contacted in the case of a proposed change.

### **Separation of Duties/Job Rotation**

Separation of duties is when more than one person is required to complete a particular task or operation. This distributes control over a system, infrastructure, or particular task. Job rotation is one of the checks and balances that might be employed to enforce the proper separation of duties. It is when two or more employees switch roles at regular intervals. It is used to increase user insight and skill level, and to decrease the risk of fraud and other illegal activities. Both of these policies are enforced to increase the security of an organization by limiting the amount of control a person has over a situation and by increasing employees' knowledge of what other employees are doing. For more information on these and similar concepts, see Chapter 10.

### **Mandatory Vacations**

Some organizations require employees to take X number of consecutive days of vacation over the course of a year as part of their annual leave. For example, a company might require an IT director to take five consecutive days' vacation at least once per year to force another person into his role for that time period. Although a

company might state that this helps the person to rest and focus on his job, and incorporate job rotation, the underlying security concept is that it can help to stop any possible malicious activity that might occur such as fraud, sabotage, embezzlement, and so on. Because IT people are smart, and often access the network remotely in a somewhat unobserved fashion, auditing becomes very important.

## Onboarding and Offboarding

**Onboarding** is when a new employee is added to an organization, and to its identity and access management system. It incorporates training, formal meetings, lectures, and human resources employee handbooks and videos. It can also be implemented when a person changes roles within an organization. It is known as a socialization technique used to ultimately provide better job performance and higher job satisfaction. Onboarding is associated with federated identity management discussed in Chapter 10. It is also sometimes connected to an employee's *role* in the company, and therefore role-based access control (RBAC).

*Offboarding* is the converse, and correlates to procedurally removing an employee from a federated identity management system, restricting rights and permissions, and possibly debriefing the person. This happens when a person changes roles within an organization, or departs the organization altogether.

An organization will commonly work with business partners, but no business relationship lasts forever, and new ones are often developed. So, onboarding and offboarding can apply to business partners as well. The main concerns are access to data. In Chapter 5, "Network Design Elements," we discussed extranets and the community cloud, which are both commonly used technologies with business partners. These technologies allow an organization to carefully select which data the business partner has access to. As relationships with business partners are severed, a systematic audit of all shared data should be made, including the various types of connectivity, permissions, policies, and even physical access to data.

## Due Diligence

When it comes to information security, **due diligence** is ensuring that IT infrastructure risks are known and managed. An organization needs to spend time assessing risk and vulnerabilities and might state in a policy how it will give due diligence to certain areas of its infrastructure.

## Due Care

**Due care** is the mitigation action that an organization takes to defend against the risks that have been uncovered during due diligence.

## Due Process

**Due process** is the principle that an organization must respect and safeguard personnel's rights. This is to protect the employee from the state and from frivolous lawsuits.

## User Education and Awareness Training

With so many possible organizational policies, employees need to be trained to at least get a basic understanding of them. Certain departments of an organization require more training than others. For example, Human Resources personnel need to understand many facets of the business and their corresponding policies, especially policies that affect personnel. HR people should be thoroughly trained in guidelines and enforcement. Sometimes the HR people train management and other employees on the various policies that those trainees are expected to enforce. In other cases, the trainer would be an executive assistant or outside consultant.

Security awareness training is an ongoing process. Different organizations have varying types of security awareness training, and employees with different roles in the organization receive different types of training. This type of training is often coupled with the signing of a user agreement. The user, when signing this, accepts and acknowledges specific rules of conduct, rules of behavior, and possibly the non-disclosure of any training (known as a nondisclosure agreement, or NDA).

All employees should be trained on **personally identifiable information (PII)**. This is information used to uniquely identify, contact, or locate a person. This type of information could be a name, birthday, Social Security number, biometric information, and so on. Employees should know what identifies them to the organization and how to keep that information secret and safe from outsiders. Another key element of user education is the dissemination of the password policy. They should understand that passwords should be complex, and know the complexity requirements. They should also understand never to give out their password or ask for another person's password to any resource.

IT personnel should be trained on what to do in the case of account changes—for example, temporarily disabling the account of employees when they take a leave of absence or disabling the account (or deleting it, less common) of an employee who has been terminated. All IT personnel should be fluent in the organization's password policy, lockout policy, and other user-related policies so that they can explain them to any other employees.

Some users might need to take additional privacy training, HIPAA training, or other types of security awareness training depending on the type of organization they work for. This user training might take the form of role-based training, where the

instructors and trainees act out the roles they might play, such as network administrator, security analyst, and so on. Instructors will often devise their training to take advantage of learning management systems and training metrics so that they can gauge the effectiveness of the training, validate compliance with policies, and analyze the security posture of the trainees in general.

### Summary of Personnel Security Policies

Table 16-5 breaks down and summarizes the various policy types mentioned in this section.

**Table 16-5** Summary of Policy Types

**Key Topic**

| Type                 | Description                                                                                                                                                                      |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Acceptable use       | Policy that defines the rules that restrict how a computer, network, or other system may be used.                                                                                |
| Change management    | A structured way of changing the state of a computer system, network, or IT procedure.                                                                                           |
| Separation of duties | When more than one person is required to complete a task.                                                                                                                        |
| Job rotation         | When a particular task is rotated among a group of employees.                                                                                                                    |
| Mandatory vacations  | When an organization requires employees to take X number of consecutive days' vacation over the course of a year as part of their annual leave.                                  |
| Onboarding           | When a new employee is added to an organization, and to its identity and access management system. It is associated with user training, federated identity management, and RBAC. |
| Due diligence        | Ensuring that IT infrastructure risks are known and managed.                                                                                                                     |
| Due care             | The mitigation action that an organization takes to defend against the risks that have been uncovered during due diligence.                                                      |
| Due process          | The principle that an organization must respect and safeguard personnel's rights.                                                                                                |

### How to Deal with Vendors

Before we begin, I should mention that the following information is *not* intended as legal advice. Before signing any contracts, an organization should strongly consider consulting with an attorney.

An organization often has in-depth policies concerning vendors. I can't tell you how many times I've seen issues occur because the level of agreement between the

organization and the vendor was not clearly defined. A proper **service-level agreement (SLA)** that is analyzed by the organization carefully before signing can be helpful. A basic service contract is usually not enough; a service contract with an SLA will have a section within it that formally and clearly defines exactly what a vendor is responsible for and what the organization is responsible for—a demarcation point so to speak. It might also define performance expectations and what the vendor will do if a failure of service occurs, timeframes for repair, backup plans, and so on. To benefit the organization, these will usually be legally binding and not informal. Due to this, it would benefit the organization to scrutinize the SLA before signing, and an organization's attorney should be involved in that process.

For instance, a company might use an ISP for its T3 connection. The customer will want to know what kind of fault-tolerant methods are on hand at the ISP and what kind of uptime they should expect, which should be monitored by a network admin. The SLA might have some sort of guarantee of measurable service that can be clearly defined; perhaps a minimum level of service and a target level of service. Before signing an SLA such as this, it is recommended that an attorney, the IT director, and other organizational management review the document carefully and make sure that it covers all the points required by the organization.

An SLA that requires products and services over and over again is known as a **blanket purchase agreement (BPA)**—similar to a blanket order. These are common in government contracts, but some organizations use them also. One thing to make sure is that there is some type of ending for the contract length. Some less than reputable cloud providers will design open-ended BPAs—try to avoid these. Sometimes, multiple government agencies will enter into a **memorandum of understanding (MoU)**, or a letter of intent, in regard to a BPA; it could be that two agencies have a sort of convergence when it comes to ordering services.

**NOTE** An SLA is also referred to as an information service agreement (ISA), especially when dealing with cloud-based services such as IaaS and PaaS.

## How to Dispose of Computers and Other IT Equipment Securely

Organizations might opt to recycle computers and other equipment or donate them. Rarely do organizations throw away equipment. It might be illegal to do so depending on your location and depending on what IT equipment is to be thrown away. The first thing an IT person should do is consult the organization's policy regarding computer disposal, and if necessary, consult local municipal guidelines.

A basic example of a policy and procedure that an organization enforces might look like the following:

Policy: Recycle or donate IT equipment that has been determined to be outdated and nonproductive to the company.

**Step 1.** Define the equipment to be disposed of.

**Step 2.** Obtain temporary storage for the equipment.

**Step 3.** Have the appropriate personnel analyze the equipment.

- Verify whether the equipment is outdated and whether it can be used somewhere else in the organization.
- If a device can be used in another area of the organization, it should be reformatted, flashed, or otherwise reset back to the original default, and then transported to its new location.
- If a device cannot be reused in the organization, move to Step 4.

**Step 4.** Sanitize the devices or computers.

- Check for any removable media inside, or connected to, the computer. These should be analyzed and recycled within the organization if possible.
- Remove any RAM, label it, and store it.
- Remove the hard drive, sanitize it, and store it. If necessary based on organizational policies, pulverize or otherwise destroy the device.
- Reset any BIOS or other passwords to the default setting.

**Step 5.** Recycle or donate items as necessary.

Again, this is just an example of a basic recycle policy and procedure, but it gives you an idea of the type of method an organization might employ to best make use of its IT equipment and to organize the entire recycling/donating process.

In Step 4, the policy specified to sanitize the hard drive, sanitizing the hard drive is a common way of removing data, but not the only one. The way data is removed might vary depending on its proposed final destination. Data removal is the most important element of computer recycling. Proper data removal goes far beyond file deletion or the formatting of digital media. The problem with file deletion/formatting is data remanence, or the residue, that is left behind, from which re-creation of files can be accomplished with the use of software such as SpinRite or other data recovery applications. Companies typically employ one of three options when met with the prospect of data removal:

- **Clearing:** This is the removal of data with a certain amount of assurance that it cannot be reconstructed. The data is actually recoverable with special techniques. In this case, the media is recycled and used within the company again. The data wiping technique is used to clear data from media by overwriting new data to that media. In some cases, patterns of ones and zeros are written to the entire drive. Several software programs are available to accomplish this.
- **Purging:** Also known as sanitizing, this is once again the removal of data, but this time, it's done in such a way so that it cannot be reconstructed by any known technique; in this case the media is released outside the company. Special bit-level erasure software (or other means) is employed to completely destroy all data on the media. It is also possible to degauss the disk, which renders the data unreadable but might also cause physical damage to the drive.
- **Destruction:** This is when the storage media is physically destroyed through pulverizing, shredding, incineration, and so on. At this point, the media can be disposed of in accordance with municipal guidelines.

The type of data removal used will be dictated by the data stored on the drive. If there is no personally identifiable information, or other sensitive information, it might simply be cleared and released outside the company. But in many cases, organizations will specify purging of data if the drive is to leave the building. In cases where a drive previously contained confidential or top secret data, the drive will usually be destroyed.

## Incident Response Procedures

**Incident response** is a set of procedures that an investigator follows when examining a computer security incident. Incident response procedures are a part of computer security **incident management**, which can be defined as the monitoring and detection of security events on a computer network and the execution of proper responses to those security events.

However, often, IT employees of the organization discover the incident. Sometimes they act as the investigators also. It depends on the resources and budget of the organization. So it is important for the IT personnel to be well briefed on policies regarding the reporting and disclosure of incidents.

Don't confuse an incident with an event. An example of a single event might be a single stop error on a Windows computer. In many cases, the blue screen of death (BSOD) won't occur again, and regardless, it has been logged in case that it does. The event should be monitored, but that is about all. An example of an incident would be when several DDoS attacks are launched at an organization's web servers over the course of a work day. This will require an incident response team that

might include the security administrator, IT or senior management, and possibly a liaison to the public and local municipality.

The seven main steps of the incident response process can be summed up simply as the following:

**Key Topic**

- Step 1. Identification**—The recognition of whether an event that occurs should be classified as an incident.
- Step 2. Containment**—Isolating the problem. For example, if it is a network attack, the attacker should be extradited to a padded cell. Or if only one server has been affected so far by a worm or virus, it should be physically disconnected from the network. The same goes for devices—they should be removed from the network or from a connected computer if the incident concerns them.
- Step 3. Evidence gathering**—Evidence of the incident is gathered by security professionals in a way that preserves the evidence’s integrity.
- Step 4. Investigation**—Investigators within the organization and perhaps consultants ascertain exactly what happened and why. In this step, reporting of the facts is also performed.
- Step 5. Eradication**—Removal of the attack or threat, quarantine of the computer(s), device removal if necessary, and other mitigation techniques covered previously in this book.
- Step 6. Recovery**—Retrieve data, repair systems, re-enable servers and networks, re-constitute server rooms and/or the IT environment, and so on. Damage and loss control comes into play here; it can be a very slow process to make sure that as much data is recovered as possible.
- Step 7. Documentation & Monitoring**—Document the process and make any changes to procedures and processes that are necessary for the future. Damage and loss should be calculated and that information should be shared with the accounting department of the organization. The affected systems should be monitored for any repercussions.

**NOTE** At any time during these steps, you might be required to notify your superior and/or escalate the problem to someone with more experience than you. That will depend on your organization’s rules and whether you encounter something that you don’t understand. It happens, and you need to be able to swallow your pride and escalate if necessary.

It all comes down to preparation. Consider a data breach, for example. An organization with no planning will take much longer to repair the problem and will have a hard time controlling the damage and loss. But an organization with a well-planned incident response procedure (in advance), a strong security posture, and a knowledgeable CISO will be able to limit the damage (to data and to the company reputation) by: quickly discovering the breach; having an internal response team ready to take action; obtaining forensics data quickly; and beginning a seamless notification process and inquiry response plan.

Of course, an incident response policy can be much more in depth, specify exact procedures, and vary in content from organization to organization. To find out more about common practices and standards for incident response, see the ISO/IEC 27002:2005 standard. Due to the length and breadth of the information, there is far too much to cover in this book. (I supplied a link to this in the “View Recommended Resources” section on the disc, or you can search the Internet for one of several documents that whittles down the content to a more manageable size—but still pretty hefty reading material!) The Security+ exam expects you to know only the basics of incident response.

The seven-step process listed previously is a typical example; however, an organization might have more or fewer steps, and their procedures might vary. An organization’s typical incident response policy and procedures generally detail the following:

- **Initial incident management process:** This includes who first found the problem, tickets, and various levels of change controls. It also defines **first responders** (also known as first-level responders) who perform preliminary analysis of the incident data and determine whether the incident is actually an incident or just an event, and the criticality of the incident.
- **Emergency response detail:** If the incident is deemed to be an emergency, this details how the event is escalated to an emergency incident. It also specifies a coordinator of the incident, how and when the incident team will meet, lock-down procedures, containment of the incident, repair and test of systems, and further investigation procedures to find the culprit (if there is one).
- **Collection and preservation of evidence:** Sherlock Holmes based his investigations on traditional clues such as footprints, fingerprints, and cigar ash. Analogous to this, a security investigator needs to collect log files, alerts, captured packets, and so on, and preserve the integrity of this information by retaining forensic images of data. Modification of any information or image files during the investigative process will most likely void its validity in a court of law. One way to preserve evidence properly is to establish a **chain of custody**—the chronological documentation or paper trail of evidence. This is something that should be set up immediately at the start of an investigation; it

documents who had custody of evidence all the way up to litigation or a court trial (if necessary) and verifies that the evidence has not been modified. An incident response policy lists proper procedures when it comes to the procurement of evidence.

- **Damage and loss control:** The incident response policy also covers how to stop the spread of damage to other IT systems and how to minimize or completely curtail loss of data.

But a lot of this is really just posturing. The toughest part of the job is figuring out what happened during an incident, and how it happened. That means hardcore forensics. This might be taken care of internally, but more often than not it will be a job for third-party vendors—forensics consultants and specialists.

The incident response policy might define how computer forensics (or digital forensics) should be carried out. It might detail how information is to be deciphered from a hard disk or other device. Often, it dictates the use of hard drive hashing so that computer forensics experts can identify tampering by outside entities. It might also specify a list of rules to follow when investigating what an attacker did. For example, forensics investigators verify the integrity of data to ensure that it has not been tampered with. It is important that computer forensics investigations are carried out properly in case legal action is taken. Policies detailing the proper collection and preservation of evidence can be of assistance when this is the case.

There are some basic forensic procedures that can be utilized within the incident response process. Most commonly, these are applied during Steps 3, 4, and 7 listed previously. Some of these include:

- **Capture and hash system images:** If a computer's data is to be used as evidence, the entire drive should be imaged (copied) before it is investigated. The imaging process should be secured and logged, and the image itself should be hashed; the hashing process should take place before and after the image is created. This will protect the image from tampering and prove the integrity of the image. Generally, imaging is done to the hard drive of the computer, but if the computer is on, memory and other components/media can also be imaged. It is important to consider order of volatility (OOV) when imaging any media, as discussed further down in this list. LiveCDs and LiveDVDs are commonly used to take an image of a computer. These are operating systems that run directly off of an optical disc. Because they are outside of the computer's regular OS environment, they are excellent options if you don't want to disturb the system. Examples of these include Knoppix and BackTrack.
- **Analyze data with software tools:** The data files may have to be analyzed carefully. Forensic toolkits (FTKs) can be invaluable for this. Examples

**Key Topic**

include Guidance Software’s EnCase, AccessData’s Forensic Toolkit, The Sleuth Kit (open source), Disk Investigator (freeware), and Defiant Technologies’ DiskDigger, to name a few.

- **Capture screenshots:** A computer that is being investigated might be compromised. Therefore, it is usually not wise to use screen capturing software that is installed on the affected computer. Instead, take actual photos of the various screens you wish to capture using a camera.
- **Review network traffic captures and logs:** As part of an investigation, an analyst will review network captures made with network sniffing programs such as Wireshark or Network Monitor: these are covered in depth in Chapters 11, “Vulnerability and Risk Assessment,” and 12, “Monitoring and Auditing.” Logs should also be preserved, hashed, and stored, including firewall logs, server logs, and router/switch logs. Various network device logs are discussed in Chapters 5 through 8.
- **Capture video:** Any video surveillance equipment that recorded an incident will need to be analyzed. Before doing so, recorded video should be captured to a computer or to an external media device. Once again, the process should be secured and logged so that a person cannot claim that the evidence has been tampered with. Different municipalities, governments, and organizations will have varying policies on how this is to be accomplished. A forensic analyst should be well versed on these policies before responding to an incident. Keep in mind that the time stamp for video might be incorrect. When this happens, the investigator should establish what “real” time is, using a legitimate time server. The “real” time should be compared to the time stamp of the video. The difference between the two is known as the *record time offset*.
- **Consider the order of volatility (OOV):** OOV can be summarized as the life expectancy of various types of captured data during forensic analysis. For example, CD-ROM discs can be preserved for tens of years, and floppy disks and tape backup can usually be preserved for years. Hard drives can be expected to last from 1 to 5 years. However, information stored in memory, cache, or CPU registers, and any running processes, only last for seconds (or even milliseconds or nanoseconds). The OOV of media and captured data should be considered when gathering evidence that will be used in a court of law.
- **Take statements from witnesses:** Witnesses are people who were present during an event and were cognizant of what happened during the event. They are used during court cases and investigations to describe what they saw, heard, smelled, felt, and so on. A witness can corroborate evidence that was gathered from video, computer logs, captures, and other technical evidence.
- **Track man hours and expenses:** Every action that is taken by the investigators of an incident response team should be logged and documented so as to

act as a proper audit trail. Investigators normally need to sign in before being allowed access to an affected area or computer. The total man hours, sign in and sign out times, as well as any expenses incurred should be thoroughly documented. Man hours might be tracked through a computer system. For more information on the login of users, and policies governing how and when they can log in, see Chapter 10.

When an examiner collects digital evidence, he or she should abide by *best practices*. One best practice is to document everything (a fairly simple concept that we have mentioned so many times that you should now have documentation on the brain). But best practices can be more encompassing. For example, the following example procedure defines a best practice for preserving evidence (including live, volatile data in memory):

1. Photograph the computer and scene.
2. If the computer is off, *do not* turn it on. (Skip to #7.)
3. If the computer is on, photograph the screen.
4. Collect live data from the RAM image. Use a tool such as Live Response.
5. Collect other live data such as logged-on users, the network connection state, and so on.
6. Only if the drive is encrypted, collect a logical image of the drive. Special software will be required.
7. Unplug the power cord from the computer. If the computer is a laptop or mobile device and it does not shut down properly, then remove the battery.
8. Diagram and label all cords.
9. Document all device model numbers and serial numbers that are visible.
10. Disconnect all cords and devices.
11. Collect an image of the hard drive using a hardware imager. Or, if a hardware imager is not available, use one of the software tools mentioned previously in this section. However, if that is the case, this step should be moved to earlier in the sequence (before all cables were disconnected). Next, hash the image.
12. Package all components using antistatic evidence bags.
13. Collect additional storage media and store it using antistatic evidence bags.
14. Keep all media away from magnets, radio transmitters, and so on.
15. Collect instruction manuals, documentation, and notes.
16. Document all steps performed during the seizure.

That is a general procedure. But it will vary depending on the scene, the tools you have at your disposal, and whether or not the computer was on (or sleeping) when you arrived.

Now, in general, I know what you are thinking: With all these policies and procedures in place, how does anything ever get done?! And how do incidents get analyzed quickly enough so as not to become a disaster? Well, training is important. Personnel need to be trained quickly and efficiently without getting too much into the minutia of things. They also need to be trained to *take action* quickly. By narrowing down an organization's policies to just what an employee needs to know, you can create a short but sweet list of key points for the employee to remember. *Need-to-know* is in itself an important security concept in companies. It is designed as much to hide information from people as it is to prevent information overload. For example, if a person were choking, the information you want to know is how to perform the Heimlich Maneuver; you don't care why a person chokes, what the person ate for breakfast, or how specifically the maneuver works. This concept helps when there is an event or incident; the employees don't need to sift through wads of policies to find the right action to take, because they are on a need-to-know basis and will quickly execute what they have been trained to do. Need-to-know also comes into play when confidential or top secret information is involved. In classified environments, top secret information is divided into pieces, only some of which particular people have access to. This compartmentalizing of information not only helps to secure data, but increases productivity and efficiency in the workforce.

## Chapter Summary

So that wraps up this chapter about policies, procedures, and people. It was a bit helter-skelter as far as the listing of content, but in a way, all the concepts are intertwined. When you are involved in any type of policing, investigative work, or other security-based IT work, consider the safety of personnel and data and the integrity of organizational information.

Environmental controls are security controls that are put in place to protect employees, servers, and the organization's data. They include fire extinguishers, sprinkler systems, special hazard systems (such as FM-200), hot and cold aisles, SCADA-based systems, and shielding. These are physical and easily understood. The security of these depends on physical keys, proximity and smart card systems, video surveillance, security guards, alarms, and so forth.

However, they can all be exploited by a smart person and some social engineering skills—and this is less tangible, and not as easily understood, or as easily prevented. People that employ social engineering rely on authority, intimidation, impersonation, trust, persistence, and a lot of patience. This enables them to perform cons

such as pretexting and hoaxes, and steal information through phishing, baiting, shoulder surfing, eavesdropping, and other methods. While this whole book is full of ways to prevent the con artist from obtaining data, secrets, and PII, it is the user education and awareness that might be the best defense. Knowledge is power, but users need to be trained in an interesting manner in order to effectively stop the threat of social engineering.

For an organization to realize a high level of security, the implementation of policies and procedures is highly recommended, and in some cases may be mandatory. Data sensitivity can be classified to better define which users are allowed to access what data sets. Personnel policies such as privacy policies, acceptable use, change management, separation of duties, job rotation, succession planning, and onboarding are all very useful to an organization in that they help to identify exactly what a user is supposed to be doing—and not doing—and how the user will be trained and brought into the mold, so to speak.

Policies are also used to describe what happens to data when it is no longer needed, and what should be done with the media that holds the data; whether it is the clearing of data, the purging of data and other methods of sanitizing data, or the destruction of the media. This might be necessary at the end of a particular device's lifespan.

Perhaps the most important policy is the one that defines what an organization will do during an *incident*. One thing that we can easily forget to do is to try to learn from incidents—because they will happen at some point. Proper documentation can really drive home the idea of the *lesson learned*. It can help us to recall what the specific problem was and why it occurred, ultimately allowing us to define ways to prevent it from happening again.

It's all of these policies and procedures, and the people that implement them, that contribute to the overall security plan of an organization. All of the technical know-how and the assessments and analysis that we discussed throughout the book can be leveraged by the power of well-defined organizational policies.

## 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 16-6 lists a reference of these key topics and the page number on which each is found.

**Table 16-6** Key Topics for Chapter 16

| <b>Key Topic Element</b> | <b>Description</b>                                    | <b>Page Number</b> |
|--------------------------|-------------------------------------------------------|--------------------|
| Bulleted list            | Fire extinguisher types                               | 612                |
| Table 16-1               | Summary of social engineering types                   | 623                |
| Table 16-4               | Acts passed concerning the disclosure of data and PII | 627                |
| Table 16-5               | Summary of policy types                               | 633                |
| Numbered list            | Seven steps of incident response process              | 637                |
| Bulleted list            | Forensic procedures                                   | 639                |

### Define Key Terms

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

fire suppression, wet pipe sprinkler system, pre-action sprinkler system, special hazard protection system, hot and cold aisles, supervisory control and data acquisition (SCADA), pretexting, diversion theft, phishing, spear phishing, whaling, vishing, hoax, shoulder surfing, eavesdropping, dumpster diving, baiting, piggybacking, tailgating, mantrap, change management, acceptable use, mandatory vacations, onboarding, due diligence, due care, due process, personally identifiable information (PII), service-level agreement (SLA), blanket purchase agreement (BPA), memorandum of understanding (MoU), incident response, incident management, first responders, chain of custody

### Review Questions

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

1. Which method would you use if you were disposing hard drives as part of a company computer sale?
  - A. Destruction
  - B. Purging
  - C. Clearing
  - D. Formatting

2. Which of these governs the disclosure of financial data?
  - A. SOX
  - B. HIPAA
  - C. GLB
  - D. Top secret
3. Jeff wants to employ a Faraday cage. What will this accomplish?
  - A. It will increase the level of wireless encryption.
  - B. It will reduce data emanations.
  - C. It will increase EMI.
  - D. It will decrease the level of wireless emanations.
4. If a fire occurs in the server room, which device is the best method to put it out?
  - A. Class A extinguisher
  - B. Class B extinguisher
  - C. Class C extinguisher
  - D. Class D extinguisher
5. What devices will not work in a Faraday cage? (Select the two best answers.)
  - A. Cell phones
  - B. Computers
  - C. Pagers
  - D. TDR
6. You go out the back door of your building and noticed someone looking through your company's trash. If this person were trying to acquire sensitive information, what would this attack be known as?
  - A. Browsing
  - B. Dumpster diving
  - C. Phishing
  - D. Hacking

7. You are told by your manager to keep evidence for later use at a court proceeding. Which of the following should you document?
  - A. Disaster recovery plan
  - B. Chain of custody
  - C. Key distribution center
  - D. Auditing
8. Which law protects your Social Security number and other pertinent information?
  - A. HIPAA
  - B. SOX
  - C. The National Security Agency
  - D. The Gramm-Leach-Bliley Act
9. User education can help to defend against which of the following? (Select the three best answers.)
  - A. Social engineering
  - B. Phishing
  - C. Rainbow tables
  - D. Dumpster diving
10. Which of these is an example of social engineering?
  - A. Asking for a username and password over the phone
  - B. Using someone else's unsecured wireless network
  - C. Hacking into a router
  - D. Virus
11. What is the most common reason that social engineering succeeds?
  - A. Lack of vulnerability testing
  - B. People sharing passwords
  - C. Lack of auditing
  - D. Lack of user awareness

- 12.** Which of the following is not one of the steps of the incident response process?
- A.** Eradication
  - B.** Recovery
  - C.** Containment
  - D.** Non-repudiation
- 13.** In which two environments would social engineering attacks be most effective? (Select the two best answers.)
- A.** Public building with shared office space
  - B.** Company with a dedicated IT staff
  - C.** Locked building
  - D.** Military facility
  - E.** An organization whose IT personnel have little training
- 14.** Of the following definitions, which would be an example of eavesdropping?
- A.** Overhearing parts of a conversation
  - B.** Monitoring network traffic
  - C.** Another person looking through your files
  - D.** A computer capturing information from a sender
- 15.** Your company expects its employees to behave in a certain way. How could a description of this behavior be documented?
- A.** Chain of custody
  - B.** Separation of duties
  - C.** Code of ethics
  - D.** Acceptable use policy
- 16.** You are a forensics investigator. What is the most important reason for you to verify the integrity of acquired data?
- A.** To ensure that the data has not been tampered with
  - B.** To ensure that a virus cannot be copied to the target media
  - C.** To ensure that the acquired data is up-to-date
  - D.** To ensure that the source data will fit on the target media

- 17.** Of the following, which type of fire suppression can prevent damage to computers and servers?
  - A.** Class A
  - B.** Water
  - C.** CO<sub>2</sub>
  - D.** ABC extinguishers
- 18.** You are the security administrator for your organization. You have just identified a malware incident. Of the following, what should be your first response?
  - A.** Containment
  - B.** Removal
  - C.** Recovery
  - D.** Monitoring
- 19.** A man pretending to be a data communications repair technician enters your building and states that there is networking trouble and he needs access to the server room. What is this an example of?
  - A.** Man-in-the-middle attack
  - B.** Virus
  - C.** Social engineering
  - D.** Chain of custody
- 20.** Employees are asked to sign a document that describes the methods of accessing a company's servers. Which of the following best describes this document?
  - A.** Acceptable use policy
  - B.** Chain of custody
  - C.** Incident response
  - D.** Privacy Act of 1974
- 21.** One of the developers for your company asks you what he should do before making a change to the code of a program's authentication. Which of the following processes should you instruct him to follow?
  - A.** Chain of custody
  - B.** Incident response
  - C.** Disclosure reporting
  - D.** Change management

- 22.** As a network administrator, one of your jobs is to deal with Internet service providers. You want to ensure that the provider guarantees end-to-end traffic performance. What is this known as?
- A.** SLA
  - B.** VPN
  - C.** DRP
  - D.** WPA
- 23.** Turnstiles, double entry doors, and security guards are all preventative measures for what kind of social engineering?
- A.** Dumpster diving
  - B.** Impersonation
  - C.** Piggybacking
  - D.** Eavesdropping
- 24.** When it comes to security policies, what should HR personnel be trained in?
- A.** Maintenance
  - B.** Monitoring
  - C.** Guidelines and enforcement
  - D.** Vulnerability assessment
- 25.** In a classified environment, clearance to top secret information that enables access to only certain pieces of information is known as what?
- A.** Separation of duties
  - B.** Chain of custody
  - C.** Non-repudiation
  - D.** Need to know
- 26.** In addition to bribery and forgery, which of the following are the most common techniques that attackers use to socially engineer people? (Select the two best answers.)
- A.** Flattery
  - B.** Assuming a position of authority
  - C.** Dumpster diving
  - D.** Whois search

- 27.** What is documentation that describes minimum expected behavior known as?
- A.** Need to know
  - B.** Acceptable usage
  - C.** Separation of duties
  - D.** Code of ethics
- 28.** You are the security administrator for your company. You have been informed by human resources that one of the employees in accounting has been terminated. What should you do?
- A.** Delete the user account.
  - B.** Speak to the employee's supervisor about the person's data.
  - C.** Disable the user account.
  - D.** Change the user's password.
- 29.** You need to protect your data center from unauthorized entry at all times. Which is the best type of physical security to implement?
- A.** Mantrap
  - B.** Video surveillance
  - C.** Nightly security guards
  - D.** 802.1X
- 30.** Which of the following targets specific people?
- A.** Pharming
  - B.** Phishing
  - C.** Vishing
  - D.** Spear phishing
- 31.** Why would you implement password masking?
- A.** To deter tailgating
  - B.** To deter shoulder surfing
  - C.** To deter impersonation
  - D.** To deter hoaxes

- 32.** Your organization already has a policy in place that bans flash drives. What other policy could you enact to reduce the possibility of data leakage?
- A.** Disallow the saving of data to a network share
  - B.** Enforce that all work files have to be password protected
  - C.** Disallow personal music devices
  - D.** Allow unencrypted HSMs
- 33.** Which of the following requires special handling and policies for data retention and distribution? (Select the two best answers.)
- A.** Phishing
  - B.** Personal electronic devices
  - C.** SOX
  - D.** PII
- 34.** A targeted e-mail attack is received by your organization's CFO. What is this an example of?
- A.** Vishing
  - B.** Phishing
  - C.** Whaling
  - D.** Spear phishing
- 35.** One of the accounting people is forced to change roles with another accounting person every three months. What is this an example of?
- A.** Least privilege
  - B.** Job rotation
  - C.** Mandatory vacation
  - D.** Separation of duties
- 36.** Which of the following environmental variables reduces the possibility of static discharges (ESD)?
- A.** Humidity
  - B.** Temperature
  - C.** EMI
  - D.** RFI

- 37.** You have been ordered to implement a secure shredding system as well as privacy screens. What two attacks is your organization attempting to mitigate?
- A.** Shoulder surfing
  - B.** Impersonation
  - C.** Phishing
  - D.** Dumpster diving
  - E.** Tailgating
- 38.** Your organization uses a third-party service provider for some of its systems and IT infrastructure. Your IT director wants to implement a governance, risk, and compliance (GRC) system that will oversee the third party and promises to provide overall security posture coverage. Which of the following is the most important activity that should be considered?
- A.** Baseline configuration
  - B.** SLA monitoring
  - C.** Security alerting and trending
  - D.** Continuous security monitoring
- 39.** Which of the following is the least volatile when performing incident response procedures?
- A.** RAM
  - B.** Registers
  - C.** Hard drive
  - D.** RAID cache
- 40.** Which of the following is a *best practice* when a mistake is made during a forensic examination?
- A.** The examiner should document the mistake and work around the problem.
  - B.** The examiner should attempt to hide the mistake during the examination.
  - C.** The examiner should disclose the mistake and assess another area of the disc.
  - D.** The examiner should verify the tools before, during, and after an examination.

## Answers and Explanations

1. **B.** Purging (or sanitizing) removes all the data from a hard drive so that it cannot be reconstructed by any known technique. If a hard drive were destroyed, it wouldn't be of much value at a company computer sale. Clearing is the removal of data with a certain amount of assurance that it cannot be reconstructed; this method is usually used when recycling the drive within the organization. Formatting is not nearly enough to actually remove data because it leaves data residue, which can be used to reconstruct data.
2. **A.** SOX, or Sarbanes-Oxley, governs the disclosure of financial and accounting data. HIPAA governs the disclosure and protection of health information. GLB, or the Gramm-Leach-Bliley Act of 1999, enables commercial banks, investment banks, securities firms, and insurance companies to consolidate. Top secret is a classification given to confidential data.
3. **B.** The Faraday cage will reduce data emanations. The cage is essentially an enclosure (of which there are various types) of conducting material that can block external electric fields and stop internal electric fields from leaving the cage, thus reducing or eliminating data emanations from such devices as cell phones.
4. **C.** When you think Class C, think copper. Extinguishers rated as Class C can suppress electrical fires, which are the most likely kind in a server room.
5. **A. and C.** Signals cannot emanate outside a Faraday cage. Therefore, cell phones and pagers will not work inside the Faraday cage.
6. **B.** Dumpster diving is when a person goes through a company's trash to find sensitive information about an individual or a company. Browsing is not an attack but something you do when connected to the Internet. Phishing is known as acquiring sensitive information through the use of electronic communication. Nowadays, hacking is a general term used to describe many different types of attacks.
7. **B.** A chain of custody is the chronological documentation or paper trail of evidence. A disaster recovery plan details how a company will recover from a disaster with such methods as backup data and sites. A key distribution center is used with the Kerberos protocol. Auditing is the verification of logs and other information to find out who did what action and when and where.
8. **D.** The Gramm-Leach-Bliley Act protects private information such as Social Security numbers. HIPAA deals with health information privacy. SOX, or the Sarbanes-Oxley Act of 2002, applies to publicly held companies and accounting firms and protects shareholders in the case of fraudulent practices.

9. **A., B., and D.** Rainbow tables are lookup tables used when recovering passwords. User education and awareness can help defend against social engineering attacks, phishing, and dumpster diving.
10. **A.** Social engineering is the practice of obtaining confidential information by manipulating people. Using someone else's network is just theft. Hacking into a router is just that, hacking. And a virus is a self-spreading program that may or may not cause damage to files and applications.
11. **D.** User awareness is extremely important when attempting to defend against social engineering attacks. Vulnerability testing and auditing are definitely important as part of a complete security plan but will not necessarily help defend against social engineering and definitely will not help as much as user awareness training. People should not share passwords.
12. **D.** Non-repudiation, although an important part of security, is not part of the incident response process. Eradication, containment, and recovery are all parts of the incident response process.
13. **A. and E.** Public buildings, shared office space, and companies with employees that have little training are all environments in which social engineering attacks are common and would be most successful. Social engineering will be less successful in secret buildings, buildings with a decent level of security such as military facilities, and organizations with dedicated and well-trained IT staff.
14. **A.** Eavesdropping is when people listen to a conversation that they are not part of. A security administrator should keep in mind that someone could always be listening, and thus should always try to protect against this.
15. **C.** The code of ethics describes how a company wants its employees to behave. A chain of custody is a legal and chronological paper trail. Separation of duties means that more than one person is required to complete a job. Acceptable use policy is a set of rules that restricts how a network or a computer system may be used.
16. **A.** Before analyzing any acquired data, you need to make sure that the data has not been tampered with, so you should verify the integrity of the acquired data before analysis.
17. **C.** CO<sub>2</sub> is the best answer that will prevent damage to computers because CO<sub>2</sub> is air-based, not water-based. CO<sub>2</sub> displaces oxygen. Fire needs oxygen; without it the fire will go out. All the other options have substances that can damage computers. However, because CO<sub>2</sub> can possibly cause ESD damage, the best solution in a server room would be Halotron or FE-36.

18. A. Most organizations' incident response procedures will specify that containment of the malware incident should be first. Next would be the removal, then recovery of any damaged systems, and finally monitoring that should actually be going on at all times.
19. C. Any person pretending to be a data communications repair person would be attempting a social engineering attack.
20. A. Acceptable use (or usage) policies set forth the principles for using IT equipment such as computers, servers, and network devices. Employees are commonly asked to sign such a document that is a binding agreement that they will try their best to adhere to the policy.
21. D. He should follow the change management process as dictated by your company's policies and procedures. This might include filing forms in paper format and electronically, and notifying certain departments of the proposed changes before they are made.
22. A. An SLA, or service-level agreement, is the agreement between the Internet service provider and you, defining how much traffic you are allowed and what type of performance you can expect. A VPN is a virtual private network. A DRP is a disaster recovery plan. And WPA is Wi-Fi Protected Access.
23. C. Turnstiles, double entry doors, and security guards are all examples of preventative measures that attempt to defeat piggybacking. Dumpster diving is when a person looks through a coworker's trash or a building's trash to retrieve information. Impersonation is when a person attempts to represent another person, possibly with the other person's identification. Eavesdropping is when a person overhears another person's conversation.
24. C. Human resources personnel should be trained in guidelines and enforcement. A company's standard operating procedures will usually have more information about this. However, a security administrator might need to train these employees in some areas of guidelines and enforcement.
25. D. In classified environments, especially when accessing top secret information, a person can get access to only what they need to know.
26. A. and C. The most common techniques that attackers use to socially engineer people include flattery, dumpster diving, bribery, and forgery. Although assuming a position of authority is an example of social engineering, it is not one of the most common. A WHOIS search is not necessarily malicious; it can be accomplished by anyone and can be done for legitimate reasons. This type of search can tell a person who runs a particular website or who owns a domain name.

- 27. D.** A code of ethics is documentation that describes the minimum expected behavior of employees of a company or organization. Need to know deals with the categorizing of data and how much an individual can access. Acceptable usage defines how a user or group of users may use a server or other IT equipment. Separation of duties refers to a task that requires multiple people to complete.
- 28. C.** When an employee has been terminated, the employee's account should be disabled, and the employee's data should be stored for a certain amount of time, which should be dictated by the company's policies and procedures. There is no need to speak to the employee's supervisor. It is important not to delete the user account because the company may need information relating to that account later on. Changing the user's password is not enough; the account should be disabled.
- 29. A.** Mantraps are the best solution listed—they are the closest to foolproof of the listed answers. Mantraps (if installed properly) are strong enough to keep a human inside until he completes the authentication process or is escorted off the premises. This is a type of preventive security control meant to stop tailgating and piggybacking. Video surveillance will not prevent an unauthorized person from entering your data center; rather, it is a detective security control. Security guards are a good idea, but if they work only at night, then they can't prevent unauthorized access at all times. 802.1X is an excellent authentication method, but it is logically implemented as software and devices; it is not a physical security control.
- 30. D.** Spear phishing is a targeted attack, unlike regular phishing, which usually works by contacting large groups of people. Pharming is when a website's traffic is redirected to another, illegitimate, website. Vishing is the phone/VoIP version of phishing.
- 31. B.** Password masking is when the characters a user types into a password field are replaced, usually by asterisks. This is done to prevent shoulder surfing. Tailgating is when an unauthorized person follows an authorized person into a secure area, without the second person's consent. Impersonation is when a person masquerades as another, authorized user. A hoax is an attempt at deceiving people into believing something that is false.
- 32. C.** By creating a policy that disallows personal music devices, you reduce the possibility of data leakage. This is because many personal music devices can store data files, not just music files. This could be a difficult policy to enforce since smartphones can play music and store data. That's when you need to configure your systems so that those devices cannot connect to the organization's network. DLP devices would also help to prevent data leakage. Network

shares are part of the soul of a network; without them, there would be chaos as far as stored data. If network shares are configured properly, there shouldn't be much of a risk of data leakage. Password protecting files is something that would be hard to enforce, and the encryption used could very easily be subpar and easily cracked. HSMs are inherently encrypted; that is their purpose. To allow an HSM would be a good thing, but there are no unencrypted HSMs.

33. **B.** and **D.** PII (personally identifiable information) must be handled and distributed carefully to prevent ID theft and fraud. In a BYOD environment, personal electronic devices should also be protected and secured and require special policies as well because the devices are being used for personal *and* business purposes. Phishing is the attempt at obtaining information fraudulently. SOX (Sarbanes-Oxley) is an act that details the disclosure of banking information.
34. **C.** Whaling is a type of spear phishing that targets senior executives such as CFOs. Regular old phishing does not target anyone, but instead tries to contact as many people as possible until an unsuspecting victim can be found. Vishing is the telephone-based version of phishing. Spear phishing does target individuals but not senior executives.
35. **B.** Job rotation is when people switch jobs, usually within the same department. This is done to decrease the risk of fraud. It is closely linked with separation of duties, which is when multiple people work together to complete a task; each person is given only a piece of the task to accomplish. Least privilege is when a process (or a person) is given only the bare minimum needed to complete its function. Mandatory vacations are when an employee is forced to take X number of consecutive days of vacation away from the office.
36. **A.** Humidity (if increased) can reduce the chance of static discharges. Temperature does not have an effect on computer systems (within reason). EMI and RFI are types of interference that in some cases could possibly increase the chance of static discharge.
37. **A.** and **D.** The privacy screens are being implemented to prevent shoulder surfing. The secure shredding system is being implemented to mitigate dumpster diving. Impersonation is when an unauthorized person masquerades as a legitimate, authorized person. Phishing is when an attacker attempts to fraudulently obtain information through e-mail scams. Tailgating is when a person (without proper credentials) attempts to gain access to an unauthorized area by following someone else in.
38. **D.** The most important activity when implementing a GRC system in this scenario is continuous security monitoring. It will provide for a secure posture while overseeing the work of the third-party vendor. Baselineing is important as

well as part of vulnerability management, but the answer “baseline configuration” refers more to the building of a baseline, and not the constant monitoring of that baseline. An SLA is a service-level agreement, which, once agreed to, isn’t something you normally *monitor* so to speak. It is a contract of sorts. Security alerting and trending is a part of continuous security monitoring.

- 39. C.** Of the listed answers, a hard drive would be considered the least volatile when performing incident response procedures. The order of volatility defines any type of registers as the most volatile, and cache and RAM as slightly less volatile. On the other hand, backup tapes are less volatile than hard drives, and optical discs are less volatile as well. Those last two options make for good options if forensics data needs to be stored over the long term.
- 40. A.** The best practice in this scenario is to document. In fact, you should always document. Document everything to be on the safe side. Work around the problem as best you can. Never try to hide anything. It could be costly to the investigation, and your livelihood. You shouldn’t have to assess another area of the disc, because you have made a copy (or more than one) and should be able to still access that portion of the disc where the mistake occurred. You should always verify the tools and software used, but this is more of a standard procedure and less of a *best practice*; besides, it doesn’t necessarily have to do with the mistake.

## Case Studies for Chapter 16

The case studies in this chapter offer generic scenarios for you to read through and answer according to your own technology and experiences. At the end of the section are example solutions. Your solutions will vary in comparison to the book, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations, which can be found on the book’s disc.

### Case Study 16-1: Identifying Social Engineering Attacks

**Scenario:** As an IT professional, you realize that your job spans much more than just computers. For instance, it deals with the intangible world of social engineering. You have recently taken over the position of security administrator for a company with 200 users, but prior to your new appointment there was little if any security. You are concerned with people that were previously allowed access to the building and how those people might try to infiltrate your company in the future through social engineering techniques.

Conduct research on the Internet and give one example each of pretexting, hoaxes, and malicious insiders. Then, define ways that you would protect your company, data, and employees from these social engineering methods.

### Case Study 16-2: Imaging a Hard Drive and Live Data for Forensic Purposes

**Scenario:** You work for a small organization and wear multiple hats: network administrator, cable installer, security administrator, and digital forensic analyst, when required. Upper management is concerned that an employee (who left work suddenly and didn't return) might have been attempting to compromise the organization's secret data. Your task is to document the potential crime scene (the ex-employee's workstation), analyze the data on the computer, and see if there is any merit to the organization's concerns.

Name a couple forensically acceptable software tools you can use to image the hard drive.

Name a forensically acceptable software tool you can use to copy the live data.

Name a couple LiveCDs that you can use to image the drive (which may or may not be forensically acceptable).

## Case Study Solutions

### Case Study 16-1 Solution

You can read all kinds of stories about social engineering experts, and the cons they have pulled off. They might be true, they might not. What matters is this: Does it sound feasible? And if so, how would you protect against it? For example, Kevin Mitnick is one of the most well-known masters of social engineering (as well as a top-notch hacker). Supposedly, in his early days, he found out from a bus driver where he could get his own ticket punch, and therefore ride the city bus for free. How did he do this? Probably through the grooming of trust, or the bus driver simply liked him, but effectively there was some kind of pretexting going on somewhere along the way. People who are good at employing social engineering techniques are usually very knowledgeable of psychology in one way or another. They can relate to the person they are attempting to con. So, in the case study scenario, can you think of anyone who used to work for the company that fits this image? Could your company withstand a sweet-talking impersonator? To protect against this, identification and authorization become your best friends.

One common example of a hoax is the virus hoax. These come in many shapes and sizes, but are usually either received through e-mail or show up on a website that a user has been redirected to. The hoax might state that the user's computer will catch on fire in 10 minutes, or perhaps that the computer's files have all been encrypted. (Be careful here, though, because there are actual ransomware attacks that will do just this.) The real problem with virus hoaxes is not that they cause computers to fail, but that they decrease productivity: people discuss the hoax, and they forward

it (as requested) to friends and co-workers. To defend against this from a technical standpoint, implementing e-mail filters, updating firewalls, IDS/IPS, and updating AV software are all recommended. To protect from a user standpoint, you should train your users what to be on the lookout for. Give actual examples on a computer screen. Explain that it is very unlikely that a computer will catch fire from a virus. Train users to screen their e-mails carefully and to not open or accept unknown attachments. In the case they do get a display that says their computer is doomed, or to pay a ransom immediately, the best thing to do is shut off the computer and notify the IT personnel.

Malicious insiders are among the deadliest, because they already have access to a certain extent, and getting full access is just one step away. Examples of victims and their respective malicious insiders include USB PaineWebber and Roger Duronio (logic bomb); the DoD and Bradley Manning (release of classified documents to WikiLeaks); and the city of San Francisco and Terry Childs (network tampering)—the examples go on and on. More often than not, these people are disgruntled and perhaps want some kind of revenge. But there are plenty of cases in which the person was simply in it for the money. But the motive doesn't really matter to a security administrator, because the end result is increased chaos, decreased productivity, and loss of money for the company. So it is a matter of protection, but how? Here are some tips. First, remember your *lessons learned*. Learn from past attacks, whether you have read about them or they have happened to your company. Understand how the attack occurred, and what security control could have prevented it. Next, protect the most important data first. For example, work on patents, the design schematics for a new computer, the code for an unreleased computer program, the secret ingredient in your latest and greatest barbecue sauce—whatever it is, use all of your security power to protect that all-important data first and foremost. Watch for suspect behavior. Human Resources will probably keep a file on people with suspect attitudes, so you should interface with HR often. Watch for quick terminations and resignations. It's good manners for an employee to give two weeks' notice so as to gracefully transition work to other employees. Quick resignations are a red flag. But all this is commentary—the real way to protect against these threats is to have strong policies, well-planned permissions, tough physical security, strong authentication, and enforcement of principles such as need-to-know and least privilege.

**Simulation:** Complete the simulations “16-1: Identifying Social Engineering Attacks” Parts A and B on the accompanying disc.

### Case Study 16-2 Solution

The key with a potentially compromised computer is to document everything you see (and can't see). Take photos, write down what you encounter, and of course, use software and hardware tools to *image* the machine.

For example, to image a hard drive you might use AccessData's Forensic Toolkit, or Guidance Software's EnCase. These are commonly used tools that are usually accepted by the courts as forensically sound applications. Of course, these tools come with a price tag attached (a hefty one), and so in some cases a smaller company will go with simply imaging the drive bit by bit, which could be done with cloning software, or with a LiveCD (or LiveDVD) such as Knoppix or BackTrack. The question here is whether these tools (and the resulting hard drive images) will be acceptable to a court of law. Also, you have to be very careful not to disturb the original drive when making the image, something that can easily be done when using a tool not designed specifically for the job.

If you were to use a LiveCD—and there are many options—it would be derived from Linux, and so a solid knowledge of the command-line would be necessary. For example, if you were to image a drive, you would need to understand the syntax of the `dd` and `nc` commands. Plus, you would need to copy the data from one system to another. Many forensic analysts will use a Linux OS (such as Ubuntu) as the destination computer for the copied image. That system would have a secondary drive that could either be analyzed or booted off if necessary.

For live data—and we are talking about the RAM and other volatile areas of the computer—you could use Live Response, which might run off of a USB key, and Helix software. That is only if the computer is already powered up when you encounter it. If the computer is off, then volatile areas of storage will most likely be cleared.



### This chapter covers the following subjects:

- **Getting Ready and the Exam Preparation Checklist:** This section gives you a step-by-step list on how to go about taking the exam. It also shows one of my favorite study methods—the cheat sheet.
- **Tips for Taking the Real Exam:** In this section, you learn all my certification test taking techniques that I have developed over the past 15 years.
- **Beyond the CompTIA Security+ Certification:** This section briefly discusses your future and the possibilities that are out there.

Now you've done it! You've accessed the final chapter. We are at the final countdown! This chapter shows you how to go about taking the exam. Then it goes over some tips and tricks I have used over the years that have helped me to pass the exam. Finally, we discuss some of the possible future avenues that can lead you to a career in IT security.

# Taking the Real Exam

## Getting Ready and the Exam Preparation Checklist

The CompTIA Security+ certification exams can be taken by anyone. There are no prerequisites, although CompTIA recommends prior networking experience and the Network+ certification. For more information on CompTIA and the Security+ exam, go to the following link:

<http://certification.comptia.org/>

To acquire your Security+ certification, you need to pass the SY0-401 exam, which is a maximum of 90 questions (consisting of multiple-choice and performance-based questions). The specific details of the exam can change over time, so to find out the latest, go to the previous link or go to my site at <http://www.davidlprowse.com>

The exam is administered by Pearson VUE. You need to register with that test agency in order to take the exam. To do so, go to the following link:  
<http://www.pearsonvue.com/comptia/>

**NOTE** If you have never taken a CompTIA exam before, and depending on your location, you might have to create an account with CompTIA first ([at www.comptia.org](http://www.comptia.org)) before registering for an exam with a testing agency. This could take up to 48 hours to complete. I recommend you check this ahead of time so that there are no surprises once you are ready to register for the exam.

CompTIA uses a somewhat unorthodox grading scale, so it can be difficult to estimate what percentage of questions you need to get correct to pass the exam. To be safe, the best bet is to attempt to know as much as possible and shoot for 90% correct or higher when taking the practice exams provided with this book.

It is important to be fully prepared for the exam, so I created a checklist that you can use to make sure you have covered all the bases. The checklist is shown in Table 17-1. Place a check in the status column as each item is completed. Historically, my readers and students have benefited greatly from this type of checklist.

**Table 17-1** Exam Preparation Checklist

| Step | Item                                    | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | SYO-401 Status |
|------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 1.   | Review the end of chapter questions.    | <p>The first step in your exam preparation checklist is to review all the end-of-chapter questions. There are well over 400 of them in total, offering you a lot of prep before you move on to the practice exams. You can review them in the text or, if you have the accompanying disc, electronically. Make sure you understand the concepts thoroughly before moving on to the following steps.</p> <p>Note: During this stage you might also want to check your local testing center and see whether there are any delays for the Security+ exam. If you are under a deadline and you see that there are delays of up to a week or two, consider other testing center locations, or consider scheduling your exam now to save your seat. If you do, be sure to commit to your study schedule. Otherwise, if there are no delays, continue through the steps as normal.</p>                                    |                |
| 2.   | Complete simulations and watch videos.  | <p>There are over 30 videos and simulations to be found on the disc. Go through them and be sure to practice any corresponding hands-on skills on your own computers. This hands-on practice will help you with the performance-based questions on the real exam, and more importantly will strengthen you for the IT field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                |
| 3.   | Complete the Practice Exam in the book. | <p>Directly after this chapter is a 100-question practice exam. Your goal should be to get at least 90% correct on this exam the <i>first time through</i>. Do not continue to any other exams until you can score at least 90% correct on this exam (100% would be even better!).</p> <p>You can also take the exam electronically if you have the disc that accompanies the print version of this book. Two more practice exams can be found on the disc as well.</p> <p>When using the practice exams, be sure to understand why the correct answer is correct and also why incorrect answers are incorrect. The explanations should help you in this regard. However, if any names, acronyms, or concepts seem new to you, go back to the chapter and section where the concept is covered and review them. Also, review the names and acronyms in the glossary, which is located after the practice exam.</p> |                |

| Step | Item                   | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | SY0-401 Status |
|------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 4.   | Visit my website.      | <p>Make use of the Security+ section of my website:<br/><a href="http://www.SY0-401.com">www.SY0-401.com</a></p> <p>Feel free to ask questions about any of the practice exam questions and explanations, or other items within this book. That's why I am here! On the site you will also find the book's errata page, videos, articles, and other materials. You can also reach the home page of my site at:<br/><a href="http://www.davidlprowse.com">www.davidlprowse.com</a></p>                                                                                                                                                                                                                                                                                                     |                |
| 5.   | Create a cheat sheet.  | <p>A cheat sheet can be very helpful for late-stage studying. See Table 17-2 for an example. The act of writing down important details helps to commit them to memory. This sheet should have facts that are tough to memorize. Due to this, each person's cheat sheet will vary. Keep in mind that you will not be allowed to take this into the actual testing room. (It's not actually for "cheating!") One great way to help build your "cheat" sheet is to go back through all of the key topics in the book.</p>                                                                                                                                                                                                                                                                    |                |
| 6.   | Register for the exam. | <p>Do not register until you have completed the previous steps; you shouldn't register until you are fully prepared (unless you saw that the testing center was delayed during step 1). When you are ready, schedule the exam to commence within a day or two so that you won't forget what you learned!</p> <p>Registration can be done over the phone or online; although, online is much easier for many people. Register at Pearson VUE at the following website:<br/><a href="http://www.pearsonvue.com/comptia/">http://www.pearsonvue.com/comptia/</a></p> <p>You need to input your personal information into a secure website. Afterward, you will be assigned an ID#, which you can refer to for all your exams. They accept payment by major credit card for the exam fee.</p> |                |
| 7.   | Final study.           | <p>Study from the cheat sheet (and perhaps the practice exams) during the day or two between when you registered and the day of the exam.</p> <p>If you need to delay your exam for any reason, reschedule, then go back to steps 1 and 2 (and optionally 3), and retake the practice exams until the test day is a day or two away. Remember that you must give the testing center at least 48 hours' notice if you wish to reschedule. Note: This timeframe can change at any time. Check the Pearson VUE FAQs for the latest updates:<br/><a href="http://www.pearsonvue.com/faqs/cand_regsched.asp">http://www.pearsonvue.com/faqs/cand_regsched.asp</a></p>                                                                                                                          |                |

| <b>Step</b> | <b>Item</b>    | <b>Details</b>                                                                                                        | <b>SY0-401 Status</b> |
|-------------|----------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------|
| 8.          | Take the exam! | Good luck! Check mark the column to the right when you pass. Let me know on my website when you have passed the exam! |                       |

Table 17-2 gives a partial example of a cheat sheet that you can create to aid in your studies. For example, the first row shows common ports. Add information that you think is important or difficult to memorize. Keep the descriptions short and to the point. A few examples are listed in the table.

**Table 17-2** Example Cheat Sheet

| <b>Concept</b>               | <b>Fill in the Appropriate Information Here</b>                                                                                                                                                                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Common port numbers          | Echo: Port 7<br>CHARGEN: Port 19<br>FTP: Port 21<br>(Complete for all ports.)                                                                                                                                                                                                                                            |
| Access control models        | MAC: Mandatory access control—Uses labels, has predefined privileges.<br>DAC: Discretionary access control—Uses ACLs, or access control lists. Owner of list establishes access permissions.<br>RBAC: Role-based access control—Permissions are assigned to roles instead of individual users. Users are assigned roles. |
| NIDS and NIPS                | (Spell out the acronym and give a brief description.)                                                                                                                                                                                                                                                                    |
| The CIA of computer security | (Spell out the acronym and give a brief description.)                                                                                                                                                                                                                                                                    |
| Etc.*                        |                                                                                                                                                                                                                                                                                                                          |

\* Continue Table 17-2 in this fashion on paper. The idea is to write down various technologies, processes, step-by-step tasks, and so on to commit them to memory.

## Tips for Taking the Real Exam

Some of you will be new to certification exams. This section is for you. For others who have taken CompTIA exams before, feel free to skip this section or use it as a review.

The exam is conducted on a computer and has two types of questions. The bulk of the exam consists of multiple-choice questions, where you select one or more correct answers from a list of possibilities. However, there are also some performance-based questions. These might ask you to drag and drop correct answers into their respective slots, or they might ask you to complete a simulation, either within the operating system, in the command-line, or otherwise. This is where your hands-on knowledge is tested. But it shouldn't matter what type of question you receive; if you have studied this book in its entirety, you should be ready for just about anything.

Note that you have the option to skip questions. If you do so, be sure to “mark” them before moving on. There will be a small checkbox that you can select to mark them. Feel free to mark any other questions that you have answered but are not completely sure about, or any questions that you think are taking you too long to answer. When you get to the end of the exam, there will be an item review section, which shows you any questions that you did not answer and any that you marked. Though you should try to avoid marking many items and skipping around, sometimes it is unavoidable and can save time in the long run if a question is overly difficult. A good rule of thumb is to keep the marked questions between 10% and 20%. Just be sure to allow some time at the end of the exam to finish up those marked questions!

The following list includes tips and tricks that I have learned over the years when it comes to taking exams. By utilizing these points, you can easily increase your score.

First, let's talk about some good general practices for taking exams:

- **Pick a good time for the exam:** It would appear that the least amount of people are at test centers on Monday and Friday mornings. Consider scheduling during these times. Otherwise, schedule a time that works well for you, when you don't have to worry about anything else. Keep in mind that Saturdays can be busy.
- **Don't over-study the day before the exam:** Some people like to study hard the day before; some don't. My recommendation is to study off the cheat sheet you created, but in general, don't overdo it. It's not a good idea to go into overload the day before the exam.
- **Get a good night's rest:** A good night's sleep (7 hours to 9 hours) before the day of the exam is probably the best way to get your mind ready for an exam.

- **Eat a decent breakfast:** Eating is good! Breakfast is number two when it comes to getting your mind ready for an exam, especially if it is a morning exam. Just watch out for the coffee and tea. Too much caffeine for a person who is not used to it can be detrimental to the thinking process.
- **Show up early:** Both testing agencies recommend that you show up 30 minutes prior to your scheduled exam time. This is important; give yourself plenty of time, and make sure you know where you are going. You don't want to have to worry about getting lost or being late. (If it is the first time going to the testing center, consider a test drive a couple days before.) Stress and fear are mind killers. Work on reducing any types of stress the day of and the day before the exam. By the way, you really do need extra time, because when you get to the testing center, you need to show ID, sign forms, get your personal belongings situated, and be escorted to your seat. Have two forms of ID (one, a photo ID, both signed) ready for the administrator of the test center. Turn your phone off when you get to the test center; they'll check that, too.
- **Bring ear plugs:** You never know when you will get a loud testing center—or worse yet, a loud test taker next to you. Ear plugs help to block out any unwanted noise that might show up. Just be ready to show your ear plugs to the test administrator.
- **Brainstorm before starting the exam:** Write down as much as you can remember from the cheat sheet before starting the exam. The testing center is obligated to give you something to write on; make use of it! By getting all the memorization out of your head and on “paper” first, it clears the brain somewhat so that it can tackle the questions. I put “paper” in quotation marks because it might not be paper; it could be a mini dry-erase board or something similar.
- **Take small breaks while taking the exam:** Exams can be brutal. You have to answer up to 100 questions while staring at a screen for an hour or more. Sometimes these screens are old and have seen better days; these older flickering monitors can cause a strain on your eyes. I recommend small breaks and breathing techniques. For example, after going through every 25 questions or so, close your eyes, and slowly take a few deep breaths, holding each one for 5 seconds or so, and releasing each one slowly. Think about nothing while doing so. Remove the test from your mind during these breaks. It takes only half a minute but can really help to get your brain refocused.
- **Be confident:** You have studied hard, gone through the practice exams, created your cheat sheet—done everything you can to prep. These things alone should build confidence. But really, you just have to be confident. You are great...I am great...there is no disputing this!

Now let's talk about some methods to use when faced with difficult questions:

- **Use the process of elimination:** If you are not sure about an answer, first eliminate any answers that are definitely incorrect. You might be surprised how often this works. This is one of the reasons why it is recommended that you not only know the correct answers to the practice exams' questions, but also know why the wrong answers are wrong. The testing center should give you something to write on; use it by writing down the letters of the answers that are incorrect to keep track.

**NOTE** Check out this chapter's video. It shows me going through a couple of questions as if I were taking an exam and shows some of my tips and tricks to taking the exam.

- **Be logical in the face of adversity:** The most difficult questions are when two answers appear to be correct, even though the test question requires you to select only one answer. Real exams do not rely on "trick" questions. Sometimes you need to slow down, think logically, and really compare the two possible correct answers.
- **Use your gut instinct:** Sometimes a person taking a test just doesn't know the answer; it happens to everyone. If you have read through the question and all the answers and used the process of elimination, sometimes the gut instinct is all you have left. In some scenarios you might read a question and instinctively know the answer, even if you can't explain why. Tap into this ability. Some test takers write down their gut instinct answer before delving into the question and then compare their thoughtful answer with their gut instinct answer.
- **Don't let one question beat you!:** Don't let yourself get stuck on any one question (especially the performance-based variety). Mark it, move on to the next question, and return to it later. When you spend too much time on one question, the brain gets sluggish. The thing is, with these exams you either know it or you don't. And don't worry too much about it; chances are you are not going to get a perfect score. Remember that the goal is only to pass the exam; how many answers you get right after that is irrelevant. If you have gone through this book thoroughly, you should be well prepared, and you should have plenty of time to go through all the exam questions with time to spare to return to the ones you skipped and marked.
- **If all else fails, guess:** Remember that the exams might not be perfect. A question might seem confusing or appear not to make sense. Leave questions

like this until the end, and when you have gone through all the other techniques mentioned, make an educated, logical guess. Try to imagine what the test is after, and why they would be bringing up this topic, vague or strange as it might appear.

And when you finish:

- **Review all your answers:** Use the time allotted to you to review the answers. Chances are you will have time left over at the end, so use it wisely! Make sure that everything you have marked has a proper answer that makes sense to you. But try not to over think! Give it your best shot and be confident in your answers.

## Beyond the CompTIA Security+ Certification

After you pass the exam, consider thinking about your technical future. Technical growth is important. Keeping up with new technology and keeping your technical skills sharp are what can keep you in demand. This technical growth equals job security.

Information Technology (IT) people need to keep learning to foster good growth in the field. Consider additional college courses (or even degrees). Contemplate taking other certification exams after you complete the Security+. The CompTIA Security+ certification acts as a springboard to other certifications. For example, you might choose to go for other more difficult non-vendor certifications such as the CISSP. And of course, there are vendor-specific certifications from Microsoft, Cisco, Check Point, and many others. Now that you know exactly how to go about passing a security-based certification exam, consider more certifications to bolster your resume, and maybe even a computer security degree.

The best advice I can give is to do what you love. From an IT perspective, I usually break that down by technology or concept, as opposed to by the vendor. Products and vendors come and go. Knowledge of a particular device or a distinct program can be fleeting. But skill sets that are based on conceptual technology will have more value in the long-term. Whatever segment (or segments) of security you decide to pursue, learn as much as you can about that field(s) *and* all its vendors. Read up on the latest technologies, visit security websites, read security periodicals, and keep in touch with fellow security people. Consider security conferences and seminars and ongoing training. Taking it to the next level, you might decide that there is a specific security threat that you would like to address. Who knows, in the future you might be interested in developing a security application or a secure hardware device. My advice is this: Good engineering can usually defy malicious individuals; the better you plan your security product, the less chance of it being compromised.

Whatever you decide, I wish you the best of luck in your IT career endeavors. And remember that I am available to answer any of your questions about this book via my website: [www.davidlprowse.com](http://www.davidlprowse.com).

## Case Study for Chapter 17

### Case Study 17-1: Analyzing Test Questions

If you want to do well on the real exam, you must analyze questions carefully. Getting the answer right is only half the battle. You also need to be able to identify why the incorrect answers are wrong. If there are any concepts that you don't understand in a question, review them, even if they were part of a listed answer that was incorrect. Work on your comprehension of the concepts from a theoretical standpoint as well as a hands-on standpoint. Ultimately, this combination of knowledge will enhance your test-taking skills.

Practice as much as you can. Use the Practice Test software on the disc that accompanies this book. That software emulates the look of the real exam. By practicing in that environment, you will feel much more comfortable when it comes time to take the real test.

Going further, consider accessing the CompTIA website. As I often say: “Go to the source!” CompTIA often has sample practice questions you can go through to gauge your readiness. They are usually listed directly on the main Security+ page, but if not, search around a little bit, or run a search for “Security+ sample questions.” If they are available, you should be able to find them on CompTIA’s website.

In summary, practice as much as you can, know the correct answers, understand why the incorrect answers are wrong, and then practice some more! The harder you push yourself, the better you will do on the exam.

**Video Solution:** Watch the video solution “17-1: Analyzing Test Questions” on the accompanying disc.



The 100 multiple-choice questions provided here help you to determine how prepared you are for the actual exam and which topics you need to review further. Write down your answers on a separate sheet of paper so that you can take this exam again if necessary. Compare your answers against the answer key that follows this exam. Following the answer key are detailed explanations for each question.

# Practice Exam 1: SY0-401

1. What is software that is designed to infiltrate a computer system without the user's knowledge or consent?
  - A. Malware
  - B. Privilege escalation
  - C. Whitelists
  - D. HIDS
2. Which of the following best describes a backdoor?
  - A. Code inserted into software that initiates one of several types of functions when specific criteria are met
  - B. Computer programs used to bypass normal authentication or other security mechanisms in place
  - C. A platonic extra added to an operating system
  - D. A group of compromised computers
3. Closing open mail relays can help prevent what type of malware?
  - A. Virus
  - B. Worm
  - C. Spam
  - D. Trojan
4. Your company uses instant messaging between the central office and satellite offices. What is the most important security issue that you need to deal with when it comes to instant messaging?
  - A. Different instant messaging programs have no common protocol.
  - B. Instant messaging has no or weak encryption.
  - C. Instant messaging can adversely affect Internet bandwidth.
  - D. Instant messaging program sessions are open and unprotected.

5. Malware can use virtualization techniques. Why would this be difficult to detect?
  - A. A portion of the malware might have already been removed by an IDS.
  - B. The malware might be using a Trojan.
  - C. The malware could be running at a more privileged level than the computer's antivirus software.
  - D. The malware might be running in the command-line.
6. Which of the following are components of hardening an operating system? (Select the two best answers.)
  - A. Disabling unnecessary services
  - B. Configuring the desktop
  - C. Applying patches
  - D. Adding users to the administrators group
  - E. Enabling services
7. A hacker develops a piece of malicious code. It is not designed to automatically spread from one system to another. Instead, it is designed to spread from one file to another file on the individual computer. What type of malware is this?
  - A. Worm
  - B. Trojan
  - C. Botnet
  - D. Virus
8. You are the network security administrator for your organization. You are in charge of deploying 50 new computers on the network. Which of the following should be completed first?
  - A. Apply a baseline configuration.
  - B. Install operating system updates.
  - C. Install the latest spyware.
  - D. Install a spreadsheet program.
9. You are attempting to apply corporate security settings to a workstation. Which of the following would be the best solution?
  - A. Hotfix
  - B. Security template

- C. Patch
  - D. Service pack
10. Which of the following characterizations best suits the term Java applet?
- A. Java applets include a digital signature.
  - B. Java applets allow for customized controls and icons.
  - C. Java applets need to have virtual machine web browser support.
  - D. Java applets are the same as ActiveX controls.
11. Which of the following security threats can be updated remotely from a command center?
- A. Virus
  - B. Worm
  - C. Spam
  - D. Zombie
12. Which of the following attacks cannot occur through e-mail?
- A. Phage virus
  - B. Dictionary attack
  - C. Polymorphic virus
  - D. Trojan horse
13. Of the following software components, which is usually associated with a web browser?
- A. Personal firewall
  - B. Anti-spyware
  - C. Pop-up blocker
  - D. Service packs
14. You are in charge of monitoring a workstation for application activity and/or modification. Which of the following types of systems should you use?
- A. RADIUS
  - B. NIDS
  - C. OVAL
  - D. HIDS

- 15.** If a switch enters fail open mode because its CAM table memory has been filled, then it will cease to function properly as a switch. What type of attack could cause this?
  - A.** Double tagging
  - B.** MAC flooding
  - C.** Physical tampering
  - D.** DoS
- 16.** Which of the following services uses port 49?
  - A.** File Transfer Protocol
  - B.** Post Office Protocol version 3
  - C.** Terminal Access Controller Access-Control System Plus
  - D.** Domain Name System
- 17.** Study the following items carefully. Which one permits a user to “float” a domain registration for a maximum of 5 days?
  - A.** DNS poisoning
  - B.** Domain hijacking
  - C.** Domain spoofing
  - D.** Kiting
- 18.** Which of the following is an area of the network infrastructure that enables a person to put public-facing systems into it without compromising the entire infrastructure?
  - A.** DMZ
  - B.** VLAN
  - C.** VPN
  - D.** NAT
- 19.** What are the two best ways to protect a Voice over IP PBX from man-in-the-middle attacks? (Select the two best answers.)
  - A.** Update the Voice over IP system.
  - B.** Use an authentication scheme.
  - C.** Install a key system.
  - D.** Use encryption.

- 20.** Which of the following is most often used to enable a client or a partner access to your network?
- A.** Intranet
  - B.** Extranet
  - C.** DMZ
  - D.** VLAN
- 21.** Which of the following is a type of packet filtering used by firewalls that retains memory of the packets that pass through the firewall?
- A.** Stateless packet filter
  - B.** Circuit-level gateway
  - C.** NAT filtering
  - D.** Stateful packet inspection
- 22.** Which of the following attacks is best described as an attacker capturing part of a communication, and then later sending some or all of that communication to a server while pretending to be the original client?
- A.** Replay attack
  - B.** TCP/IP hijacking
  - C.** Backdoor
  - D.** Man-in-the-middle attack
- 23.** Of the following, which type of device attempts to serve client requests without the user actually contacting the remote server?
- A.** IP proxy
  - B.** HTTP proxy
  - C.** Firewall
  - D.** DMZ
- 24.** Which of the following is the strongest password?
- A.** password
  - B.** Apassword
  - C.** Apassword123
  - D.** A#password123

- 25.** What is one of the potential risks associated with WEP when that protocol is used to secure a WLAN?
- A.** SSID broadcast
  - B.** Weak encryption
  - C.** Data emanation
  - D.** Zero protection against war-driving attacks
- 26.** Which one of the following attacks misuses the Transmission Control Protocol three-way handshake process in an attempt to overload network servers so that authorized users are denied access to network resources?
- A.** SYN attack
  - B.** Man-in-the-middle attack
  - C.** Teardrop attack
  - D.** Smurf attack
- 27.** Which of the following security applications *cannot* proactively detect computer anomalies?
- A.** NIDS
  - B.** HIPS
  - C.** Antivirus software
  - D.** Personal software firewall
- 28.** Which of the following is used to transmit data between a web server and a web browser?
- A.** IMAP
  - B.** SSH
  - C.** HTTP
  - D.** FTP
- 29.** You have been commissioned by a customer to implement a network access control model that limits remote users' network usage to normal business hours only. You create one policy that applies to all the remote users. What access control model are you implementing?
- A.** Role-based access control
  - B.** Mandatory access control

- C. Discretionary access control
  - D. Rule-based access control
30. Which of the following does the discretionary access control model use to identify users who have permissions to a resource?
- A. Roles that users have in the organization
  - B. Predefined access privileges
  - C. Access control lists
  - D. Security labels
31. Your organization asks you to design a web-based application. It wants you to design the application so that it runs under a security context that allows only those privileges required for the application to run to minimize risk if an attack occurs. Which of the following security concepts does this describe?
- A. Implicit deny
  - B. Mandatory access control
  - C. Separation of duties
  - D. Principle of least privilege
32. Which of the following network authentication protocols uses symmetric key cryptography, stores a shared key for each network resource, and uses a Key Distribution Center (KDC)?
- A. Kerberos
  - B. RADIUS
  - C. TACACS+
  - D. PKI
33. Which of the following can restrict access to resources according to the identity of the user?
- A. Mandatory access control
  - B. Role-based access control
  - C. Discretionary access control
  - D. CRL

- 34.** Which of the following access control methods is best described as providing a username, password, and biometric thumbprint scan to gain access to a network?
- A.** Biometrics
  - B.** Three-way handshake
  - C.** Mutual authentication
  - D.** Multifactor
- 35.** Your organization has several separate logins necessary to gain access to several different sets of resources. What access control method could solve this problem?
- A.** SSO
  - B.** Two-factor authentication
  - C.** Biometrics
  - D.** Smart card
- 36.** Which port does Kerberos use by default?
- A.** 21
  - B.** 80
  - C.** 88
  - D.** 389
- 37.** Which of the following access control methods does a smart card rely on?
- A.** Password policies
  - B.** Logical token
  - C.** Access control lists
  - D.** Username and password
- 38.** Which of the following authentication models places importance on a ticket-granting server?
- A.** PAP
  - B.** CHAP
  - C.** Kerberos
  - D.** RADIUS

- 39.** In which of the following phases of identification and authentication does proofing occur?
- A.** Verification
  - B.** Authentication
  - C.** Authorization
  - D.** Identification
- 40.** Which of the following inbound ports must be opened on a server to allow a user to log in remotely?
- A.** 53
  - B.** 3389
  - C.** 389
  - D.** 636
- 41.** You review the system logs for your organization's firewall and see that an implicit deny is within the ACL. Which is an example of an implicit deny?
- A.** An access control list is a secure way of moving traffic from one network to another.
  - B.** Implicit deny will deny all traffic from one network to another.
  - C.** Items not specifically given access are denied by default.
  - D.** Everything will be denied because of the implicit deny.
- 42.** Password-cracking tools are easily available over the Internet. Which of the following is a password-cracking tool?
- A.** AirSnort
  - B.** Nessus
  - C.** Wireshark
  - D.** John the Ripper
- 43.** The IT director asks you to perform a risk assessment of your organization's network. Which of the following should you do first?
- A.** Identify vulnerabilities.
  - B.** Identify organizational assets.
  - C.** Identify threats and threat likelihood.
  - D.** Identify potential monetary impact.

- 44.** Again, you perform risk assessment for your organization. What should you do during the impact assessment?
- A.** Determine actions that can be taken to mitigate any potential threat.
  - B.** Determine how likely it is that a threat might actually occur.
  - C.** Determine the potential monetary costs related to a threat.
  - D.** Determine how well the organization is prepared to manage the threat.
- 45.** You've created a baseline for your Windows Server file server. Which of the following tools can best monitor changes to your system baseline?
- A.** Key management software
  - B.** Resource planning software
  - C.** Antivirus software
  - D.** Performance monitoring software
- 46.** You work as a network administrator for your organization and use a tool to capture ICMP, HTTP, FTP, and other packets of information. Which of the following tools should you use?
- A.** Protocol analyzer
  - B.** Penetration tester
  - C.** Vulnerability scanner
  - D.** Port scanner
- 47.** Which of the following tools can find the open ports on a network?
- A.** Performance monitor
  - B.** Network scanner
  - C.** Protocol analyzer
  - D.** Cain & Abel
- 48.** Which of the following tools require a computer with a network adapter that can be placed in promiscuous mode? (Select the two best answers.)
- A.** Password cracker
  - B.** Vulnerability scanner
  - C.** Network mapper
  - D.** Protocol analyzer
  - E.** Port scanner

49. Which of the following items is a protocol analyzer?
- A. Wireshark
  - B. John the Ripper
  - C. Nessus
  - D. Cain & Abel
50. Which of the following tools can be used to check network traffic for clear-text passwords?
- A. Password cracker
  - B. Protocol analyzer
  - C. Port scanner
  - D. Performance monitor
51. You suspect that files are being illegitimately copied to an external location. The file server that the files are stored on does not have logging enabled. Which log should you access to find out more about the files that are being copied illegitimately?
- A. DNS logs
  - B. Firewall log
  - C. Antivirus log
  - D. System log
52. What are most of the current encryption methods based on?
- A. PKI
  - B. Timestamps
  - C. Algorithms
  - D. DRM
53. You look through some graphic files and discover that confidential information has been encoded into the files. These files are being sent to a sister company outside your organization. What is this an example of?
- A. Confidentiality
  - B. Cryptography
  - C. Digital signature
  - D. Steganography

- 54.** Which of the following is the most complicated centralized key management scheme?
- A.** Asymmetric
  - B.** Symmetric
  - C.** Whole disk encryption
  - D.** Steganography
- 55.** Which of the following types of keys are stored in a CRL?
- A.** Private keys only
  - B.** TPM keys
  - C.** Public and private keys
  - D.** Public keys only
- 56.** For a user to obtain a certificate from a certificate authority, the user must present two items. The first is proof of identity. What is the second?
- A.** Password
  - B.** Public key
  - C.** Private key
  - D.** Authentication
- 57.** What is secret key encryption also called?
- A.** Asymmetrical encryption
  - B.** One-way function
  - C.** Symmetrical encryption
  - D.** Quantum encryption
- 58.** Which of the following algorithms is used by the protocol TLS to establish a session key?
- A.** AES
  - B.** RSA
  - C.** RC4
  - D.** HTTPS

**59.** In this scenario, your organization and a sister organization use multiple certificate authorities (CAs). Which component of PKI is necessary for one CA to know whether to accept or reject certificates from another CA?

- A.** CRL
- B.** Key escrow
- C.** RA
- D.** Recovery agent

**60.** Which of the following OSI model layers is where SSL provides encryption?

- A.** Network
- B.** Application
- C.** Transport
- D.** Session

**61.** Which of the following social engineering attacks relies on impersonation in an attempt to gain personal information?

- A.** Hoaxes
- B.** Phishing
- C.** Dumpster diving
- D.** Shoulder surfing

**62.** You are designing the environmental controls for a server room that contains several servers and other network devices. What role will an HVAC system play in this environment? (Select the two best answers.)

- A.** Shield equipment from EMI.
- B.** Provide isolation in case of a fire.
- C.** Provide an appropriate ambient temperature.
- D.** Maintain appropriate humidity levels.
- E.** Vent fumes from the server room.

**63.** You have been contracted to conduct a forensics analysis on a server. Which of the following should you do first?

- A.** Analyze temporary files.
- B.** Run an antivirus scan.

- C. Obtain a binary copy of the system.
  - D. Search for spyware.
- 64.** What should you be concerned with when transferring evidence?
- A. Change management
  - B. Job rotation
  - C. Due diligence
  - D. Chain of custody
- 65.** The IT director tasks you to set up a backup plan to ensure that your organization can be back up and running within hours if a disaster occurs. Which of the following should you implement?
- A. Hot site
  - B. Redundant servers
  - C. Cold site
  - D. Tape backup
- 66.** One of your database servers is mission-critical. You cannot afford any downtime. What is the best item to implement to ensure minimal downtime of the server and ensure fault tolerance of the data stored on the database server?
- A. UPS
  - B. RAID
  - C. Redundant server
  - D. Spare parts
- 67.** The IT director recommends that you require your service provider to give you an end-to-end traffic performance guarantee. What document will include this guarantee?
- A. Chain of custody
  - B. SLA
  - C. DRP
  - D. Incident response procedures

- 68.** You are the network security administrator for your organization. You recently audited a server and found that a user logged in to the server with a regular account, executed a program, and performed activities that should be available only to an administrator. What type of attack does this describe?
- A.** Privilege escalation
  - B.** Backdoor
  - C.** Trojan horse
  - D.** Brute force
- 69.** Which of the following will a Faraday cage prevent the usage of?
- A.** USB flash drives
  - B.** Uninterruptible power supplies
  - C.** Cell phones
  - D.** Wired keyboards
- 70.** Which of the following statements best defines a computer virus?
- A.** It is a find mechanism, initiation mechanism, and can propagate.
  - B.** It is a search mechanism, connection mechanism, and can integrate.
  - C.** It is a learning mechanism, contamination mechanism, and can exploit.
  - D.** It is a replication mechanism, activation mechanism, and has an objective.
- 71.** Which of the following is the first step in creating a security baseline?
- A.** Define a security policy.
  - B.** Install software patches.
  - C.** Perform vulnerability testing.
  - D.** Mitigate risk.
- 72.** You are the network administrator for your organization and are in charge of many servers, including one web server. Which of the following is the best way to reduce vulnerabilities on your web server?
- A.** Enable auditing and review log files.
  - B.** Block DNS on port 80.
  - C.** Apply updates and patches.
  - D.** Use a 24/7 packet sniffer.

- 73.** The IT director asks you to verify that the organization's virtualization technology is implemented securely. What should you take into consideration?
- A.** Verify that virtual machines are multihomed.
  - B.** Perform penetration testing on virtual machines.
  - C.** Subnet the network so that each virtual machine is on a different network segment.
  - D.** Verify that virtual machines have the latest service packs and patches installed.
- 74.** E-mail servers can be maliciously exploited in many ways, for example, spoofing e-mail messages. Which of the following is a common component that attackers would use to spoof e-mails?
- A.** Open relay
  - B.** Web proxy
  - C.** Session hijacking
  - D.** Logic bomb
- 75.** What are kernel-level rootkits designed to do to a computer? (Select the two best answers.)
- A.** Make a computer susceptible to pop-ups
  - B.** Extract confidential information
  - C.** Hide evidence of an attacker's presence
  - D.** Hide backdoors into the computer
  - E.** Crack the user's password
- 76.** Which of the following methods should you use to fix a single security issue on a computer?
- A.** Configuration baseline
  - B.** Patch
  - C.** Service pack
  - D.** Patch management
- 77.** What kind of attack enables an attacker to access administrator-level resources using a Windows service that uses the local system account?
- A.** Trojan
  - B.** Spyware

- C. Spam
  - D. Privilege escalation
78. You want to make sure that the most recent hotfixes have been applied to a Windows server, and you want to minimize the effort necessary to maintain this solution. What is the best way to accomplish this?
- A. Enable Windows automatic updates.
  - B. Install a third-party patch management system.
  - C. Install a security template.
  - D. Install the latest service pack.
79. Which of the following is the most effective way of preventing adware?
- A. Install an antivirus program.
  - B. Install a host-based intrusion detection system.
  - C. Install a pop-up blocker.
  - D. Install a firewall.
80. Which of the following threats has the highest probability of being increased by the availability of devices such as USB flash drives on your network?
- A. Introduction of new data on the network
  - B. Increased loss of business data
  - C. Loss of wireless connections
  - D. Removal of PII data
81. One of your users complains that files are being randomly renamed and deleted. The last action the user took was to download and install a new screensaver on the computer. The user says that the file activity started immediately after installation of the screensaver. Which of following would be the best description for this screensaver?
- A. Trojan horse
  - B. Logic bomb
  - C. Virus
  - D. Worm

- 82.** Which of the following is often misused by spyware to collect and report a user's activities?
- A.** Session cookie
  - B.** Tracking cookie
  - C.** Persistent cookie
  - D.** Web bug
- 83.** Which of the following enables an attacker to hide the presence of malicious code by altering Registry entries?
- A.** Worm
  - B.** Logic bomb
  - C.** Rootkit
  - D.** Trojan
- 84.** Which of the following is a Class B private IP address?
- A.** 10.254.254.1/16
  - B.** 192.168.1.1/16
  - C.** 172.16.1.1/16
  - D.** 169.254.50.1/24
- 85.** Your manager has asked you to run cables for your network through a boiler room where there is a furnace and air conditioning equipment. These devices are known to cause interference. Which of the following types of cabling will have the best chance of preventing interference when working in this area?
- A.** UTP
  - B.** Fiber optic
  - C.** STP
  - D.** Coaxial
- 86.** Which of the following best describes the baseline process of securing a device within a network infrastructure?
- A.** Active prevention
  - B.** Enumerating
  - C.** Hardening
  - D.** Passive detection

- 87.** Which of the following attacks involve intercepting a session and modifying network packets? (Select the two best answers.)
- A.** TCP/IP hijacking
  - B.** Denial of service
  - C.** Man-in-the-middle attack
  - D.** DNS poisoning
  - E.** Null session
- 88.** Which of the following transport protocols and port numbers does Secure Shell use?
- A.** UDP (User Datagram Protocol) port 19
  - B.** TCP (Transmission Control Protocol) port 22
  - C.** TCP (Transmission Control Protocol) port 389
  - D.** UDP (User Datagram Protocol) port 53
- 89.** Which of the following will most likely enable an attacker to force a switch to function like a hub?
- A.** DNS spoofing
  - B.** ARP poisoning
  - C.** MAC flooding
  - D.** DNS poisoning
- 90.** Which of the following are best practices when installing and securing a new computer for a home user? (Select the three best answers.)
- A.** Install remote control software.
  - B.** Install a firewall.
  - C.** Apply service packs.
  - D.** Apply system patches.
- 91.** The IT director asks you to create a solution to protect your network from Internet-based attacks. The solution should include pre-admission security checks and automated remediation and should also integrate with existing network infrastructure devices. Which of the following solutions should you implement?
- A.** NAC
  - B.** NAT

**C. VLAN**

**D. Subnetting**

**92.** Which of the following technologies was originally designed to decrease broadcast traffic and reduce the likelihood of having information compromised by network sniffers?

**A. DMZ**

**B. VPN**

**C. RADIUS**

**D. VLAN**

**93.** A client contracts you to prevent users from accessing inappropriate websites. Which of the following technologies should you implement?

**A. NIDS**

**B. Internet content filter**

**C. Honeypot**

**D. IP proxy**

**94.** A Uniform Resource Locator (URL) is a type of Uniform Resource Identifier (URI) that specifies where an identified resource is available. When a user attempts to go to a website, she notices the URL has changed. Which attack is the most likely cause of the problem?

**A. Denial of service**

**B. ARP poisoning**

**C. DNS poisoning**

**D. DLL injection**

**95.** Which of the following would a DMZ typically contain?

**A. FTP server**

**B. SQL server**

**C. Customer account database**

**D. User workstations**

96. Which device uses stateful packet inspection?
- A. Switch
  - B. Firewall
  - C. Hub
  - D. IDS
97. Which of the following types of firewalls provides inspection of data at layer 7 of the OSI model?
- A. Network address translation
  - B. Stateful inspection
  - C. Application-proxy
  - D. Circuit-level gateway
98. What is the primary purpose of network address translation (NAT)?
- A. To hide the public network from internal hosts
  - B. To convert IP addresses into domain names
  - C. To cache web pages
  - D. To hide internal hosts from the public network
99. Which of the following threats is not associated with Bluetooth?
- A. Discovery mode
  - B. Bluesnarfing
  - C. Fraggle attack
  - D. Bluejacking
100. In a secure environment, which authentication mechanism performs better?
- A. RADIUS because it encrypts client/server passwords.
  - B. TACACS+ because it encrypts client/server negotiation dialogs.
  - C. TACACS+ because it is a remote access authentication service.
  - D. RADIUS because it is a remote access authentication service.

## Answers to Practice Exam 1

- |                      |                      |                      |                           |
|----------------------|----------------------|----------------------|---------------------------|
| <b>1.</b> A.         | <b>26.</b> A.        | <b>51.</b> B.        | <b>76.</b> B.             |
| <b>2.</b> B.         | <b>27.</b> A.        | <b>52.</b> C.        | <b>77.</b> D.             |
| <b>3.</b> C.         | <b>28.</b> C.        | <b>53.</b> D.        | <b>78.</b> A.             |
| <b>4.</b> D.         | <b>29.</b> A.        | <b>54.</b> A.        | <b>79.</b> C.             |
| <b>5.</b> C.         | <b>30.</b> C.        | <b>55.</b> C.        | <b>80.</b> D.             |
| <b>6.</b> A. and C.  | <b>31.</b> D.        | <b>56.</b> B.        | <b>81.</b> A.             |
| <b>7.</b> D.         | <b>32.</b> A.        | <b>57.</b> C.        | <b>82.</b> B.             |
| <b>8.</b> A.         | <b>33.</b> C.        | <b>58.</b> B.        | <b>83.</b> C.             |
| <b>9.</b> B.         | <b>34.</b> D.        | <b>59.</b> C.        | <b>84.</b> C.             |
| <b>10.</b> C.        | <b>35.</b> A.        | <b>60.</b> D.        | <b>85.</b> B.             |
| <b>11.</b> D.        | <b>36.</b> C.        | <b>61.</b> B.        | <b>86.</b> C.             |
| <b>12.</b> B.        | <b>37.</b> B.        | <b>62.</b> C. and D. | <b>87.</b> A. and C.      |
| <b>13.</b> C.        | <b>38.</b> C.        | <b>63.</b> C.        | <b>88.</b> B.             |
| <b>14.</b> D.        | <b>39.</b> D.        | <b>64.</b> D.        | <b>89.</b> C.             |
| <b>15.</b> B.        | <b>40.</b> B.        | <b>65.</b> A.        | <b>90.</b> B., C., and D. |
| <b>16.</b> C.        | <b>41.</b> C.        | <b>66.</b> B.        | <b>91.</b> A.             |
| <b>17.</b> D.        | <b>42.</b> D.        | <b>67.</b> B.        | <b>92.</b> D.             |
| <b>18.</b> A.        | <b>43.</b> B.        | <b>68.</b> A.        | <b>93.</b> B.             |
| <b>19.</b> A. and B. | <b>44.</b> C.        | <b>69.</b> C.        | <b>94.</b> C.             |
| <b>20.</b> B.        | <b>45.</b> D.        | <b>70.</b> D.        | <b>95.</b> A.             |
| <b>21.</b> D.        | <b>46.</b> A.        | <b>71.</b> A.        | <b>96.</b> B.             |
| <b>22.</b> A.        | <b>47.</b> B.        | <b>72.</b> C.        | <b>97.</b> C.             |
| <b>23.</b> B.        | <b>48.</b> C. and D. | <b>73.</b> D.        | <b>98.</b> D.             |
| <b>24.</b> D.        | <b>49.</b> A.        | <b>74.</b> A.        | <b>99.</b> C.             |
| <b>25.</b> B.        | <b>50.</b> B.        | <b>75.</b> B. and C. | <b>100.</b> B.            |

## Answers with Explanations

### 1. Answer: A. Malware

Explanation: Malware is software that can possibly gain access to a person's computer without that person's knowledge. It is a broad term that includes viruses, worms, spyware, and so on. Privilege escalation is the act of exploiting a bug or design flaw. Whitelists are e-mail lists that keep track of safe senders of e-mail. HIDS stands for *host-based intrusion detection system*. A HIDS might be used to prevent malware.

See the section titled "Computer Systems Security Threats" in Chapter 2, "Computer Systems Security," for more information.

### 2. Answer: B. Computer programs used to bypass normal authentication or other security mechanisms in place.

Explanation: Backdoors are used by programmers and hackers to gain access to software, operating systems, and devices without having to provide proper authentication. One example, Back Orifice, uses backdoors to enable the remote control of Windows computers. "Code inserted into software that initiates one of several types of functions when specific criteria are met" describes a *logic bomb*. "A platonic extra added to an operating system" describes an Easter egg. "A group of compromised computers" could describe a botnet, if the computers are working collectively.

See the section titled "Computer Systems Security Threats" in Chapter 2, "Computer Systems Security," for more information.

### 3. Answer: C. Spam.

Explanation: Spam e-mail can be prevented in several ways. By closing open mail relays, also known as SMTP relays, only properly authenticated users can use those e-mail servers. A virus is code that runs on a computer without the user's consent. A worm is similar to a virus except that worms can self-replicate, whereas viruses do not. A Trojan, or Trojan horse, appears to perform desired functions but performs malicious actions behind the scenes. See the section titled "Computer Systems Security Threats" in Chapter 2, "Computer Systems Security," for more information.

### 4. Answer: D. Instant messaging program sessions are open and unprotected.

Explanation: By default, most instant messaging program sessions are open and unprotected. The inbound port numbers used by these programs are well known to hackers. Although instant messaging programs quite often have no common protocol, no encryption or very weak encryption, and will often adversely affect Internet bandwidth, these issues are not as severe as the fact that instant messaging program sessions are open and unprotected.

See the section titled “Securing Other Applications” in Chapter 4, “Application Security,” for more information.

5. Answer: C. The malware could be running at a more privileged level than the computer’s antivirus software.

Explanation: By using privilege escalation, the malware can gain access to the system and possibly run at a higher privilege level than the computer’s antivirus software. One of the ways to do this is through the use of virtualization techniques.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

6. Answers: A. and C. Disabling unnecessary services and applying patches.

Explanation: When hardening an operating system, unnecessary services should be disabled, and the latest patches should be applied to operating systems and applications. Basic configurations, such as configuring the desktop, or graphics or video settings, don’t have an impact on operating system security. You want to keep the administrators group as small as possible, so it is not wise to add users to the administrators group. Enabling services should be done only if the corresponding application is indeed necessary.

See the section titled “Hardening Operating Systems” in Chapter 3, “OS Hardening and Virtualization,” for more information.

7. Answer: D. Virus.

Explanation: A virus is designed to spread from one file to another file on an individual computer. It is not designed to automatically spread from one system to another; that would be a worm. A Trojan is malicious code that appears to do something legitimate but does something illegitimate outside the view of the user. A botnet is a group of compromised computers normally known as zombies.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

8. Answer: A. Apply a baseline configuration.

Explanation: When installing 50 new computers (or any number of computers) on a network, you should first apply the baseline configuration from information and tests that you have previously collected. This will ensure that all computers comply with the same configuration. Afterward, the latest operating system updates should be installed, followed by antivirus and anti-spyware programs, and finally applications such as word processors and spreadsheet programs.

See the section titled “Hardening Operating Systems” in Chapter 3, “OS Hardening and Virtualization,” for more information.

**9. Answer: B. Security template.**

Explanation: Security templates can be applied to computers to configure many rules and policies at once. These security templates will have many rules defining group policies and are common in corporate environments. The terms hotfix and patch are often used interchangeably; they are singular updates to an operating system. Service packs are groups of updates to an operating system. Although service packs, hotfixes, and patches should be installed to operating systems, and although they might offer additional security, a security template is always used to increase the security of the workstation.

See the section titled “Hardening Operating Systems” in Chapter 3, “OS Hardening and Virtualization,” for more information.

**10. Answer: C. Java applets need to have virtual machine web browser support.**

Explanation: Web browsers must have the capability to run Java applets in a virtual machine environment. If the virtual machine browser does not have the capability to do this, the Java applet cannot function. Virtual machines isolate an operating system or a web browser to secure them. However, they need to function properly; therefore, the virtual web browser must support Java applets. Java applets can be used for various things, but not all will include a digital signature, nor will all of them be used for customized controls and icons. The answers concerning digital signatures and customized controls are absolute, whereas Java applets will have many functions. Java applets are not the same as Microsoft’s ActiveX controls.

See the section titled “Securing the Browser” in Chapter 4, “Application Security,” for more information.

**11. Answer: D. Zombie.**

Explanation: A zombie is an individual compromised computer connected to the Internet. The owner is unaware that the computer has been installed with malware. The zombie can be updated and controlled remotely from a master computer at a control center. This master computer controls the entire botnet or group of compromised computers. A virus is code that runs on a computer without the user’s knowledge, infecting files. A worm is similar to a virus but has the capability to self-replicate to other systems. Spam is unwanted, or unsolicited, e-mail.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

**12.** Answer: B. Dictionary attack.

Explanation: A dictionary attack is a type of attack used to find out passwords. It cannot be accomplished through e-mail. Viruses and Trojan horses can be sent through e-mail and commonly are.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

**13.** Answer: C. Pop-up blocker.

Explanation: Pop-up blockers are associated with web browsers. They are used to block unwanted advertisements common to many websites. Personal firewalls are software installed to an operating system to protect it from the Internet and from other networked computers. Anti-spyware programs are installed to prevent the installation of spyware. Spyware is software that tracks what a person is doing on the Internet. Service packs are collections of patches installed at one time to an operating system.

See the section titled “Securing the Browser” in Chapter 4, “Application Security,” for more information.

**14.** Answer: D. HIDS.

Explanation: HIDS, or host-based intrusion detection system, checks for unwanted or malicious activity within an operating system and within the applications on an individual workstation. RADIUS is a service used for authentication of remote users. NIDS, or network intrusion detection system, is used to monitor an entire network. OVAL, Open Vulnerability and Language Assessment, standardizes the transfer of secure data.

See the section titled “Implementing Security Applications” in Chapter 2, “Computer Systems Security,” for more information.

**15.** Answer: B. MAC flooding.

Explanation: MAC flooding is when an attacker attempts to flood the CAM table of a switch with many packets, each of which has a different source MAC address. The CAM table is an area in memory set aside to store MAC address to physical port translations. Double tagging is an attack by a host that attaches VLAN tags to the frames it transmits. Physical tampering can be done to a switch at a dedicated monitoring port; from there a person could perpetuate a variety of attacks on the network. A DoS attack is a denial of service usually associated with servers. In this type of attack, a user seeks to stop the server from functioning.

See the section titled “Network Design” in Chapter 5, “Network Design Elements,” for more information.

- 16.** Answer: C. Terminal Access Controller Access-Control System Plus.

Explanation: Terminal Access Controller Access-Control System Plus (TACACS+) uses port 49. This is an authentication protocol used to verify users' identities. The File Transfer Protocol (FTP) uses port 21. Post Office Protocol version 3 (POP3) uses port 110. The Domain Name System (DNS) uses port 53.

See the section titled "Ports and Protocols" in Chapter 6, "Networking Protocols and Threats," for more information.

- 17.** Answer: D. Kiting.

Explanation: Kiting is when a person floats a domain for up to 5 days. Domain name kiting is the process of deleting a previously registered domain name within the 5-day grace period given to the user by the domain registrar. This grace period is also known as an add grace period, or AGP. The person doing the kiting will immediately reregister the domain name for another 5-day period and continue the process until the domain name is sold for a profit. Otherwise, the person will continue to use the domain without ever paying for it. DNS poisoning is the modification of name resolution information in a DNS server's cache. Domain hijacking is the process by which the registration of a domain name is transferred without the permission of the owner. Domain spoofing is attempting to make users think that your domain is actually another one; this is commonly done with similar-looking domain names.

See the section titled "Malicious Attacks" in Chapter 6, "Networking Protocols and Threats," for more information.

- 18.** Answer: A. DMZ.

Explanation: A DMZ, or demilitarized zone, is an area in between the LAN and the Internet. Servers that are accessed by users on the Internet can do their job without the possibility of intrusion to the LAN. A VLAN is a virtual local-area network, a way of compartmentalizing the local-area network on the physical and data link layers. A VPN is a virtual private network that mimics a LAN for authentication but enables people to connect to the LAN remotely. NAT is a network address translation that translates one set of IP addresses to another.

See the section titled "Network Design" in Chapter 5, "Network Design Elements," for more information.

- 19.** Answers: A. and B. Update the Voice over IP system and use an authentication scheme.

Explanation: By keeping the Voice over IP system up to date, you can avoid a lot of the attacks that look for backdoors or other entrances to the system.

Using a strong authentication scheme that has complex passwords is the next best way to protect the system. Key systems are older types of phone systems that you would not want to employ, unless as a backup, if you have a Voice over IP system. Encryption is a good idea for Voice over IP, but it won't necessarily stop a man-in-the-middle attack; however, it will be difficult for the attacker to decrypt the information.

See the section titled "Network Design" in Chapter 5, "Network Design Elements," for more information.

**20.** Answer: B. Extranet.

Explanation: An extranet is created so that sister companies, partner companies, or clients of your organization can gain access to some of your data at your discretion. Intranets normally share information with people within your organization. A DMZ, or demilitarized zone, is an area in between the LAN and the Internet that stores servers. A DMZ might be used with an extranet, but it is not necessary. A VLAN is a virtual local-area network that groups computers virtually by port or by a MAC address.

See the section titled "Network Design" in Chapter 5, "Network Design Elements," for more information.

**21.** Answer: D. Stateful packet inspection.

Explanation: A firewall running stateful packet inspection is normally not vulnerable to IP spoofing attacks because it examines the header in each packet. This type of packet inspection can distinguish between legitimate and illegitimate packets. Stateless packet filtering does not retain a memory of packets that pass through the firewall and, because of this, is vulnerable to IP spoofing attacks. Circuit-level gateway firewalls apply security mechanisms when TCP or UDP connections are established but do not examine the headers of the packets themselves. NAT filtering filters out traffic according to TCP or UDP ports.

See the section titled "Firewalls and Network Security" in Chapter 7, "Network Perimeter Security," for more information.

**22.** Answer: A. Replay attack.

Explanation: A replay attack is a network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. Attackers often use packet sniffers to intercept the data and then retransmit later. This differs from session hijacking or TCP/IP hijacking in that the original session is simply being intercepted and analyzed for later use. A backdoor is a way of accessing a server or device without being authenticated properly. A man-in-the-middle (MITM) attack is a form of eavesdropping that intercepts all data between a client and a server.

See the section titled “Malicious Attacks” in Chapter 6, “Networking Protocols and Threats,” for more information.

- 23.** Answer: B. HTTP proxy.

Explanation: An HTTP proxy caches information from a web server for a set amount of time. This way an organization can save bandwidth, and the users can get their web pages quicker. An HTTP proxy is also known as a caching proxy. An IP proxy secures a network by keeping the computers behind it anonymous, usually through the use of network address translation. A firewall protects a network from external attack. A DMZ, or demilitarized zone, is an area between the LAN and the Internet used to store servers that serve information to Internet users.

See the section titled “Firewalls and Network Security” in Chapter 7, “Network Perimeter Security,” for more information.

- 24.** Answer: D. A#password123.

Explanation: A#password123 is the strongest password because it uses uppercase and lowercase characters, numeric characters, and a special character and is the longest password listed. password has none of those complexity requirements. Apassword has an uppercase character. Apassword123 has an uppercase character and numeric characters; however, the word “password” should never be used in a password, even if additional complexity requirements have been met. It is one of those words that is easy for dictionary attacks and brute-force attacks to uncover.

See the section titled “Securing Wired Networks and Devices” in Chapter 8, “Securing Network Media and Devices,” for more information.

- 25.** Answer: B. Weak encryption.

Explanation: WEP is a deprecated standard. Its encryption level is weak. Using WPA or WPA2 instead to protect wireless networks is recommended. The SSID broadcast functions regardless of the type of encryption protocol used on the wireless network; however, disabling the SSID broadcast is important after all clients have been connected to the wireless access point. Data emanation (also known as signal emanation) is an electromagnetic field generated by devices and cables. If nothing else is available, you should use WEP. This will at least offer some level of protection against war-driving attacks; it is better than using no encryption whatsoever.

See the section titled “Securing Wireless Networks” in Chapter 8, “Securing Network Media and Devices,” for more information.

**26.** Answer: A. SYN attack.

Explanation: The SYN attack (or SYN flood) is a type of DoS attack in which an attacker sends a large amount of SYN (synchronize) request packets to a server in an attempt to deny service. The man-in-the-middle attack is a form of eavesdropping that intercepts all data between the client and the server relaying that information back and forth. The teardrop attack is a type of denial of service that sends mangled IP fragments with overlapping and oversized payloads. A Smurf attack is a type of denial of service that sends large amounts of ICMP echoes, broadcasting those requests to every computer on the network.

See the section titled “Malicious Attacks” in Chapter 6, “Networking Protocols and Threats,” for more information.

**27.** Answer: A. NIDS.

Explanation: NIDS, or network intrusion detection system, cannot proactively detect computer anomalies. It is deployed to the entire network and looks for a network intrusion, not intrusions to individual computers. HIPS (host-based intrusion prevention system), antivirus software, and personal software firewalls can all be loaded on an individual computer and can be updated as well. These can proactively detect computer anomalies.

See the section titled “NIDS Versus NIPS” in Chapter 7, “Network Perimeter Security,” for more information.

**28.** Answer: C. HTTP.

Explanation: HTTP (Hypertext Transfer Protocol) transmits data between a web server and a web browser. It uses addresses such as <http://www.comptia.org>. IMAP is the Internet Message Access Protocol. It is the second most used e-mail protocol for e-mail retrieval next to POP3. SSH is the Secure Shell protocol, used to remotely control computers in a secure fashion. FTP is the File Transfer Protocol; it is used to move files back and forth between computers.

See the section titled “Ports and Protocols” in Chapter 6, “Networking Protocols and Threats,” for more information.

**29.** Answer: A. Role-based access control.

Explanation: Role-based access control (RBAC) works with sets of permissions; each set of permissions constitutes a role. Users are assigned to roles to gain access to resources. Examples of user groups that are assigned to roles include remote users, extranet users, guests, and so on. In this question, the remote users are the group that has been assigned a role that enables them to access the network only during normal business hours. This should not be confused with a rule-based access control that is a type of mandatory access

control. Mandatory access control (MAC) is an access control policy determined by a computer system and not by a user or owner. Discretionary access control (DAC) is generally determined by the owner of a resource.

See the section titled “Access Control Models Defined” in Chapter 10, “Access Control Methods and Models,” for more information.

**30. Answer: C. Access control lists.**

**Explanation:** Access control lists (ACLs) are used in the discretionary access control (DAC) model to identify users’ permissions to resources. This is common in the Windows client/server networks. By default, the owner assigns permissions to resources. Role-based access control (RBAC) defines the roles that users have in an organization that are based on sets of predefined permissions. Predefined access privileges can be found in mandatory access control (MAC) and RBAC models. Security labels are used in MAC.

See the section titled “Access Control Models Defined” in Chapter 10, “Access Control Methods and Models,” for more information.

**31. Answer: D. Principle of least privilege.**

**Explanation:** The principle of least privilege requires that any users or portions of the program must be able to access only such information and resources necessary to accomplish the goal without accessing any other information or resources. Implicit deny is a concept that denies all traffic to a resource unless a user is specifically granted access to the resource; it is a default setting in many operating systems. Mandatory access control (MAC) is a type of access control model that has permissions set by the system and uses labels for object permissions. Separation of duties is when more than one person is required to complete a particular task or operation.

See the section titled “Access Control Models Defined” in Chapter 10, “Access Control Methods and Models,” for more information.

**32. Answer: A. Kerberos.**

**Explanation:** Kerberos is an authentication protocol that enables computers to prove their identity to each other in a secure manner; it is quite often used in a client/server environment such as a Microsoft domain. Kerberos is the only answer listed that uses a Key Distribution Center. It uses two-way authentication, otherwise known as mutual authentication. RADIUS is used to provide centralized administration of dial-up VPN and wireless authentication. TACACS+ is another remote authentication protocol; however, it is used more often in Unix networks. PKI stands for public-key infrastructure, which is an entire system of parts, people, computers, and protocols all working together to encrypt data.

See the section titled “Authentication Models and Components” in Chapter 9, “Physical Security and Authentication Models,” for more information.

**33.** Answer: C. Discretionary access control.

Explanation: Discretionary access control is an access control policy generally determined by the owner. Objects such as files and printers can be created and accessed by the owner, and the owner decides which users are allowed to have access to the objects. Mandatory access control and role-based access control models are controlled by the system, not by the owner of a resource. CRL stands for certificate revocation list. This deals with the revoking of compromised encryption certificates within a public-key infrastructure.

See the section titled “Authentication Models and Components” in Chapter 9, “Physical Security and Authentication Models,” for more information.

**34.** Answer: D. Multifactor.

Explanation: Multifactor authentication is when two or more types of authentication are used when dealing with user access control. Biometrics is the science of recognizing humans based on one or more physical characteristics; the thumbprint scan would be one example of this. Smartly designed networks use biometrics with something a user knows, to create a secure or multifactor authentication scheme. The three-way handshake has to do with the creation of TCP sessions and networking. Mutual authentication, or two-way authentication, is when a client computer and server computer both verify each other’s identity.

See the section titled “Authentication Models and Components” in Chapter 9, “Physical Security and Authentication Models,” for more information.

**35.** Answer: A. SSO.

Explanation: SSO, or single sign-on, is when a user can log in one time to gain access to multiple systems without being asked to log in again. This allows the user to access two different sets of resources without having to log in several times. Two-factor authentication means that two different types of identity are required to gain access to a system or building. Two examples of this could be biometrics and smart cards but could also include passwords, pin numbers, and so on.

See the section titled “Authentication Models and Components” in Chapter 9, “Physical Security and Authentication Models,” for more information.

**36.** Answer: C. 88.

Explanation: Kerberos uses inbound port 88 by default. An example of this would be a Microsoft domain controller that accepts incoming logins. Kerberos

is a type of mutual authentication. Port 21 is used by FTP. Port 80 is used by HTTP. Port 389 is used by the Lightweight Directory Access Protocol (LDAP).

See the section titled “Authentication Models and Components” in Chapter 9, “Physical Security and Authentication Models,” for more information.

- 37.** Answer: B. Logical token.

Explanation: Physical smart cards incorporate logical tokens. They fall into the category of something a person has. Password policies, usernames, and passwords are all part of the access control methods known as logging in. Access control lists are used to allow or deny traffic to pass through a firewall or permit or deny users to access resources.

See the section titled “Physical Security” in Chapter 9, “Physical Security and Authentication Models,” for more information.

- 38.** Answer: C. Kerberos.

Explanation: Kerberos is an authentication protocol commonly used on client/server networks. The server works with tickets that prove the identity of users. The tickets are obtained from a ticket-granting server, which is part of the Key Distribution Center. Kerberos is generally used within a local network; the rest of the answers deal with remote authentication. PAP and CHAP are types of authentication schemes used within remote access service, although PAP is not secure. RADIUS is another type of remote authentication service, but this provides centralized administration for authentication.

See the section titled “Authentication Models and Components” in Chapter 9, “Physical Security and Authentication Models,” for more information.

- 39.** Answer: D. Identification.

Explanation: Identification is the phase in which identity proofing occurs. Identity proofing is an initial validation of an identity. Authentication happens afterward, granting access to a network or building. Then authorization occurs when a person is approved access to specific resources. Verification of identification is important within authentication schemes; for example, a security guard may be required to run checks of employees’ IDs.

See the section titled “Physical Security” in Chapter 9, “Physical Security and Authentication Models,” for more information.

- 40.** Answer: B. 3389.

Explanation: Port 3389 is the inbound port used by the Remote Desktop Protocol. It is implemented on Microsoft systems as either Remote Desktop Services or the older Microsoft Terminal Services. If this port is open, it enables

a remote user to log in to the computer. Port 53 is used by DNS. Port 389 is used by LDAP. Port 636 is used by secure LDAP.

See the section titled “Authentication Models and Components” in Chapter 9, “Physical Security and Authentication Models,” for more information.

- 41.** Answer: C. Items not specifically given access are denied by default.

Explanation: If a user or group of users does not have permissions to gain access to a resource, many systems will deny access by default; this is known as implicit deny and is common in firewalls and Windows operating systems. Default access control lists, or ACLs, will be set up for implicit deny and remain that way unless they are changed. ACLs are not a secure way of moving traffic, but rather they are a secure way of permitting or denying traffic to pass through a firewall or permitting or denying a user or group of users access to resources. Implicit deny does not deny all traffic, only traffic that has not been previously allowed.

See the section titled “Access Control Models Defined” in Chapter 10, “Access Control Methods and Models,” for more information.

- 42.** Answer: D. John the Ripper.

Explanation: John the Ripper is a password-cracking tool, otherwise known as a password analysis or recovery tool; it all depends on who uses the tool. This particular tool can do dictionary attacks, brute-force attacks, and cryptanalysis attacks on passwords. AirSnort is a wireless network finder. Nessus is a vulnerability scanner, and Wireshark is a protocol analyzer, otherwise known as a network sniffer.

See the section titled “Assessing Vulnerability with Security Tools” in Chapter 11, “Vulnerability and Risk Assessment,” for more information.

- 43.** Answer: B. Identify organizational assets.

Explanation: When you first perform a risk assessment, you need to know exactly what you are assessing. Organizational assets can include firewalls, servers, and other computers and devices. These need to be identified first before you can identify vulnerabilities and threats. Last on the list when assessing risk is to identify potential monetary impact, which can be done in a qualitative or quantitative manner.

See the section titled “Conducting Risk Assessments” in Chapter 11, “Vulnerability and Risk Assessment,” for more information.

- 44.** Answer: C. Determine the potential monetary costs related to a threat.

Explanation: During impact assessment, you want to know what kind of impact a threat can have, and potential monetary costs are a big portion of

that impact on an organization. During this stage you do not assess potential threats, or how likely it is that a threat might occur. You do not assess how well the organization is prepared to manage the threat. You are more interested in monetary impact and the impact on servers; for example, loss of data availability and the impact on employees.

See the section titled “Conducting Risk Assessments” in Chapter 11, “Vulnerability and Risk Assessment.”

**45. Answer: D. Performance monitoring software.**

Explanation: Use performance monitoring software to monitor for any changes to your system baseline. CPU spikes, higher levels of hard drive access, and other objects within your server performing other than normal can be detected by the performance monitoring software. Key management software manages the deployment of encrypted keys and certificates. Resource planning software is for planning for fault tolerance and disaster recovery. Antivirus software protects and prevents against malware attack.

See the section titled “Using Tools to Monitor Systems and Networks” in Chapter 12, “Monitoring and Auditing,” for more information.

**46. Answer: A. Protocol analyzer.**

Explanation: Protocol analyzers capture packets of information for later analysis. Any packets that pass through a network adapter can be captured and analyzed with a protocol analyzer, also known as a network sniffer. Penetration testers evaluate the security of a system by simulating one or more attacks on that system. Vulnerability scanners will look for vulnerabilities to servers and other network devices. Examples of vulnerability scanners include web scanners, ping scanners, and so on.

See the section titled “Assessing Vulnerability with Security Tools” in Chapter 11, “Vulnerability and Risk Assessment.”

**47. Answer: B. Network scanner.**

Explanation: Network scanners, including port scanners and vulnerability scanners, can find the open ports on your network or on individual devices. You can program vulnerability scanners such as Nessus to scan the entire network. Performance monitoring programs monitor the hardware and software of a server. Protocol analyzers capture packets of information. Cain & Abel is a password-cracking program.

See the section titled “Assessing Vulnerability with Security Tools” in Chapter 11, “Vulnerability and Risk Assessment,” for more information.

- 48.** Answers: C. and D. Network mapper and protocol analyzer.

Explanation: Some network mapping programs such as AirMagnet require that a network adapter be placed in promiscuous mode. This is when the network adapter captures all packets that it has access to regardless of the destination of those packets. Some protocol analyzers (for example, Wireshark) also require that a network adapter be placed in promiscuous mode. Password crackers, port scanners, and other vulnerability scanners do not require promiscuous mode.

See the section titled “Using Tools to Monitor Systems and Networks” in Chapter 12, “Monitoring and Auditing,” for more information.

- 49.** Answer: A. Wireshark.

Explanation: Wireshark is a protocol analyzer that can be freely downloaded from the Internet. It is used to capture packets for later analysis. John the Ripper and Cain & Abel are password-cracking programs. Nessus is a vulnerability scanner.

See the section titled “Using Tools to Monitor Systems and Networks” in Chapter 12, “Monitoring and Auditing,” for more information.

- 50.** Answer: B. Protocol analyzer.

Explanation: Protocol analyzers can be used to check for clear-text passwords. If a password is sent by a client computer (for example, from Outlook Express), it will be sent by default as clear text. A protocol analyzer can look inside packets to locate clear-text passwords. Password-cracking programs are used to analyze, recover, or crack passwords. Port scanners are used to find open vulnerabilities in the form of open ports on servers and other network devices. A performance monitor is used to analyze the performance of a server through monitoring the CPU, RAM, hard drive, and so on.

See the section titled “Using Tools to Monitor Systems and Networks” in Chapter 12, “Monitoring and Auditing,” for more information.

- 51.** Answer: B. Firewall log.

Explanation: The firewall log can help to find out whether files are being illegitimately copied to an external location. This is the only log listed that can give you any information about files being copied to an external or remote location. DNS logs can find out whether unauthorized zone transfers or DNS poisoning has occurred. Antivirus logs show what viruses have been detected and quarantined on a system. The System log is a log file within the event viewer that provides information about the operating system and device drivers.

See the section titled “Conducting Audits” in Chapter 12, “Monitoring and Auditing,” for more information.

**52.** Answer: C. Algorithms.

Explanation: Algorithms, or ciphers, are what most current encryption methods are based on. Regardless of whether the encryption type is symmetric (AES, RC4) or asymmetric (RSA, Diffie-Hellman), the encryption rests on the mathematics or algorithm. The two core parts of an encryption scheme include the algorithm and the key. PKI, which stands for public-key infrastructure, is an entire set of hardware, software, policies, procedures, and people that creates and distributes digital certificates. Timestamps are used in various technologies, including the hashing of files; this helps with the integrity of the file. DRM, which stands for Digital Rights Management, is a type of encryption placed on media such as MP3s.

See the section titled “Cryptography Concepts” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**53.** Answer: D. Steganography.

Explanation: Steganography is the science and art of writing hidden messages. It is a form of security through obscurity. The goal is that no one aside from the sender and receiver should even suspect that a hidden message exists. Although it can come in different forms, it is most commonly found in image files. Confidentiality means preventing the disclosure of information to unauthorized persons. By definition, cryptography is the practice and study of hiding information. In computer science, cryptography uses encryption to hide information and make it secret, whereas steganography, if accomplished correctly, does not imply that a hidden message even exists. If a person were to see an encrypted cryptographic message, they know it for what it is and may try to crack it. A digital signature authenticates a document or e-mail, letting the recipient know that the document was created and sent by the actual sender and not someone else.

See the section titled “Cryptography Concepts” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**54.** Answer: A. Asymmetric.

Explanation: Asymmetric systems such as PKI (public-key infrastructure) have a complicated centralized key management scheme. A system such as PKI creates a symmetric key pair that includes a public key and a private key. The private key is kept secret, whereas the public key can be distributed. Symmetric systems use two keys, but they are the same type of key, usually identical, thus the name symmetric. Whole disk encryption schemes such as BitLocker use trusted platform modules (TPMs) that store the symmetric encrypted keys; these keys are often based on the Advanced Encryption Standard (AES). Steganography is the science of hiding messages within files and doesn’t use keys.

See the section titled “Cryptography Concepts” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

- 55.** Answer: C. Public and private keys.

Explanation: A CRL, or certificate revocation list, stores revoked certificates that contain both public and private keys associated with the certificate. This is common within a PKI, which is asymmetric, using private and public keys. TPMs, trusted platform modules, use one type of key, usually secret and private.

See the section titled “Public Key Infrastructure” in Chapter 14, “PKI and Encryption Protocols,” for more information.

- 56.** Answer: B. Public key.

Explanation: A public key must be presented by the user to the certificate authority (CA) to obtain a certificate and gain access to things such as secure websites. The private key is stored by the CA and is part of the key pair. Passwords are not necessary to obtain a certificate. Users cannot provide authentication; however, they can provide identification that helps authenticate them to the CA.

See the section titled “Public Key Infrastructure” in Chapter 14, “PKI and Encryption Protocols,” for more information.

- 57.** Answer: C. Symmetrical encryption.

Explanation: Symmetrical encryption is also referred to as secret key encryption, shared key, private key, single key, and even session key. Asymmetrical encryption uses private and public key pairs, only one of which is secret. A one-way function is easy to compute when being generated but difficult or impossible to compute in reverse. Quantum encryption, also known as quantum cryptography, uses quantum mechanics to guarantee secure communications. It enables two parties to produce a shared, random-bit string, known only to them, that encrypts and decrypts messages.

See the section titled “Cryptography Concepts” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

- 58.** Answer: B. RSA.

Explanation: RSA is the asymmetric cryptographic algorithm used by TLS (Transport Layer Security) to establish a session key. TLS is the successor to SSL (Secure Sockets Layer) that can use RSA or Diffie-Hellman for key exchange as well as AES and RC4 for the encryption of the rest of the session. HTTPS is the web-based secure protocol that makes use of TLS (or SSL), which then makes use of RSA for the key exchange at the start of a session.

See the section titled “Encryption Algorithms” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**59.** Answer: C. RA.

Explanation: An RA is a registration authority used to verify requests for certificates from a certificate authority or multiple certificate authorities. A CRL is a certificate revocation list; if for some reason a certificate cannot be verified by any parties involved and the issuer of the certificate confirms this, the issuer needs to revoke the certificate. The certificate is placed in the CRL that is published. Key escrow is when certificates are held if the third parties need them in the future. Recovery agents recover certificates that were corrupted or lost.

See the section titled “Public-Key Infrastructure” in Chapter 14, “PKI and Encryption Protocols,” for more information.

**60.** Answer: D. Session.

Explanation: The session layer, layer 5 of the OSI model, is where SSL provides encryption. Though it is considered to be an application layer protocol, the actual encryption happens at layer 5. The transport layer deals with ports used by sessions; for example, an SSL session will use port 443. The network layer transmits the actual packets of information from one IP address to another. SSL relies on a PKI to obtain and validate certificates (for example, when you go to a secure e-commerce website).

See the section titled “Security Protocols” in Chapter 14, “PKI and Encryption Protocols,” for more information.

**61.** Answer: B. Phishing.

Explanation: Phishing is the attempt to fraudulently obtain private information. Usually the phisher masquerades as someone else. A hoax is an attempt at deceiving people into believing something that is false. Dumpster diving is when a person literally scavenges for private information in the garbage. Shoulder surfing is when a person uses direct observation to find out a target password and other personally identifiable information.

See the section titled “Social Engineering” in Chapter 16, “Policies, Procedures, and People,” for more information.

**62.** Answers: C. and D. Provide an appropriate ambient temperature, and maintain appropriate humidity levels.

Explanation: The HVAC system’s primary responsibilities are to provide an appropriate ambient temperature for the equipment and to maintain appropriate humidity levels. This keeps the equipment from overheating and prevents

electrostatic discharge (ESD). Some HVAC equipment needs to be shielded to reduce electromagnetic interference (EMI) after it is installed. Isolation can be provided by other methods such as the material used in the perimeter of the room (for example, physical firewalls). A separate ventilation system can be installed to vent fumes away from the server room; however, there shouldn't be any fumes. Products that contain fumes should be stored in a separate and specially secured area. And if a fire were to occur, the sprinkler system or special hazards system should end that threat, eliminating any fumes that were a result of the fire.

See the section titled “Environmental Controls” in Chapter 16, “Policies, Procedures, and People,” for more information.

- 63.** Answer: C. Obtain a binary copy of the system.

Explanation: A forensics investigator should first make a copy of the system and store it in a safe place, in case the system fails while the forensics investigation is carried out. Afterward, the forensics analysis might include the analysis of temporary files, and other files as well, running antivirus scans, and possibly searching for spyware. The forensics investigator will have a specific list of rules to go by when investigating what an attacker did.

See the section titled “Legislative and Organizational Policies” in Chapter 16, “Policies, Procedures, and People,” for more information.

- 64.** Answer: D. Chain of custody.

Explanation: Chain of custody is the chronological documentation or paper trail of evidence. Change management is a structured way of changing the state of a computer network or IT procedure. Job rotation is used to increase user insight and skill level and increase security. Due diligence is the ensuring that IT infrastructure risks are known and managed.

See the section titled “Legislative and Organizational Policies” in Chapter 16, “Policies, Procedures, and People,” for more information.

- 65.** Answer: A. Hot site.

Explanation: A hot site is a backup site that can be running within hours, perhaps immediately. It contains computers, phones, servers, and a complete backup of the data so that employees can begin working immediately when they enter the hot-site building. This is sometimes referred to as a hot-backup site. Cold sites do not have a complete copy of the network infrastructure, and as such it could take a few days or up to a week to get a cold site up and running. Redundant servers are a fault-tolerant method. If the redundant servers are in the same server room, a disaster will make them all nonfunctional. Tape backup is important and should be stored offsite in case of a disaster. A hot site

should have a complete backup of all data, preferably copies of the exact servers, ready to go at a moment's notice. A complete backup of all data on tape is not acceptable for a hot site because the amount of data that an organization might have on tape could take days to restore.

See the section titled “Disaster Recovery Planning and Procedures” in Chapter 15, “Redundancy and Disaster Recovery,” for more information.

**66.** Answer: B. RAID.

Explanation: RAID (redundant array of inexpensive disks) is a way to make data fault-tolerant. The best example would be to use **RAID 5** or **RAID 1**. **RAID 5** will have minimal downtime if data failure occurs; **RAID 1** should have a zero downtime if data failure occurs. A redundant server might or might not offer all the data fault tolerance that you want; it depends on how it is configured. A UPS should be installed to protect from power outages but cannot protect from a hard drive error.

See the section titled “Redundancy Planning” in Chapter 15, “Redundancy and Disaster Recovery,” for more information.

**67.** Answer: B. SLA.

Explanation: An SLA, service-level agreement, is the part of a service contract in which the level of service is formally defined. This might include traffic performance guarantees, restoration guarantees, and minimum downtime guarantees. A chain of custody is the chronological documentation of evidence. DRP stands for disaster recovery plan, which includes contact information, determination of impact, a recovery plan, and so on. Incident response procedures are sets of procedures that an investigator will use when examining a computer security incident. They might include the identification of the incident, containment, evidence gathering, investigation, eradication, recovery, and documentation and monitoring.

See the section titled “Legislative and Organizational Policies” in Chapter 16, “Policies, Procedures, and People,” for more information.

**68.** Answer: A. Privilege escalation.

Explanation: Privilege escalation is when typical users gain access to systems and devices that they normally should not have access to. This can occur on many levels but is generally used to gain administrative access to a system. Backdoors are used in computer programs to bypass normal authentication. This was originally done as a legitimate way of accessing an application but later became a vulnerability that attackers would exploit. Trojan horses are examples of malware that appear to be doing legitimate things on a system, while

in the background malicious activity is attempted. Brute force is a type of password attack.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security.”

- 69.** Answer: C. Cell phones.

Explanation: Cell phones cannot obtain a signal within a Faraday cage because of the cage’s shielding. In addition, if a cell phone is used outside the Faraday cage, the signal emanation cannot pass through the cage to the inside. The Faraday cage is meant to block signal or data emanations through the air. USB flash drives, uninterruptible power supplies, and wired keyboards do not use the air to transmit their data.

See the section titled “Securing Wired Network and Devices” in Chapter 8, “Securing Network Media and Devices,” for more information.

- 70.** Answer: D. It is a replication mechanism, activation mechanism, and has an objective.

Explanation: Computer viruses are code that acts as a replication mechanism, replicating from file to file. They are activated by users who execute the virus. Viruses have an objective, which could be one of many malicious functions. Viruses do not propagate from computer to computer, but worms do. Viruses are not search or learning mechanisms either.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

- 71.** Answer: A. Define a security policy.

Explanation: When creating a security baseline, you should first define what the security policy will be for the organization. The organization might already have a policy written and expected to be enforced. After a security policy is created, perform vulnerability testing and mitigate risks by installing software patches, uninstalling applications, disabling unnecessary services, and so on.

See the section titled “Hardening Operating Systems” in Chapter 3, “OS Hardening and Virtualization,” for more information.

- 72.** Answer: C. Apply updates and patches.

Explanation: By applying updates and patches to the web server, you decrease the amount of vulnerabilities on that server. You need to keep up to date with all the latest hotfixes and patches for your applications and operating systems. This is generally the best way to reduce vulnerabilities on any system or device.

Enabling auditing and reviewing log files is a smart idea, but it is not proactive. DNS uses port 53, but regardless the web server doesn't actually deal with DNS. A separate DNS server redirects clients to the web server. Packet sniffing is important when checking for vulnerabilities but is not the best way to reduce vulnerabilities; instead, it is a good way to find vulnerabilities. However, 24/7 packet sniffers that run all day can be resource-intensive and are not usually recommended.

See the section titled "Hardening Operating Systems" in Chapter 3, "OS Hardening and Virtualization," for more information.

- 73.** Answer: D. Verify that virtual machines have the latest service packs and patches installed.

**Explanation:** One of the most important security precautions you can take is to install the latest service packs and patches. This concept applies to regular operating systems, applications, and virtual machines. It is unnecessary for virtual machines to be multihomed because this will not increase their security. Penetration testing should be completed before the virtual machines have been implemented. Subnetting is not necessary for virtual machines, although it can increase security. Subnetting should be taken into account during the planning and implementation stage.

See the section titled "Virtualization Technology" in Chapter 3, "OS Hardening and Virtualization," for more information.

- 74.** Answer: A. Open relay.

**Explanation:** An open relay is an invitation for attackers to send out spoofed e-mails and spam. These relays should be closed on SMTP servers so that only authenticated users can gain access to them. Web proxies are go-betweens for clients on the network and the web servers that they want to connect to. The web proxy stores web page information so that the organization can save Internet bandwidth and the clients can get their information faster. Session hijacking is the exploitation of a computer session in an attempt to gain unauthorized access to data services or other resources on the computer. Logic bombs are code that has in some way been inserted into software, initiating malicious functions when specific criteria are met.

See the section titled "Computer Systems Security Threats" in Chapter 2, "Computer Systems Security," for more information.

- 75.** Answers: B. and C. Extract confidential information, and hide evidence of an attacker's presence.

**Explanation:** Rootkits in general are designed to gain administrator access while not being detected. Kernel-level rootkits will change code within the

operating system and possibly device drivers, enabling the attacker to execute with the same privileges as the operating system. This type of rootkit allows for unrestricted security access.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

**76.** Answer: B. Patch.

Explanation: A patch or hotfix is designed to fix one security issue on a computer. Service packs fix multiple security issues and update the system in other ways. Patch management is the disbursement and monitoring of patches installed to multiple computers. A configuration baseline is a set of information about a particular process on a computer; it is what is used to compare future performance analyses.

See the section titled “Hardening Operating Systems” in Chapter 3, “OS Hardening and Virtualization,” for more information.

**77.** Answer: D. Privilege escalation.

Explanation: Privilege escalation is the act of gaining a higher level of access to resources. It is sometimes done by using the local system account in Windows. Privilege escalation is a method of attack, whereas Trojans, spyware, and spam are types of malware.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

**78.** Answer: A. Enable Windows automatic updates.

Explanation: By turning on automatic updates in Windows, the server can be configured to continually download and install hotfixes. This maintains the solution, and does so with a minimal amount of effort. However, this might not be the best solution in production or mission-critical environments. A third-party patch management system requires more time and money. A security template is a good idea for Windows servers because it applies many security policies, but this cannot help to keep the system up to date as far as hotfixes are concerned. You need to install the latest service pack, but this is also a static solution; it does not continually download and install hotfixes.

See the section titled “Hardening Operating Systems” in Chapter 3, “OS Hardening and Virtualization,” for more information.

**79.** Answer: C. Install a pop-up blocker.

Explanation: Pop-up blockers are the most-effective way to prevent adware. Adware consists of the advertisements that pop up on your screen when you

go to particular websites. Pop-up blockers are generally installed as add-ons to your web browser and are most often associated with the browser. Antivirus programs protect the computer from various types of malware. In some cases they include a pop-up blocker, but not always. The best way to be sure is to install a separate pop-up blocker directly into the web browser. Host-based intrusion detection systems look for attackers in particular types of attacks that might not stop pop-ups. A firewall blocks intrusions and closes off any open ports but does not detect pop-ups.

See the section titled “Securing the Browser” in Chapter 4, “Application Security,” for more information.

**80.** Answer: D. Removal of PII data.

Explanation: Personally identifiable information (PII) and other sensitive data can easily be removed from the network through the use of USB flash drives and other similar removable media. This is the most important threat you need to be aware of that could increase due to the use of these devices. Although new data on the network might be introduced, or business data might be lost, the most common threat when USB flash drives are available is the removal of PII data. A loss of a wireless connection will be rare but possible if the USB flash drive has a special type of malware installed on it. Generally, companies disable USB access on the computer either within the operating system or within the BIOS if they are concerned about the removal of PII data.

See the section titled “Securing Computer Hardware, Peripherals, and Mobile Devices” in Chapter 2, “Computer Systems Security,” for more information.

**81.** Answer: A. Trojan horse.

Explanation: A Trojan horse disguises itself as a legitimate program but conducts malicious activity behind the scenes. Logic bombs are code designed to set off at a particular time. They may set off viruses or worms that can cause additional damage to the system. The only one of the answers that actually disguises itself is a Trojan horse.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

**82.** Answer: B. Tracking cookie.

Explanation: Tracking cookies track where a user has been on the Internet. Spyware misuses this to report on a user’s activities in many malicious ways. The spyware might open additional advertising websites, share information with third parties, or lead the user to additional malicious websites.

See the section titled “Securing the Browser” in Chapter 4, “Application Security,” for more information.

**83.** Answer: C. Rootkit.

Explanation: A rootkit subverts an operating system by altering system processes and Registry entries. This can enable the attackers to hide the presence of their malicious code. Worms are similar to viruses except that they self-replicate across the network. Logic bombs are pieces of code set to go off at a certain time. Trojans are a type of malware that disguises itself as a legitimate program.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

**84.** Answer: C. 172.16.1.1/16.

Explanation: The IPv4 address 172.16.1.1/16 is a Class B private IP address. It is within the Class B range of 128 to 191. The /16 simply tells us the amount of bits masked within the subnet mask for that IP. /16 equates to 11111111. 11111111.00000000.00000000 or 255.255.0.0. For a Class B IP address such as 172.16.1.1, this is the default subnet mask. 10.254.254.1 would normally be Class A, but the /16 in this case makes it classless; it effectively makes what would usually be a Class A address function as a Class B address. 192.168.1.1 would normally be Class C, but the /16 makes it classless as well. 169.254.50.1 would normally be an APIPA Class B private address, but the /24 makes it classless, effectively functioning as a Class C address. You need to use private IP addresses for your internal network to keep them secure and separate from the Internet.

See the section titled “Network Design” in Chapter 5, “Network Design Elements,” for more information.

**85.** Answer: B. Fiber optic.

Explanation: Fiber-optic cable does not suffer from electromagnetic interference the way that copper cabling does. UTP is unshielded twisted-pair, STP is shielded twisted-pair, and both of these are copper-based. Although STP gives better protection against EMI than UTP does, it is not nearly as effective as fiber-optic cable simply because fiber-optic cable does not rely on electricity. Coaxial cable may or may not have a shield and will rarely be used for running network lines.

See the section titled “Securing Wired Networks and Devices” in Chapter 8, “Securing Network Media and Devices,” for more information.

**86.** Answer: C. Hardening.

Explanation: The hardening of computers and network devices is part of the baseline process of securing those devices. Active prevention can refer to network intrusion prevention systems that have not yet been hardened. Enumerating is the listing of possible security threats. Passive detection can refer to network intrusion detection systems that have not yet been hardened.

See the section titled “Securing Wired Networks and Devices” in Chapter 8, “Securing Network Media and Devices,” for more information.

**87.** Answers: A. and C. TCP/IP hijacking and man-in-the-middle attack.

Explanation: TCP/IP hijacking and man-in-the-middle attacks are both examples of attacks that involve intercepting a user’s session and modifying network packets. TCP/IP hijacking is when a hacker takes over a TCP session between two computers without the need of a cookie. Man-in-the-middle attacks intercept all data between the client and the server; if successful all communications now go through the MITM attacking computer. These are both types of hijacking; other types of hijacking include session theft and blind hijacking. Denial of service is a broad term given to many different types of network attacks including flood attacks, Smurf, Fraggle, and SYN Flood. DNS poisoning is the modification of name resolution information located in a DNS server’s cache. A null session is a connection to the Windows interprocess communications share (IPC\$); it exploits NetBIOS connections.

See the section titled “Malicious Attacks” in Chapter 6, “Networking Protocols and Threats,” for more information.

**88.** Answer: B. TCP (Transmission Control Protocol) port 22.

Explanation: Secure Shell (SSH) uses port 22 and by default makes its connections via TCP. Port 19 is used by CHARGEN, port 389 is used by LDAP, and port 53 is used by DNS.

See the section titled “Ports and Protocols” in Chapter 6, “Networking Protocols and Threats,” for more information.

**89.** Answer: C. MAC flooding.

Explanation: MAC flooding sends many packets to a switch, each of which has a different source MAC address in an attempt to use up the memory on the switch, changing the state of the switch to fail open mode, which ultimately makes it function as a hub. Spoofing attacks are when an attacker masquerades as another person, which can be done with DNS, websites, e-mail, and so on. ARP poisoning is an attack that exploits Ethernet networks that may enable an attacker to sniff frames of information or modify that information. DNS

poisoning is the modification of name resolution information that should be within a DNS server's cache.

See the section titled “Malicious Attacks” in Chapter 6, “Networking Protocols and Threats,” for more information.

- 90.** Answers: B., C., and D. Install a firewall, apply service packs, and apply system patches.

Explanation: Firewalls, service packs, and system patches should always be installed to a new computer to secure it before the user starts working with it. Remote control software should not be installed because this creates an entrance to the user's computer that is not necessary.

See the section titled “Firewalls and Network Security” in Chapter 7, “Network Perimeter Security,” for more information.

- 91.** Answer: A. NAC.

Explanation: NAC, or network access control, makes security checks of the users or the actual connections that are made before sessions are initiated. It can also remediate issues automatically if configured properly. Examples of network access control include 802.1X and FreeNAC. NAT is a network address translation that converts one set of IP addresses to another. VLAN is a virtual local-area network, and subnetting compartmentalizes IP networks by way of IP addresses and mathematics.

See the section titled “Network Design” in Chapter 5, “Network Design Elements,” for more information.

- 92.** Answer: D. VLAN.

Explanation: A VLAN, or virtual local-area network, was originally designed to decrease broadcast traffic on the data link layer. However, if implemented properly, it can also reduce the likelihood of having information compromised by network sniffers. It does both of these by compartmentalizing the network, usually by MAC address. This should not be confused with subnetting, which compartmentalizes the network by IP address on the network layer. A DMZ, or demilitarized zone, is used as a buffer area between the LAN and the Internet and stores servers. A VPN, or virtual private network, enables the secure connection of remote users to your network. RADIUS authenticates users to a network and is sometimes used with a VPN.

See the section titled “Network Design” in Chapter 5, “Network Design Elements,” for more information.

93. Answer: B. Internet content filter.

Explanation: Internet content filters prevent users from accessing inappropriate websites. Quite often they are built into caching proxies; however, IP proxies are used to enable the connection of many hosts on a LAN through one IP address out to the Internet. A NIDS, or network intrusion detection system, can detect attacks on the network and alert a network administrator if they occur. A honeypot is used to attract and trap attackers on the network for further analysis.

See the section titled “Firewalls and Network Security” in Chapter 7, “Network Perimeter Security,” for more information.

94. Answer: C. DNS poisoning.

Explanation: DNS poisoning is the modification of name resolution information stored on a DNS server. This can redirect users to incorrect websites, even if they typed the correct URL. A denial of service is an attack on a server that attempts to use all the server’s resources so that it cannot serve clients any longer. ARP poisoning is an attack that spoofs data that contains a false source MAC address. DLL injection is a technique used to run code within the address space of another process.

See the section titled “Malicious Attacks” in Chapter 6, “Networking Protocols and Threats,” for more information.

95. Answer: A. FTP server.

Explanation: A DMZ typically contains servers such as FTP servers, web servers, and e-mail servers. Basically it contains servers that users on the Internet would need to access. SQL servers are database servers normally stored on a company’s internal network. The same holds true for customer account databases and user workstations.

See the section titled “Network Design” in Chapter 5, “Network Design Elements,” for more information.

96. Answer: B. Firewall.

Explanation: Some firewalls have stateful packet inspection built in; however, this should be checked because other firewalls will have stateless packet inspection. Stateful packet inspection keeps track of the state of network connections by examining the header in each packet. Switches and hubs are essential connecting devices that connect computers. An IDS, or intrusion detection system, is software or a device that detects attackers and sends administrative alerts if an attack is detected; they can be installed on individual computers or on the network.

See the section titled “Firewalls and Network Security” in Chapter 7, “Network Perimeter Security,” for more information.

**97. Answer: C. Application-proxy.**

Explanation: An Application-proxy firewall inspects data at layer 7 of the OSI model. These types of firewalls are also known as application-level gateways, or ALGs. They apply security mechanisms to applications such as FTP. Network address translation, or NAT, firewalls filter traffic according to TCP or UDP ports, which concerns the transport layer, layer 4 of the OSI model. Stateful inspection, or stateful packet inspection (SPI), keeps track of network connections by examining the header of each packet, which concerns the network layer, layer 3 of the OSI model. Circuit-level gateways work at the session layer of the OSI model and apply security mechanisms when TCP or UDP connections are established.

See the section titled “Firewalls and Network Security” in Chapter 7, “Network Perimeter Security,” for more information.

**98. Answer: D. To hide internal hosts from the public network.**

Explanation: The primary purpose of network address translation is to hide internal hosts from the public network. This is usually done by displaying a single public IP address to the Internet that is used by all the internal private hosts. An IP proxy usually employs NAT. It is not necessary to hide the public network from internal hosts; if you were to do so, the internal hosts could not access the Internet. A DNS server can convert IP addresses to domain names and vice versa. The device that caches web pages would be an HTTP proxy, one of several types of caching proxies.

See the section titled “Network Design” in Chapter 5, “Network Design Elements,” for more information.

**99. Answer: C. Fraggle attack.**

Explanation: A Fraggle attack is a type of denial-of-service attack that sends a large amount of UDP Echo traffic and is not associated with Bluetooth. Discovery mode is a configuration setting that, if enabled, can allow security threats to access the Bluetooth-enabled device; some people consider it a threat unto itself. If Bluetooth devices are set to “discoverable,” bluesnarfing and bluejacking attacks could possibly occur. Bluesnarfing is the unauthorized access of information through the Bluetooth connection and is generally the theft of data such as calendar information and phonebook contacts. Bluejacking is the sending of unsolicited messages to Bluetooth-enabled devices. One way to prevent both of these attacks is to set the Bluetooth device to “undiscoverable.”

See the section titled “Network Design” in Chapter 5, “Network Design Elements,” for more information.

- 100.** Answer: B. TACACS+ because it encrypts client/server negotiation dialogs.

Explanation: TACACS+ has a few advantages over RADIUS. It encrypts the initial negotiation between the remote client and the server. It also separates authentication and authorization into two separate functions that introduce another layer of security. Finally, it offers more types of authentication requests than RADIUS. However, RADIUS is more common in Windows environments, whereas TACACS+ is used in a variety of environments. So a security administrator should analyze the IT environment carefully before implementing either of these remote authentication systems.

See the section titled “Authentication Models and Components” in Chapter 9, “Physical Security and Authentication Models,” for more information.

*This page intentionally left blank*

# Glossary

This glossary contains the key terms from the book. All the terms from each chapter’s “Define Key Terms” tasks are defined here.

**3-leg perimeter** A type of DMZ where a firewall has three legs that connect to the LAN, the Internet, and the DMZ.

**10 tape rotation** A backup rotation scheme in which ten backup tapes are used over the course of two weeks.

**802.1X** An authentication technology used to connect devices to a LAN or WLAN. It is an example of port-based network access control (NAC).

**acceptable use** Often defined as a policy, acceptable use defines the rules that restrict how a computer, network, or other system may be used.

**access control list (ACL)** A list of permissions attached to an object. ACLs specify what level of access a user, users, or groups have to an object. When dealing with firewalls, an ACL is a set of rules that applies to a list of network names, IP addresses, and port numbers.

**access control model** Specifies methodologies by which admission to physical areas and, more importantly, computer systems, is managed and organized.

**account expiration** The date when a user’s account they use to log on to the network expires.

**accounting** The tracking of data, computer usage, and network resources. Often it means logging, auditing, and monitoring of the data and resources.

**active interception** Normally refers to placing a computer between the sender and the receiver in an effort to capture and possibly modify information.

**ad filtering** Ways of blocking and filtering out unwanted advertisements; pop-up blockers and content filters are considered to be ad filtering methods.

**Advanced Encryption Standard (AES)** An encryption standard used with WPA and WPA2. The successor to DES/3DES and is another symmetric key encryption standard composed of three different block ciphers: AES-128, AES-192, and AES-256.

**adware** Type of spyware that pops up advertisements based on what it has learned about the user.

**algorithms** Well-defined instructions that describe computations from their initial state to their final state.

**anomaly-based monitoring** Also known as statistical anomaly-based monitoring, establishes a performance baseline based on a set of normal network traffic evaluations.

**AP isolation** Each client connected to the AP will not be able to communicate with each other, but they can each still access the Internet.

**application black-listing** A method of disallowing one or more applications from use.

**application firewall** A firewall that can control the traffic associated with specific applications. Works all the way up to the Application Layer of the OSI model.

**application-level gateway (ALG)** Applies security mechanisms to specific applications, such as FTP and/or BitTorrent. It supports address and port translation and checks whether the type of application traffic is allowed.

**application white-listing** A method of restricting users to specific applications.

**ARP poisoning** An attack that exploits Ethernet networks, and it may enable an attacker to sniff frames of information, modify that information, or stop it from getting to its intended destination.

**asymmetric key algorithm** A type of cipher that uses a pair of different keys to encrypt and decrypt data.

**attack vector** The path or means by which an attacker gains access to a computer.

**audit trails** Records or logs that show the tracked actions of users, regardless of whether the users successfully completed the actions.

**authentication** When a person's identity is confirmed. Authentication is the verification of a person's identity.

**authorization** When a user is granted access to specific resources after authentication is complete.

**availability** Data is obtainable regardless of how information is stored, accessed, or protected.

**backdoors** Used in computer programs to bypass normal authentication and other security mechanisms in place.

**back-to-back perimeter** A type of DMZ where the DMZ is located between the LAN and the Internet.

**backup generator** Part of an emergency power system used when there is an outage of regular electric grid power.

**baiting** When a malicious individual leaves malware-infected removable media, such as a USB drive or optical disc, lying around in plain view.

**banner grabbing** A technique used to gain information about servers and take inventory of systems and services. It can be used legitimately by network administrators or illegitimately by attackers to grab information such as HTTP headers.

**baseline reporting** Identification of the security posture of an application, system, or network.

**baselining** The process of measuring changes in networking, hardware, software, and so on.

**behavior-based monitoring** A monitoring system that looks at the previous behavior of applications, executables, and/or the operating system and compares that to current activity on the system.

**biometrics** The science of recognizing humans based on one or more physical characteristics.

**birthday attack** An attack on a hashing system that attempts to send two different messages with the same hash function, causing a collision.

**black-box testing** When people test a system but have no specific knowledge of the system code involved with the system.

**black hat** A hacker that breaks into computer systems without permission, with the express purpose of theft, piracy, credit card fraud, or other illegal activities.

**blackout** When a total loss of power for a prolonged period occurs.

**blanket purchase agreement (BPA)** A service-level agreement (SLA) that is reoccurring.

**block cipher** A type of algorithm that encrypts a number of bits as individual units known as blocks.

**bluejacking** The sending of unsolicited messages to Bluetooth-enabled devices such as mobile phones and tablets.

**bluesnarfing** The unauthorized access of information from a wireless device through a Bluetooth connection.

**botnet** A group of compromised computers used to distribute malware across the Internet; the members are usually zombies.

**broadcast storm** When there is an accumulation of broadcast and multicast packet traffic on the LAN coming from one or more network interfaces.

**brownout** When the voltage drops to such an extent that it typically causes the lights to dim and causes computers to shut off.

**brute-force attack** A password attack where every possible password is attempted.

**buffer overflow** When a process stores data outside the memory that the developer intended to be used for storage. This could cause erratic behavior in the application, especially if the memory already had other data in it.

**business impact analysis** The examination of critical versus noncritical functions, it is part of a business continuity plan (BCP).

**butt set (or lineman's handset)** A device that looks similar to a phone but has alligator clips that can connect to the various terminals used by phone equipment, enabling a person to listen in to a conversation.

**CAM table** The Content Addressable Memory table, a table that is in a switch's memory that contains ports and their corresponding MAC addresses.

**CAPTCHA** A type of challenge-response mechanism used primarily in websites to tell whether or not the user is human. Stands for Completely Automated Public Turing test to tell Computers and Humans Apart.

**certificate authority (CA)** The entity (usually a server) that issues digital certificates to users.

**certificate revocation list (CRL)** A list of certificates no longer valid or that have been revoked by the issuer.

**certificates** Digitally signed electronic documents that bind a public key with a user identity.

**chain of custody** Documents who had custody of evidence all the way up to litigation or a court trial (if necessary) and verifies that the evidence has not been modified.

**Challenge Handshake Authentication Protocol (CHAP)** An authentication scheme used by the Point-to-Point Protocol (PPP) that is the standard for dial-up connections.

**change management** A structured way of changing the state of a computer system, network, or IT procedure.

**chromatic dispersion** The refraction of light as in a rainbow. If light is refracted in such a manner on fiber-optic cables, the signal cannot be read by the receiver.

**cipher** An algorithm that can perform encryption or decryption.

**circuit-level gateway** Works at the Session Layer of the OSI model and applies security mechanisms when a TCP or UDP connection is established; acts as a go-between for the Transport and Application Layers in TCP/IP.

**closed-circuit television (CCTV)** A video system (often used for surveillance) that makes use of traditional coaxial-based video components, but is used privately, within a building or campus.

**cloud computing** A way of offering on-demand services that extend the capabilities of a person's computer or an organization's network.

**cluster** Two or more servers that work with each other.

**cold site** A site that has tables, chairs, bathrooms, and possibly some technical setup (for example, basic phone, data, and electric lines), but will require days if not weeks to set up properly.

**Common Vulnerabilities and Exposures (CVE)®** An online list of known vulnerabilities (and patches) to software, especially web servers. It is maintained by the MITRE Corporation.

**computer security audits** Technical assessments made of applications, systems, or networks.

**confidentiality** Preventing the disclosure of information to unauthorized persons.

**content filters** Individual computer programs that block external files that use JavaScript or images from loading into the browser.

**cookies** Text files placed on the client computer that store information about it, which could include your computer's browsing habits and credentials. Tracking cookies are used by spyware to collect information about a web user's activities. Session cookies are used by attackers in an attempt to hijack a session.

**cross-site request forgery (XSRF)** An attack that exploits the trust a website has in a user's browser in an attempt to transmit unauthorized commands to the website.

**cross-site scripting (XSS)** A type of vulnerability found in web applications used with session hijacking.

**crosstalk** When a signal transmitted on one copper wire creates an undesired effect on another wire; the signal "bleeds" over, so to speak.

**cryptanalysis attack** A password attack that uses a considerable set of precalculated encrypted passwords located in a lookup table.

**cryptographic hash functions** Hash functions based on block ciphers.

**cryptography** The practice and study of hiding information.

**data emanation (or signal emanation)** The electromagnetic field generated by a network cable or network device, which can be manipulated to eavesdrop on conversations or to steal data.

**Data Encryption Standard (DES)** An older type of block cipher selected by the United States federal government back in the 1970s as its encryption standard; due to its weak key, it is now considered deprecated.

**data loss prevention (DLP)** Systems that are designed to protect data by way of content inspection. They are meant to stop the leakage of confidential data, often concentrating on communications.

**default account** An account installed by default on a device or within an operating system with a default set of user credentials that are usually insecure.

**defense in depth** The building up and layering of security measures that protect data from inception, on through storage and network transfer, and lastly to final disposal.

**demilitarized zone (DMZ)** A special area of the network (sometimes referred to as a subnetwork) that houses servers that host information accessed by clients or other networks on the Internet.

**denial-of-service (DoS)** A broad term given to many different types of network attacks that attempt to make computer resources unavailable.

**dictionary attack** A password attack that uses a prearranged list of likely words, trying each of them one at a time.

**differential backup** Type of backup that backs up only the contents of a folder that have changed since the last full backup.

**Diffie-Hellman key exchange** Invented in the 1970s, it was the first practical method for establishing a shared secret key over an unprotected communications channel.

**digital signature** A signature that authenticates a document through math, letting the recipient know that the document was created and sent by the actual sender and not someone else.

**directory traversal** Also known as the ../ (dot dot slash) attack, a method of accessing unauthorized parent directories.

**disaster recovery plan** A plan that details the policies and procedures concerning the recovery and/or continuation of an organization's technology infrastructure.

**discretionary access control (DAC)** An access control policy generally determined by the owner.

**disk duplexing** When each disk is connected to a separate controller.

**distributed denial-of-service (DDoS)** An attack in which a group of compromised systems attack a single target, causing a DoS to occur at that host, usually using a botnet.

**diversion theft** When a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location.

**DNS poisoning** The modification of name resolution information that should be in a DNS server's cache.

**domain name kiting** The process of deleting a domain name during the five-day grace period (known as the add grace period, or AGP) and immediately reregistering it for another five-day period to keep a domain name indefinitely and for free.

**due care** The mitigation action that an organization takes to defend against the risks that have been uncovered during due diligence.

**due diligence** Ensuring that IT infrastructure risks are known and managed.

**due process** The principle that an organization must respect and safeguard personnel's rights.

**dumpster diving** When a person literally scavenges for private information in garbage and recycling containers.

**Easter egg** A platonic extra added to an OS or application as a sort of joke; the harmless cousin of the logic bomb.

**eavesdropping** When a person uses direct observation to "listen" in to a conversation.

**electromagnetic interference (EMI)** A disturbance that can affect electrical circuits, devices, and cables due to electromagnetic conduction or radiation.

**elliptic curve cryptography (ECC)** A type of public key cryptography based on the structure of an elliptic curve.

**encryption** The process of changing information using an algorithm (or cipher) into another form that is unreadable by others—unless they possess the key to that data.

**ethical hacker** An expert at breaking into systems and can attack systems on behalf of the system's owner and with the owner's consent.

**evil twin** A rogue wireless access point that uses the same SSID as a nearby legitimate access point.

**explicit allow** When an administrator sets a rule that allows a specific type of traffic through a firewall, often within an ACL.

**explicit deny** When an administrator sets a rule that denies a specific type of traffic access through a firewall, often within an ACL.

**Extensible Authentication Protocol (EAP)** Not an authentication mechanism in itself but instead defines message formats. 802.1X would be the authentication mechanism and defines how EAP is encapsulated within messages.

**fail-open mode** When a switch broadcasts data on all ports the way a hub does.

**failover clusters** Also known as high-availability clusters, these are designed so that a secondary server can take over in the case that the primary one fails, with limited or no downtime.

**false negative** When a system denies a user who actually should be allowed access to the system—for example, when an IDS/IPS fails to block an attack, thinking it is legitimate traffic.

**false positive** When a system authenticates a user who should not be allowed access to the system—for example, when an IDS/IPS blocks legitimate traffic from passing on to the network.

**false rejection** When a biometric system fails to recognize an authorized person and doesn't allow that person access.

**Faraday cage** An enclosure formed by conducting material or by a mesh of such material; it blocks out external static electric fields and can stop emanations from cell phones and other devices within the cage from leaking out.

**federated identity management (FIM)** When a user's identity is shared across multiple identity management systems.

**fire suppression** The process of controlling and/or extinguishing fires to protect people and an organization's data and equipment.

**firewall** A part of a computer system or network designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit or deny computer applications based on a set of rules and other criteria.

**first responders** People who perform preliminary analysis of the incident data and determine whether the incident is an incident or just an event, and the criticality of the incident.

**flood guard** Security feature implemented on some firewalls to protect against SYN floods and other flooding attacks. Also known as attack guards.

**fork bomb** An attack that works by creating a large number of processes quickly to saturate the available processing space in the computer's operating system. It is a type of wabbit.

**Frapple** A type of DoS similar to the Smurf attack, but the traffic sent is UDP echo traffic as opposed to ICMP echo traffic.

**full backup** Type of backup where all the contents of a folder are backed up.

**fuzz testing (fuzzing)** When random data is inputted into a computer program in an attempt to find vulnerabilities.

**grandfather-father-son** A backup rotation scheme in which three sets of backup tapes must be defined—usually they are daily, weekly, and monthly, which correspond to son, father, and grandfather.

**grayware** A general term used to describe applications that are behaving improperly but without serious consequences; often describes types of spyware.

**Group Policy** Used in Microsoft environments to govern user and computer accounts through a set of rules.

**hardening** The act of configuring an OS securely, updating it, creating rules and policies to help govern the system in a secure manner, and removing unnecessary applications and services.

**hardware security module (HSM)** A physical device that deals with the encryption of authentication processes, digital signings, and payment processes.

**hash** A summary of a file or message. It is generated to verify the integrity of the file or message.

**hash function** A mathematical procedure that converts a variable-sized amount of data into a smaller block of data.

**hoax** The attempt at deceiving people into believing something that is false.

**honeynet** One or more computers, servers, or an area of a network, used to attract and trap potential attackers to counteract any attempts at unauthorized access of the network.

**honeypot** Generally is a single computer but could also be a file, group of files, or an area of unused IP address space used to attract and trap potential attackers to counteract any attempts at unauthorized access of the network.

**host-based intrusion detection system (HIDS)** A type of system loaded on an individual computer; it analyzes and monitors what happens inside that computer—for example, if any changes have been made to file integrity.

**hot and cold aisles** The aisles in a server room or data center that circulate cold air into the systems and hot air out of them. Usually, the systems and cabinets are supported by a raised floor.

**hot site** A near duplicate of the original site of the organization, complete with phones, computers, networking devices, and full backups.

**hotfix** Originally, a hotfix was defined as a single problem fixing patch to an individual OS or application that was installed live while the system was up and running, and without a reboot necessary. However, this term has changed over time and varies from vendor to vendor.

**HTTP proxy (web proxy)** Caches web pages from servers on the Internet for a set amount of time.

**hypervisor** The portion of virtual machine software that allows multiple virtual operating systems (guests) to run at the same time on a single computer.

**identification** When a person is in a state of being identified. It can also be described as something that identifies a person such as an ID card.

**identity proofing** An initial validation of an identity.

**implicit deny** Denies all traffic to a resource unless the users generating that traffic are specifically granted access to the resource. For example, when a device denies all traffic unless a rule is made to open the port associated with the type of traffic desired to be let through.

**incident management** The monitoring and detection of security events on a computer network and the execution of proper responses to those security events.

**incident response** A set of procedures that an investigator follows when examining a computer security incident.

**incremental backup** Type of backup that backs up only the contents of a folder that have changed since the last full backup or the last incremental backup.

**information assurance** The practice of managing risks that are related to computer hardware and software systems.

**information security** The act of protecting information from unauthorized access. It usually includes an in-depth plan on how to secure data, computers, and networks.

**Infrastructure as a Service (IaaS)** A cloud computing service that offers computer networking, storage, load balancing, routing, and VM hosting.

**input validation (data validation)** A process that ensures the correct usage of data.

**integer overflow** When arithmetic operations attempt to create a numeric value that is too big for the available memory space.

**integrity** This means that authorization is necessary before data can be modified.

**Internet content filter** A filter that 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 is used most often to disallow access to inappropriate web material.

**Internet Protocol Security (IPsec)** A TCP/IP protocol that authenticates and encrypts IP packets, effectively securing communications between computers and devices using the protocol.

**IP proxy** Secures a network by keeping machines behind it anonymous; it does this through the use of NAT.

**IV attack** A type of related-key attack, which is when an attacker observes the operation of a cipher using several different keys and finds a mathematical relationship between them, allowing the attacker to ultimately decipher data.

**job rotation** When users are cycled through various assignments.

**Kerberos** An authentication protocol that enables computers to prove their identity to each other in a secure manner.

**key** The essential piece of information that determines the output of a cipher.

**key escrow** When certificate keys are held in case third parties, such as government or other organizations, need access to encrypted communications.

**key recovery agent** Software that can be used to archive and restore keys if necessary.

**key stretching** Takes a weak key, processes it, and outputs an enhanced and more powerful key, usually increasing key size to 128 bits.

**LANMAN hash** The original hash used to store Windows passwords, known as LM hash, based off the DES algorithm.

**Layer 2 Tunneling Protocol (L2TP)** A tunneling protocol used to connect virtual private networks. It does not include confidentiality or encryption on its own. It uses port 1701 and can be more secure than PPTP if used in conjunction with IPsec.

**least privilege** When a user is given only the amount of privileges needed to do his job.

**Lightweight Directory Access Protocol (LDAP)** An Application Layer protocol used for accessing and modifying directory services data.

**load-balancing clusters** When multiple computers are connected in an attempt to share resources such as CPU, RAM, and hard disks.

**locally shared objects (LSOs)** Also known as Flash cookies, these are files stored on users' computers that allow websites to collect information about visitors. Also referred to as "local shared objects."

**logic bomb** Code that has, in some way, been inserted into software; it is meant to initiate some type of malicious function when specific criteria are met.

**MAC filtering** A method used to filter out which computers can access the wireless network; the WAP does this by consulting a list of MAC addresses that have been previously entered.

**MAC flooding** An attack that sends numerous packets to a switch, each of which has a different source MAC address, in an attempt to use up the memory on the switch. If this is successful, the switch will change state to fail-open mode.

**malware** Software designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent.

**mandatory access control (MAC)** An access control policy determined by a computer system, not by a user or owner, as it is in DAC.

**mandatory vacations** When an organization requires that employees take a certain number of days of vacation consecutively.

**man-in-the-browser (MITB)** Infects a vulnerable web browser and modifies online transactions. Similar to MITM.

**man-in-the-middle (MITM)** A form of eavesdropping that intercepts all data between a client and a server, relaying that information back and forth.

**mantrap** An area between two doorways, meant to hold people until they are identified and authenticated.

**many-to-one mapping** When multiple certificates are mapped to a single recipient.

**mean time between failures** Defines the average number of failures per million hours for a product in question.

**memorandum of understanding (MoU)** A letter of intent between two entities (such as government agencies) concerning SLAs and BPAs.

**Message-Digest Algorithm 5 (MD5)** A 128-bit key hash used to provide integrity of files and messages.

**mobile device management (MDM)** A centralized software solution that allows for the control and configuration of mobile devices.

**multifactor authentication** When two or more types of authentication are used when dealing with user access control.

**mutual authentication** When two computers (for example, a client and a server) verify each other's identity.

**network access control (NAC)** Sets the rules by which connections to a network are governed.

**network address translation (NAT)** The process of changing an IP address while it is in transit across a router. This is usually implemented so that one larger address space (private) can be remapped to another address space, or single IP address (public).

**network intrusion detection system (NIDS)** A type of IDS that attempts to detect malicious network activities—for example, port scans and DoS attacks—by constantly monitoring network traffic.

**network intrusion prevention system (NIPS)** Designed to inspect traffic, and based on its configuration or security policy, the system can remove, detain, or redirect malicious traffic.

**Network Management System (NMS)** The software run on one or more servers that controls the monitoring of network-attached devices and computers.

**network mapping** The study of physical and logical connectivity of networks.

**network perimeter** The border of a computer network, commonly secured by devices such as firewalls and NIDS/NIPS solutions.

**nonce** A random number issued by an authentication protocol that can only be used once.

**non-promiscuous mode** When a network adapter captures only the packets that are addressed to it.

**non-repudiation** The idea of ensuring that a person or group cannot refute the validity of your proof against them.

**NTLM hash** Successor to the LM hash. A more advanced hash used to store Windows passwords, based off the RC4 algorithm.

**NTLMv2 hash** Successor to the NTLM hash. Based off the MD5 hashing algorithm.

**null session** When used by an attacker, a malicious connection to the Windows inter-process communications share (IPC\$).

**onboarding** When a new employee is added to an organization, and to its identity and access management system.

**one-time pad** A cipher that encrypts plaintext with a secret random key that is the same length as the plaintext.

**one-to-one mapping** When an individual certificate is mapped to a single recipient.

**Online Certificate Status Protocol (OCSP)** An alternative to using a certificate revocation list (CRL). It contains less information than a CRL does, and does not require encryption.

**open mail relay** Also known as an SMTP open relay, enables anyone on the Internet to send e-mail through an SMTP server.

**Open Vulnerability and Assessment Language (OVAL)** A standard and a programming language designed to standardize the transfer of secure public information across networks and the Internet utilizing any security tools and services available.

**packet filtering** In the context of firewalls, inspects each packet passing through the firewall and accepts or rejects it based on rules. Two types of packet filtering include stateless packet filters and stateful packet inspection (SPI).

**password cracker** Software tool used to recover passwords from hosts or to discover weak passwords.

**patch** An update to a system. Patches generally carry the connotation of a small fix in the mind of the user or system administrator, so larger patches often are referred to as software updates, service packs, or something similar.

**patch management** The planning, testing, implementing, and auditing of patches.

**penetration testing** A method of evaluating the security of a system by simulating one or more attacks on that system.

**permanent DoS (PDoS) attack** Generally consists of an attacker exploiting security flaws in routers and other networking hardware by flashing the firmware of the device and replacing it with a modified image.

**permissions** Control which file system resources a person can access on the network.

**personal firewall** An application that protects an individual computer from unwanted Internet traffic; it does so by way of a set of rules and policies.

**personally identifiable information (PII)** Information used to uniquely identify, contact, or locate a person.

**pharming** When an attacker redirects one website's traffic to another bogus and possibly malicious website by modifying a DNS server or hosts file.

**phishing** The criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

**piggybacking** When an unauthorized person tags along with an authorized person to gain entry to a restricted area.

**ping flood** When an attacker attempts to send many ICMP echo request packets (pings) to a host in an attempt to use up all available bandwidth. Also known as an ICMP flood attack.

**Ping of Death (POD)** A type of DoS that sends an oversized and/or malformed packet to another computer.

**Platform as a Service (PaaS)** A cloud computing service that provides various software solutions to organizations, especially the ability to develop applications without the cost or administration of a physical platform.

**Point-to-Point Tunneling Protocol (PPTP)** A tunneling protocol used to support VPNs. Generally includes security mechanisms, and no additional software or protocols need to be loaded. A VPN device or server must have inbound port 1723 open to enable incoming PPTP connections.

**policy** Rules or guidelines used to guide decisions and achieve outcomes. They can be written or configured on a computer.

**pop-up blocker** An application or add-on to a web browser that blocks pop-up windows that usually contain advertisements.

**port address translation (PAT)** Like NAT, but it translates both IP addresses and port numbers.

**port scanner** Software used to decipher which ports are open on a host.

**pre-action sprinkler system** Similar to a dry pipe system, but there are requirements for it to be set off such as heat or smoke.

**pretexting** When a person invents a scenario, or pretext, in the hope of persuading a victim to divulge information.

**Pretty Good Privacy (PGP)** An encryption program used primarily for signing, encrypting, and decrypting e-mails in an attempt to increase the security of e-mail communications.

**private key** A type of key that is known only to a specific user or users who keep the key a secret.

**privilege escalation** The act of exploiting a bug or design flaw in a software or firmware application to gain access to resources that normally would've been protected from an application or user.

**promiscuous mode** In a network adapter, this passes all traffic to the CPU, not just the frames addressed to it. When the network adapter captures all packets that it has access to regardless of the destination for those packets.

**protected distribution system** Security system implemented to protect unencrypted data transfer over wired networks.

**Protected Extensible Authentication Protocol (PEAP)** Protocol used to encapsulate EAP packets within encrypted and authenticated tunnels.

**protocol analyzer** Software tool used to capture and analyze packets.

**proxy server** Acts as an intermediary between clients, usually located on a LAN, and the servers that they want to access, usually located on the Internet.

**public key** A type of key that is known to all parties involved in encrypted transactions within a given group.

**public key cryptography** Uses asymmetric keys alone or in addition to symmetric keys. The asymmetric key algorithm creates a secret private key and a published public key.

**public key infrastructure (PKI)** An entire system of hardware and software, policies and procedures, and people, used to create, distribute, manage, store, and revoke digital certificates.

**qualitative risk assessment** An assessment that assigns numeric values to the probability of a risk and the impact it can have on the system or network.

**quantitative risk assessment** An assessment that measures risk by using exact monetary values.

**radio frequency interference (RFI)** Interference that can come from AM/FM transmissions and cell towers.

**RAID 1** Mirroring. Data is copied to two identical disks. If one disk fails, the other continues to operate.

**RAID 5** Striping with parity. Data is striped across multiple disks; fault-tolerant parity data is also written to each disk.

**rainbow table** In password cracking, a set of precalculated encrypted passwords located in a lookup table.

**ransomware** A type of malware that restricts access to a computer system, and demands a ransom be paid.

**recovery point objective (RPO)** In business impact analysis, the acceptable latency of data.

**recovery time objective (RTO)** In business impact analysis, the acceptable amount of time to restore a function.

**redundant ISP** Secondary connections to another ISP; for example, a backup T-1 line.

**redundant power supply** An enclosure that contains two complete power supplies, the second of which turns on when the first fails.

**registration authority (RA)** Used to verify requests for certificates.

**Remote Access Service (RAS)** A networking service that allows incoming connections from remote dial-in clients. It is also used with VPNs.

**Remote Authentication Dial-In User Service (RADIUS)** Used to provide centralized administration of dial-up, VPN, and wireless authentication.

**remote code execution (RCE)** When an attacker acquires control of a remote computer through a code vulnerability. Also known as arbitrary code execution. Attackers often use a web browser's URL field or a tool such as Netcat to accomplish this.

**replay attack** An attack in which valid data transmission is maliciously or fraudulently repeated or delayed.

**residual risk** The risk that is left over after a security plan and a disaster recovery plan have been implemented.

**risk** The possibility of a malicious attack or other threat causing damage or downtime to a computer system.

**risk acceptance** The amount of risk an organization is willing to accept. Also known as risk retention.

**risk assessment** The attempt to determine the amount of threats or hazards that could possibly occur in a given amount of time to your computers and networks.

**risk avoidance** When an organization avoids risk because the risk factor is too great.

**risk management** The identification, assessment, and prioritization of risks, and the mitigation and monitoring of those risks.

**risk mitigation** When a risk is reduced or eliminated altogether.

**risk reduction** When an organization mitigates risk to an acceptable level.

**risk transference** The transfer or outsourcing of risk to a third party. Also known as risk sharing.

**role-based access control (RBAC)** An access model that works with sets of permissions, instead of individual permissions that are label-based. So roles are created for various job functions in an organization.

**rootkit** A type of software designed to gain administrator-level control over a computer system without being detected.

**RSA** A public key cryptography algorithm created by Rivest, Shamir, Adleman. It is commonly used in e-commerce.

**S/MIME** An IETF standard that provides cryptographic security for electronic messaging such as e-mail.

**sag** An unexpected decrease in the amount of voltage provided.

**salting** The randomization of the hashing process to defend against cryptanalysis password attacks and rainbow tables.

**sandbox** When a web script runs in its own environment for the express purpose of not interfering with other processes, possibly for testing.

**secure code review** An in-depth code inspection procedure.

**secure coding concepts** The best practices used during the life cycle of software development.

**Secure Hash Algorithm (SHA)** A group of hash functions designed by the NSA and published by the NIST, widely used in government. The most common currently is SHA-1.

**Secure Shell (SSH)** A protocol that can create a secure channel between two computers or network devices.

**Secure Sockets Layer (SSL)** A cryptographic protocol that provides secure Internet communications such as web browsing, instant messaging, e-mail, and VoIP.

**security log files** Files that log activity of users. They show who did what and when, plus whether they succeeded or failed in their attempt.

**security posture** The risk level to which a system, or other technology element, is exposed.

**security posture assessment (SPA)** An assessment that uses baseline reporting and other analyses to discover vulnerabilities and weaknesses in systems and networks.

**security template** Groups of policies that can be loaded in one procedure.

**security tokens** Physical devices given to authorized users to help with authentication. These devices might be attached to a keychain or are part of a card system.

**separation of duties (SoD)** This is when more than one person is required to complete a particular task or operation.

**service-level agreement (SLA)** Part of a service contract where the level of service is formally defined.

**service pack (SP)** A group of updates, bug fixes, updated drivers, and security fixes that is installed from one downloadable package or from one disc.

**service set identifier (SSID)** The name of a wireless access point (or network) to which network clients will connect; it is broadcast through the air.

**shoulder surfing** When a person uses direct observation to find out a target's password, PIN, or other such authentication information.

**signature-based monitoring** Frames and packets of network traffic are analyzed for predetermined attack patterns. These attack patterns are known as signatures.

**Simple Network Management Protocol (SNMP)** A TCP/IP protocol that monitors network-attached devices and computers. It's usually incorporated as part of a network management system.

**single point of failure** An element, object, or part of a system that, if it fails, will cause the whole system to fail.

**single sign-on (SSO)** When a user can log in once but gain access to multiple systems without being asked to log in again.

**Smurf attack** A type of DoS that sends large amounts of ICMP echoes, broadcasting the ICMP echo requests to every computer on its network or subnetwork. The header of the ICMP echo requests will have a spoofed IP address. That IP address is the target of the Smurf attack. Every computer that replies to the ICMP echo requests will do so to the spoofed IP.

**SNMP agent** Software deployed by the network management system that is loaded on managed devices. The software redirects the information that the NMS needs to monitor the remote managed devices.

**Software as a Service (SaaS)** A cloud computing service where users access applications over the Internet that are provided by a third party.

**spam** The abuse of electronic messaging systems such as e-mail, broadcast media, and instant messaging.

**spear phishing** A type of phishing attack that targets particular individuals.

**special hazard protection system** A clean agent sprinkler system such as FM-200 used in server rooms.

**spike** A short transient in voltage that can be due to a short circuit, tripped circuit breaker, power outage, or lightning strike.

**spim** The abuse of instant messaging systems, a derivative of spam.

**spoofing** When an attacker masquerades as another person by falsifying information.

**spyware** A type of malicious software either downloaded unwittingly from a website or installed along with some other third-party software.

**standby generator** Systems that turn on automatically within seconds of a power outage.

**stateful packet inspection (SPI)** Type of packet inspection that keeps track of network connections by examining the header in each packet.

**static NAT** When a single private IP address translates to a single public IP address. This is also called one-to-one mapping.

**steganography** The science (and art) of writing hidden messages; it is a form of security through obscurity.

**storage segmentation** A clear separation of organizational and personal information, applications, and other content.

**stream cipher** A type of algorithm that encrypts each byte in a message one at a time.

**supervisory control and data acquisition (SCADA)** System of hardware and software that controls and monitors industrial systems such as HVAC.

**surge** Means that there is an unexpected increase in the amount of voltage provided.

**symmetric key algorithm** A class of cipher that uses identical or closely related keys for encryption and decryption.

**SYN flood** A type of DoS where an attacker sends a large amount of SYN request packets to a server in an attempt to deny service.

**Systems Development Life Cycle (SDLC)** The process of creating systems and applications, and the methodologies used to do so.

**tailgating** A type of piggybacking where an unauthorized person follows an authorized person into a secure area, without the authorized person's consent.

**TCP reset attack** Sets the reset flag in a TCP header to 1, telling the respective computer to kill the TCP session immediately.

**TCP/IP hijacking** When a hacker takes over a TCP session between two computers without the need of a cookie or any other type of host access.

**teardrop attack** A type of DoS that sends mangled IP fragments with overlapping and oversized payloads to the target machine.

**TEMPEST** Refers to the investigations of conducted emissions from electrical and mechanical devices, which could be compromising to an organization.

**Temporal Key Integrity Protocol (TKIP)** An algorithm used to secure wireless computer networks; meant as a replacement for WEP.

**Terminal Access Controller Access-Control System Plus (TACACS+)** A remote authentication protocol similar to RADIUS used in Cisco networks.

**threat modeling** A way of prioritizing threats to an application.

**threat vector** The method a threat uses to gain access to a target computer.

**tickets** Part of the authentication process used by Kerberos.

**time bomb** A Trojan set off on a certain date.

**time of day restriction** When a user's logon hours are configured to restrict access to the network during certain times of the day and week.

**Towers of Hanoi** A backup rotation scheme based on the mathematics of the Towers of Hanoi puzzle. Uses three backup sets. For example, the first tape is used every second day, the second tape is used every fourth day, and the third tape is used every eighth day.

**Transport Layer Security (TLS)** The successor to SSL. Provides secure Internet communications. This is shown in a browser as HTTPS.

**Triple DES (3DES)** Similar to DES but applies the cipher algorithm three times to each cipher block.

**Trojan horse** An application that appears to perform desired functions but is actually performing malicious functions behind the scenes.

**Trusted Computer System Evaluation Criteria (TCSEC)** A DoD standard that sets basic requirements for assessing the effectiveness of computer security access policies. Also known as The Orange Book.

**Trusted Operating System (TOS)** A system that adheres to criteria for multilevel security and meets government regulations.

**typosquatting (URL hijacking)** A method used by attackers that takes advantage of user typos when accessing websites. Instead of the expected website, the user ends up at a website with a similar name but often malicious content.

**UDP flood attack** A similar attack to the Fraggle. It uses the connectionless User Datagram Protocol. It is enticing to attackers because it does not require a synchronization process.

**uninterruptible power supply (UPS)** Takes the functionality of a surge suppressor and combines that with a battery backup, protecting computers not only from surges and spikes, but also from sags, brownouts, and blackouts.

**User Account Control (UAC)** A security component of Windows that keeps every user (besides the actual Administrator account) in standard user mode instead of as an administrator with full administrative rights—even if they are a member of the administrators group.

**vampire tap** A device used to add computers to a 10BASE5 network. It pierces the copper conductor of a coaxial cable and can also be used for malicious purposes.

**virtual machine (VM)** Created by virtual software; VMs are images of operating systems or individual applications.

**virtual private network (VPN)** A connection between two or more computers or devices that are not on the same private network.

**virtualization** The creation of a virtual entity, as opposed to a true or actual entity.

**virus** Code that runs on a computer without the user's knowledge; it infects the computer when the code is accessed and executed.

**voishing** A type of phishing attack that makes use of telephones and VoIP.

**VLAN hopping** The act of gaining access to traffic on other VLANs that would not normally be accessible by jumping from one VLAN to another.

**VPN concentrator** A hardware appliance that allows hundreds of users to connect to the network from remote locations via a VPN.

**vulnerability** Weaknesses in your computer network design and individual host configuration.

**vulnerability assessment** Baselining of the network to assess the current security state of computers, servers, network devices, and the entire network in general.

**vulnerability management** The practice of finding and mitigating software vulnerabilities in computers and networks.

**vulnerability scanning** The act of scanning for weaknesses and susceptibilities in the network and on individual systems.

**war-chalking** The act of physically drawing symbols in public places that denote open, closed, or protected wireless networks.

**war-dialing** The act of scanning telephone numbers by dialing them one at a time and adding them to a list, in an attempt to gain access to computer networks.

**war-driving** The act of searching for wireless networks by a person in a vehicle through the use of a device with a wireless antenna, often a particularly strong antenna.

**warm site** A site that has computers, phones, and servers, but they might require some configuration before users can start working on them.

**watering hole attack** An attacker profiles which websites a user accesses and later infects those sites to redirect the user to other websites.

**web of trust** A decentralized model used for sharing certificates without the need for a centralized CA.

**web security gateway** An intermediary that can scan for viruses and filter Internet content.

**wet pipe sprinkler system** Consists of a pressurized water supply system that can deliver a high quantity of water to an entire building via a piping distribution system.

**whaling** A phishing attack that targets senior executives.

**white-box testing** A method of testing applications or systems where the tester is given access to the internal workings of the system.

**white hat** A type of hacker that is contracted to break into a company's system.

**Wi-Fi Protected Access (WPA)** A security protocol created by the Wi-Fi Alliance to secure wireless computer networks; more secure than WEP.

**Wi-Fi Protected Setup (WPS)** A simplified way of connecting to wireless networks using an eight-digit code. It is now deprecated due to its insecure nature and should be disabled if currently used.

**Wired Equivalent Privacy (WEP)** A deprecated wireless network security standard, less secure than WPA.

**wiretapping** Tapping into a network cable in an attempt to eavesdrop on a conversation or steal data.

**worm** Code that runs on a computer without the user's knowledge; a worm self-replicates, whereas a virus does not.

**X.509** A common PKI standard developed by the ITU-T that incorporates the single sign-on authentication method.

**zero day attack** An attack that is executed on a vulnerability in software before that vulnerability is known to the creator of the software.

**zombie** An individual compromised computer in a botnet.

*This page intentionally left blank*



# Index

## Numbers

3DES (Triple DES), 516

10 tape rotation, 593

802.1X, 348-351, 361

allowing, 148

denying, 147

## A

access control lists (ACLs). *See ACLs (access control lists)*

access control models, 382

accounts, consolidating, 393

best practices, 388-391

DAC (discretionary access control), 384-385

groups, 393

MAC (mandatory access control), 386-387

moving/copying folders and files, 397

permission inheritance, 396

permissions, 394

policies, 400-401

propagation, 396

RBAC (role-based access control), 387

security permissions, 394

summary of, 387

time-of-day restrictions, 393

UAC (User Account Control), 403-404

usernames and passwords, 397-399

users, groups, and permissions, 391-395

access policies, clouds, 201

accessing, data emanations, 308

Account Lockout Threshold, 402

accounting, 5

accounts, consolidating, 393

ACLs (access control lists), 185

firewalls, 270

active fingerprinting, 430

active security analysis, 429

ActiveX controls, IE (Internet Explorer), 140

add-ons

Firefox, 145

IE (Internet Explorer), 139

administration interface, wireless networks, 310

ADUC (Active Directory Users and Computers), 391-392

Advanced option, Firefox, 143

Advanced tab, IE (Internet Explorer), 139

AES (Advanced Encryption Standard), 312, 517

AH (authentication header), 561

AIM (AOL Instant Messenger), 84

ALE (annualized loss expectancy), 426

ALG (application-level gateway), 271

algorithms, 525

asymmetric key algorithms, 513

*Diffie-Hellman*, 521

*RSA (Rivest, Shamir, and Adelman)*, 519-520

ECC (elliptic curve cryptography), 521-522

encryption, 516

*3DES (Triple DES)*, 516

*AES (Advanced Encryption Standard)*, 517

*Blowfish*, 518

*DES (Data Encryption Standard)*, 516

*RC (Rivest Cipher)*, 518

*summary of*, 519

*Twofish*, 518

symmetric versus asymmetric key

algorithms, 512-513

all-in-one devices, firewalls, 274

allowing, access, 148

- Alt+F4, 132**
- altered hosts files, 247**
- analytical tools, 475-477**
- analyzing test questions, case studies, 671**
- annualized loss expectancy (ALE), 426**
- annualized rate of occurrence (ARO), 426**
- anomaly-based monitoring, 466**
- anti-malware software, 7**
- antivirus software, 28, 31**
- anycast, 187**
- Apache, 206**
- application layer protocols, 558**
- application patch management, 149**
- application security, mobile devices, 54-57**
- application-level gateway (ALG), 271**
- applications, securing, 147-149**
- arbitrary code execution, secure programming, 158**
- ARO (annualized rate of occurrence), 426**
- ARP poisoning, 247**
- assessing vulnerabilities with security tools, 435**
- network mapping, 435-437
- network sniffing, 441-443
- password analysis, 443-445
- vulnerability scanning, 438-441
- assessments**
- impact assessment, 425
- risk assessments. *See* risk assessments
- asymmetric key algorithms, 513**
- Diffie-Hellman, 521
- RSA (Rivest, Shamir, and Adelman), 519-520
- versus symmetric, 512
- attacks**
- birthday attacks, 528-529
- brute-force attacks, 444
- cryptanalysis attacks, 445
- dictionary attacks, 444
- DoS (denial of service). *See* DoS (denial of service)
- flood attacks. *See* flood attacks
- malicious attacks. *See* malicious attacks
- zero day attacks, 161-162
- auditing**
- files, 478-481
- patch management, 99
- system security settings, 486-489
- audits**
- conducting, 478
- log file maintenance and security, 485-486
- logging, 481-484
- AUPs (acceptable usage policies), 629**
- authentication, 5, 7, 340**
- clouds, 201
- defined, 338
- localized authentication technologies, 348
- 802.1X, 348-350
- EAP (Extensible Authentication Protocol), 350-351*
- Kerberos, 352-354*
- LDAP (Lightweight Directory Access Protocol), 351-352*
- Remote Desktop Services, 354-355*
- mobile devices, 56
- passwords, 397-399
- remote authentication technologies, 356
- RADIUS (Remote Authentication Dial-In User Service), 360-361*
- RAS (Remote Access Service), 356-358*
- TACACS (Terminal Access Controller Access-Control System), 361*
- VPNs (virtual private networks), 358-360*
- summary of, 361
- usernames, 397-399
- authentication header (AH), 561**
- authentication models, 345-347**
- authorization, 5**
- defined, 338
- automated monitoring, 466**
- AutoRun, 24**
- AV (antivirus software), 28, 31**
- availability, 5**
- avoiding, risk, 424**

## B

- 
- back office applications, securing, 151**
- backdoors, 26-27**
- secure programming, 157
- wired networks and devices, 303
- backing up data, 104**
- backup generators, 581-582**
- considerations when selecting, 582
- backup rotation schemes, 593**
- backups, 590-594**
- schedules
- 10 tape rotation, 593*

- grandfather-father-son*, 593
- Towers of Hanoi*, 593-594
- tape backups, 590-591
- Windows Server, 592
- badware**, 34
- baiting**, 622
- bare metal**, 109
- Barracuda Spam Firewall**, 36
- baselines**, 102
  - creating, 432
  - performance baselining, 468-470
- battery backup**, 580
- battery-inverter generators**, 582
- behavior-based monitoring**, 467
- best practices**
  - access control models, 388-391
  - documentation, 641
- biometric readers**, 344-345
- BIOS**
  - configuring, 47
  - flashing, 47
  - passwords, 46-47
  - securing, 46-47
- birthday attacks**, 528-529
- BitLocker**, 48-49
- BitLocker Drive Preparation Tool**, 49
- Black Book Example**, 508-509
- black hats**, 9
- black-box testing**, 154, 433
- Blackhole exploit kit**, 25
- blackholes**, 239-240
- blacklists**, 37
- blackouts**, 578
- blind hijacking**, 242
- block ciphers**, 512
- Blowfish**, 518
- blue hats**, 9
- blue screen of death (BSOD)**, 637
- bluejacking**, 53, 319
- bluesnarfing**, 53, 319-320
- bluetooth**, 53
  - wireless networks, 318-319
- boot sector viruses**, 31
- botnets**, 25-26
  - mobile devices, 52
- brownouts**, 578
- browsers**, 126
  - Firefox, vulnerabilities, 128
  - IE (Internet Explorer), 128
  - Linux, 128
  - securing, 126-129
    - Chrome*, 145
    - Firefox*, 141-145
    - general security procedures*, 129
    - IE (Internet Explorer)*, 135-140
    - implementing policies*, 129-132
    - malicious code*, 135
    - proxies and content filters*, 133-135
    - Safari*, 145-146
    - training users*, 132-133
  - brute-force attacks, 444
- BSOD (blue screen of death)**, 637
- buffer overflows**, 157-158
- building security**, 340-342
  - door access, 342-344
  - hardware-based security tokens, 343
- business continuity plans, disaster recovery planning**, 597
- butt sets**, 308
- BYOD concerns, mobile devices**, 57-59

## C

---

- CA (certificate authority)**, 552-556
- cable media vulnerabilities**, 304
- CAC (Common Access Card)**, 343
- caching proxy, firewalls**, 275
- Caesar Cipher**, 509
- Cain & Abel password recovery tool**, 443
- California SB 1386**, 627
- captive portals**, 355
- case studies, analyzing test questions**, 671
- castle analogy**, 266-268
- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)**, 312
- CCTV (closed-circuit television)**, 341
- certificate keys**, 555
- certificate mapping**, 554
- certificate revocation list (CRL)**, 554
- certificate signing request (CSR)**, 553
- certificates**
  - PKI (public key infrastructure)**, 552
  - single-sided and dual-sided, 556

- change management**, 629-630
- CHAP (Challenge Handshake Authentication Protocol)**, 241, 356, 361
- CHARGEN**, 228
- cheat sheets**, 664
- chkdsk command**, 104
- chkrootkit**, 35
- Chrome**, securing, 145
- CIA (confidentiality, integrity, and availability)**, 2-5
- SDLC (systems development life cycle), 152
- ciphers**
  - block ciphers, 512
  - defined, 510-511
  - stream ciphers, 512
- circuit-level gateway**, 271
- classification of information, legislative policies and organizational policies**, 626-628
- classifying, RAID (redundant array of independent disks)**, 585
- clean machines**, 31
- clearing, disposing of computers and other equipment securely**, 636
- client-side attacks**, 244-245
- closed-circuit television (CCTV)**, 341
- closing, unnecessary ports**, 233-234
- cloud computing**, 198-200
- cloud computing services**, 199
- cloud security**, 200-202
- clouds**, 198
  - access policies, 201
  - authentication, 201
  - considerations when using, 202-203
  - encryption, 201
  - P2P networks, 202-203
  - passwords, 200-201
  - protecting data, 201
  - standardization of programming, 201
  - types of, 199-200
- clusters**
  - failover clusters, 588
  - load-balancing clusters, 588
- CO<sub>2</sub> extinguishers**, 613
- coaxial cable**, 304
- code injection, secure programming**, 159-161
- cold sites**, 589
- collection and preservation of evidence**, 638-639
- command ports**, 232
- Command Prompt**, 147
- command-line scripting**, 244
- Common Access Card (CAC)**, 343
- community clouds**, 200
- company policies**. *See organizational policies*
- compartmentalizing, subnetting**, 192-194
- computer forensics**, 639-641
- conducting, audits**, 478
- confidentiality**, 4
- configuration baselines, hardening operating systems**, 100-102
- configuring, BIOS**, 47
- connecting to punch blocks**, 308
- Connections tab, IE (Internet Explorer)**, 139
- consolidating accounts**, 393
- contact information, disaster recovery planning**, 596
- content filtering**, 185
- content filters, browsers**, 133-135
- Content tab, IE (Internet Explorer)**, 139
- cookies**
  - Firefox, 142
  - Flash cookies, 138
  - IE (Internet Explorer), 136-137
  - tracking cookies, 138
- copies of agreements, disaster recovery planning**, 597
- copying folders and files**, 397
- corrective controls**, 431
- CPU, monitoring**, 469
- CRCs (cyclic redundancy checks)**, 531
- CRL (certificate revocation list)**, 554-555
- cross-site request forgery (XSRF), secure programming**, 159
- cross-site scripting (XSS)**, 138
- crosstalk**, 305-306
- cryptanalysis attacks**, 445
- cryptographic hash functions**, 527
  - birthday attacks, 528-529
  - HMAC (Hash-based Message Authentication Code), 528
  - MD5 (Message-Digest algorithm 5), 527

RIPEMD (RACE Integrity Primitives Evaluation Message Digest), 528  
SHA (Secure Hash Algorithm), 527-528

**cryptography, 506-511**  
asymmetric key algorithms, 513  
defined, 510  
key management, 515  
public key cryptography, 513-514  
quantum cryptography, 522-523  
steganography, 515-516  
symmetric key algorithms, 512-513  
symmetric versus asymmetric key algorithms, 512

**CryptoLocker, 20-21**

**CSR (certificate signing request), 553**

**Ctrl+Alt+Del, 399**

**cyclic redundancy checks (CRCs), 531**

## D

---

**DAC (discretionary access control), 384-385**

**damage control, incident response procedures, 639**

**Darkleech, 206**

**data, 16**  
backing up, 104  
redundancy planning, 582-586

**data backups, 7-8, 590-594**  
tape backups, 590-591

**data emanation, 306-307**  
accessing, 308

**Data Encryption Standard (DES), 516**

**data labeling, 386**

**data loss prevention (DLP), 45, 278**

**data removal, 8**

**data sensitivity, legislative policies and organizational policies, 626-628**

**DCE Endpoint Resolution, 228**

**dcomscm, 228**

**DDoS (distributed denial-of-service), 25, 239, 247**

**Default Domain Policy, 400**

**defense in depth, 153**

**defragmenting drives, 104**

**delivering malicious software, 24**  
backdoors, 26-27  
botnets and zombies, 25-26

logic bombs, 27  
privilege escalation, 26  
via software, messaging, and media, 24-25

**demilitarized zone (DMZ), network design, 189-190**

**denying, access, 147**

**DES (Data Encryption Standard), 516**

**destruction, disposing of computers and other equipment securely, 636**

**detective controls, 431**

**DHE (Diffie-Hellman), 521**

**dictionary attacks, passwords, 444**

**differential backups, 591**

**Diffie-Hellman, 521**

**digital forensics, 639-641**

**digital rights management (DRM), 302**

**Digital Signature Algorithm (DSA), 522**

**digital signatures, 514**

**Directory Service log, 482**

**directory traversal, secure programming, 161**

**dirty power, 580**

**disaster recovery. *See DR (disaster recovery)***

**disaster recovery drills and exercises, 597**

**disaster recovery planning, 594-597**  
fires, 595  
floods, 595  
long-term power loss, 596  
loss of building, 596  
malicious attacks, 596  
policies, procedures, and information, 596-597  
theft, 596

**disaster-tolerant disk systems, 585**

**discretionary access control. *See DAC (discretionary access control)***

**disposing of computers and other equipment securely, 634-636**

**distributed denial-of-service (DDoS), 25**

**diversion theft, 619**

**D-Link router/firewall internet sessions, 272**

**DLP (data loss prevention), 45, 278**

**DMZ (demilitarized zone)**  
firewalls, 271  
network design, 189-190

**DNS (Domain Name System),** 228  
**DNS attacks,** 245-247  
**DNS logs,** 482  
**DNS poisoning,** 245-247  
**DNS Server logs,** 482  
**DNSBL (DNS blackhole list),** 239-240  
**documentation**  
  best practices, 641  
  final network documentation, 320  
  network documentation, 435  
**domain name kiting,** 246-247  
**door access,** 342-344  
**DoS (denial-of-service),** 236  
  flood attacks, 236-238  
  fork bomb, 238-239  
  permanent DoS attack, 238  
  POD (ping of death), 238  
  teardrop attacks, 238  
**double tagging,** 195  
**DR (disaster recovery),** 590  
  data backups, 590-594  
  planning, 594-597  
**drawbridges,** 266  
**drives, defragmenting,** 104  
**DRM (digital rights management),** 302  
**DSA (Digital Signature Algorithm),** 522  
**dual-sided certificates,** 556  
**due care,** 631  
**due diligence,** 631  
**due process,** 632  
**dumpster diving,** 622

## E

---

**EAP (Extensible Authentication Protocol),** 348-351  
**EAP-FAST,** 350  
**EAP-MD5,** 350  
**EAP-TLS,** 350  
**EAP-TTLS,** 350  
**easter eggs,** 27  
**eavesdropping,** 306, 622  
**ECC (elliptic curve cryptography),** 521-522  
**Echo,** 228  
**EDH (Ephemeral Diffie-Hellman),** 521  
**EFS (Encrypting File System),** 517

**electromagnetic interference (EMI),** 305  
**elite hackers,** 9-10  
**elliptic curve cryptography (ECC),** 521-522  
**e-mail servers,** 204-205  
**emergency response detail,** 638  
**EMI (electromagnetic interference),** 305  
**emulators,** 108  
**Encapsulating Security Payload (ESP),** 561  
**Encrypting File System (EFS),** 517  
**encryption,** 8, 30, 506  
  algorithms, 516  
    *3DES (Triple DES),* 516  
    *AES (Advanced Encryption Standard),* 517  
    *Blowfish,* 518  
    *DES (Data Encryption Standard),* 516  
    *RC (Rivest Cipher),* 518  
    *summary of,* 519  
    *Twofish,* 518  
  application security, mobile devices, 55  
  clouds, 201  
  defined, 510  
  mobile devices, 53  
  one-time pad, 523-524  
  PGP (Pretty Good Privacy), 524-525  
  weak encryption, wireless networks, 311-313  
  whole disk encryption, 48-50  
**encryption types,** 511  
**endpoint DLP systems,** 45  
**endpoint-based DLP,** 278  
**enterprise-level virtual software,** 111  
**environmental controls**  
  fire extinguishers, 612-613  
  fire suppression, 610-612  
  HVAC, 615-616  
  shielding, 616-617  
  special hazard protection systems, 614-615  
  sprinkler systems, 613-614  
**environments, monitoring,** 432  
**epap,** 228  
**ESP (Encapsulating Security Payload),** 561  
**Ethereal,** 441  
**Ethernet switching,** 183  
**evil twins,** 311  
**exams**  
  beyond certification, 670-671  
  case studies, analyzing test questions, 671  
  cheat sheets, 664  
  cheat sheets, 664

practice, 662-664  
tips for taking, 672

**Excel**, securing, 149

**Extensible Authentication Protocol.**  
*See EAP (Extensible Authentication Protocol)*

extranets, network design, 190-191

---

**F**

fail securely, 153

fail-closed, 577

fail-open, 577

failover clusters, 588

failover redundancy, 577

failure in time (FIT), 428

failure-resistant disk systems, 585

failure-tolerant disk systems, 585

false negatives authentication, 347

false negatives IDS (intrusion detection system), 42

false positives

- authentication, 347
- IDS (intrusion detection system), 42

**Faraday cages, 616-617**

**FCIP (Fiber Channel over Internet Protocol)**, 228

federated identity management (FIM), 346

**FEXT (far end crosstalk)**, 306

fiber-optic cable, 304

fiber-optic networks, passive optical splitters, 308-309

file permissions, 395

**File Replication Service log**, 482

file servers, 203-204

file systems, hardening, 103-105

files

- auditing, 478-481
- copying/moving, 397

filters, spam, 36

**FIM (federated identity management)**, 346, 393

**findstr**, 94

fingerprinting, 430

**Fire Class A**, 612

**Fire Class B**, 612

**Fire Class C**, 612

**Fire Class D**, 612

**Fire Class K**, 612

fire extinguishers, 612-613

fire suppression, environmental controls, 610-612

**Firefox**

- add-ons, 145
- Advanced option, 143
- cookies, 142
- General tab, 141
- HTTP proxies, 144
- Network tab, 143
- Options dialog box, 142
- privacy options, 142
- proxies, 144
- proxy connections, 144
- securing, 141-145
- Security option, 143
- vulnerabilities, 128

**fires, disaster recovery planning**, 595

**firewall logs**, 482-483

**firewalls**, 29, 268-274

- ALG (application-level gateway), 271
- all-in-one devices, 274
- caching proxy, 275
- circuit-level gateway, 271
- DLP (data loss prevention), 278
- DMZ (demilitarized zone), 271
- honeynets, 277-278
- honeypots, 277-278
- implementing, 268
- logging, 272
- NAT filtering, 271
- network firewalls, 274
- NIDS (network intrusion detection system), 279-280
- NIPS (network intrusion prevention system), 280-282
- packet filtering, 271
- personal software firewalls, 39-41
- proxy servers, 274-277
- Internet content filtering*, 276
- routers, protecting, 185
- rules, 270

**first responders**, 638

**FIT (failure in time)**, 428

**Flash cookies**, 138

flashing, BIOS, 47

**flood attacks**  
 fraggle, 237  
 Ping flood, 236  
 smurf attacks, 236  
 SYN flood, 237  
 UDP flood attacks, 237  
 Xmas attack, 238

**floods, disaster recovery planning**, 595

**folders, copying/moving**, 397

**fork bomb**, 238-239

**fraggle**, 237, 247

**fsck command**, Linux, 104

**FTP (File Transfer Protocol)**, 228

**FTP Data Connection**, 232

**FTP servers**, 207-208

**FTP, connections**, 233

**FTPS (FTP Secure)**, 228

**full backups**, 590  
 schedules, 592

**fuzz testing (fuzzing)**, 156

## G

---

**general security procedures, browsers**, 129

**General tab, Firefox**, 141

**generators**  
 backup generators, 581-582  
 permanently installed generators, 581

**genetic algorithms**, 525

**geotagging, mobile devices**, 56

**GLB (Gramm-Leach-Bliley Act)**, 627

**GMER**, 35

**Gnutella**, 272

**GPMC (Group Policy Management Console)**, 132

**GPS tracking, mobile devices**, 53

**Gramm-Leach-Bliley Act (GLB)**, 627

**grandfather-father-son, backup rotation schemes**, 593

**gray hats**, 9

**gray-box testing**, 155, 433

**group policies, hardening, operating systems**, 100-102

**Group Policy Editor**, 100

**Group Policy Management Console (GPMC)**, 132

**groups, access control models**, 391-395

**guessing passwords**, 444

## H

---

**hackers**, 8  
 black hats, 9  
 blue hats, 9  
 elite, 9-10  
 gray hats, 9  
 white hats, 9

**hard drives, hardening**, 103-105

**hardening**  
 file systems, 103-105  
 hard drives, 103-105  
 operating systems, 82-84  
*group policies, security templates, and configuration baselines*, 100-102  
*hotfixes*, 96-98  
*patch management*, 99-100  
*patches*, 96-98  
*removing unnecessary applications and services*, 84-92  
*service packs*, 92-95  
*Windows updates, patches, and hotfixes*, 95-96

**hardware, RAID (redundant array of independent disks)**, 585

**hardware security modules (HSMs)**, 50

**hardware-based security tokens**, 343

**Hash-based Message Authentication Code (HMAC)**, 528

**hashes**, 526  
 cryptographic hash functions, 527  
*birthday attacks*, 528-529  
*HMAC (Hash-based Message Authentication Code)*, 528  
*MD5 (Message-Digest algorithm 5)*, 527  
*RIPEMD (RACE Integrity Primitives Evaluation Message Digest)*, 528  
*SHA (Secure Hash Algorithm)*, 527-528

**LANMAN (LAN Manager)**, 529-531

**NTLM hash**, 531

**NTLMv2**, 531

**hashing passwords**, 531-533

**HAVA (Help America Vote Act of 2002)**, 627

**header manipulation**, 471

**Health Insurance Portability and Accountability Act (HIPPA)**, 627

heating systems, environmental controls, 615

**Help America Vote Act of 2002 (HAVA),** 627

**HID Global,** 343

**HIDS (host-based intrusion detection system),** 39-43, 279-280, 343

hierarchical list of critical systems, disaster recovery planning, 597

high-availability clusters, 588

**HIPAA (Health Insurance Portability and Accountability Act),** 627

**HMAC (Hash-based Message Authentication Code),** 528

**HMAC-based OTP (HOTP),** 532

hoaxes, 621

honeynets, 277-278

honeypots, 277-278

horizontal privilege escalation, 302

host-based intrusion detection system. *See HIDS (host-based intrusion detection system)*

hosts files, 246

hot sites, 589

hotfixes, hardening operating systems, 95-98

**HOTP (HMAC-based OTP),** 532

**HouseCall,** 31

**HSMs (hardware security modules),** 50, 520

**HTTP (Hypertext Transfer Protocol),** 55, 228

**HTTP proxies**

- browsers, 133-135
- Firefox, 144
- Firewalls, 275

**HTTPS (HTTP Secure),** 55

**HTTPS (Hypertext Transfer Protocol Secure),** 228, 559

hubs, network design, 182

**HVAC,** 615-616

**HVAC shielding,** 616

hybrid clouds, 200

hypervisor, 109-110

---

**I**

**IA (information assurance),** 424

**IaaS (infrastructure as a service),** 109, 199

**ICMP flood attack,** 236

**identification, defined,** 338

**identity proofing,** 340

**IDPSS (intrusion detection and prevention systems),** 43

**IDS (intrusion detection system),** 41-42

**IE (Internet Explorer),** 128

- ActiveX controls, 140
- Advanced tab, 139
- Connections tab, 139
- Content tab, 139
- cookies, 136-137
- Local Computer Policy, 130
- policies, 131
- pop-up blocking tools, 135
- pop-ups, 139
- Privacy tab, 139
- Programs tab, 139
- securing, 135-140
- Security features, 129
- security zones, 135-136
- SSL, 139
- Windows Update feature, 135

**IF-Then statements,** 511

**IKE (Internet Key Exchange),** 561

**IM spam,** 23

**IMAP,** 228

**impact assessment,** 425

**impact determination, disaster recovery planning,** 596

**implementing**

- firewalls, 268
- patch management, 99

**implicit deny,** 388-389

**inbound ports,** 226-228

**incident response procedures,** 636-642

- documentation, best practices, 641
- steps of, 637-639

**incremental backups,** 590-591

- schedules, 591

**information assurance (IA),** 424

**information security,** 5-8

**information service agreement (ISA),** 634

infrastructure as a service (IaaS), 199  
initial incident management process, 638  
integrity, 4-5  
interconnections, network design, 188  
interference  
  crosstalk, 305-306  
  data emanation, 306-307  
  wired networks and devices, 305  
Internet, network design, 189  
Internet content filtering, proxy servers, 276  
Internet filtering appliances, 276  
Internet Key Exchange (IKE), 561  
intranets, network design, 190-191  
intrusion detection and prevention systems (IDPSs), 43  
intrusion detection system. *See* IDS (intrusion detection system)  
intrusion prevention systems (IPS), 43, 185  
IP address spoofing, 240  
IP addresses, ports, 232-233  
IP proxy, 274-275  
IP security, 187  
ipfirewall, 40  
IP-PBX, 197  
IPS (intrusion prevention systems), 43  
IPsec, 561  
IPSS (intrusion prevention systems), 185  
iptables, 40  
IPv6 addresses, 187  
ISA (information service agreement), 634  
iSCSI (Internet Small Computer System Interface), 228  
ISO/IEC 27002:2005, 626  
ISP (internet service provider), redundancy planning, 587  
IT folder's permissions, 487

## J

---

jailbreaking, 146  
job rotation, 390, 630  
Junk E-mail Options, 36

## K

---

KDC (key distribution center), 353  
keeping well-maintained computers, 105-107  
Kerberos, 228, 352-354, 361, 512  
key distribution center (KDC), 353  
key escrow, 555  
key management, 515  
  mobile devices, 55  
keyloggers, 21  
keys  
  defined, 511  
  private keys, 511-512  
  public key cryptography, 513-514  
kill command, Linux, 91  
Knoppix, 32

## L

---

L2TP (Layer 2 Tunneling Protocol), 228, 358, 560  
LANMAN (LAN Manager), 529-531  
LANs (local area networks), network design, 188-189  
lattice-based access control, 386  
layers, OSI (Open Systems Interconnection) model, 180  
LDAP (Lightweight Directory Access Protocol), 228, 351-352, 361  
LDAP injection, 160, 204  
LDAP over TLSL, 228  
LEAP (Lightweight EAP), 351  
least privilege, 389-390  
legislative policies, 625  
  data sensitivity and classification of information, 626-628  
  personnel security policies, 628  
line conditioning devices, 580  
Linux  
  browsers, 128  
  file permissions, 395  
  kill command, 91  
  removing unnecessary applications and services, 90-91  
  System Monitor, 470

**LM Hash, Local Group Policy**, 530  
**load-balancing clusters**, 588  
**Local Computer Policy**, 479  
  IE (Internet Explorer), 130  
**Local Group Policy, LM Hash**, 530  
**localized authentication technologies**  
  802.1X, 348-350  
  EAP (Extensible Authentication Protocol),  
    350-351  
  Kerberos, 352-354  
  LDAP (Lightweight Directory Access  
    Protocol), 351-352  
  Remote Desktop Services, 354-355  
**locally shared objects (LSOs)**, 138  
**locking doors**, 342-344  
**log file maintenance and security**, 485-486  
**log files, securing**, 486  
**logging**  
  audits, 481-484  
  firewall logs, 482-483  
  firewalls, 272  
  verbose logging, 485  
**logic bombs**, 27  
**long-term power loss, disaster recovery  
  planning**, 596  
**loss of building, disaster recovery  
  planning**, 596  
**LSOs (locally shared objects)**, 138

## M

---

**MAC (mandatory access control)**, 386-387  
**MAC (Message Authentication Code)**, 528  
**MAC filtering**, 316  
**MAC flooding**, 183, 247  
  VLANs (virtual local area networks), 195  
**malicious attacks**  
  ARP poisoning, 247  
  blackholes, 239-240  
  DDoS (distributed denial-of-service), 239  
  disaster recovery planning, 596  
  DNS poisoning, 245-247  
  DoS (denial-of-service), 236  
    *fork bomb*, 238-239  
    *permanent DoS attack*, 238  
    *POD (ping of death)*, 238  
    *teardrop attacks*, 238  
  null sessions, 244  
  replay attacks, 243  
**session hijacking**, 241  
  *blind hijacking*, 242  
  MITB (*man-in-the-browser*), 242  
  MITM (*man-in-the-middle*), 242  
  *session theft*, 241  
  TCP/IP hijacking, 241-242  
    *watering hole attacks*, 242-243  
  sinkholes, 239-240  
  spoofing, 240-241  
  summary of network attacks, 247  
  transitive access and client-side attacks,  
    244-245  
**malicious code, securing against**, 135  
**malicious insiders, social engineering**,  
  618-619  
**malicious software**, 6, 18  
  delivering  
    *active interception*, 26  
    *backdoors*, 26-27  
    *botnets and zombies*, 25-26  
    *logic bombs*, 27  
    *privilege escalation*, 26  
    *via software, messaging, and media*, 24-25  
  DoS (denial-of-service), flood attacks,  
    236-238  
**Malicious Software Removal Tool**, 31  
**malware**  
  mobile devices, 51-52  
  preventing, 28, 38  
  troubleshooting, 28  
**malware threats**, 23  
**management controls**, 430  
**mandatory access control (MAC)**, 386-387  
**mandatory vacations**, 630-631  
**man-in-the-browser (MITB)**, 242, 247  
**man-in-the-middle (MITM)**, 242, 247  
**mantraps**, 622  
**manually monitoring**, 465-466  
**MD5 (Message-Digest algorithm 5)**, 527  
**MDM (mobile device management)**  
  platforms, 57  
**mean time between failure (MTBF)**, 587  
**mean time to failure (MTTF)**, 428  
**mean time to repair (MTTR)**, 428, 587  
**Message Authentication Code (MAC)**, 528  
**Message-Digest algorithm 5 (MD5)**, 527  
**Microsoft, IE (Internet Explorer)**, 128  
**Microsoft Developer Network (MSDN)**, 94

- Microsoft Endpoint Mapper**, 228
- Microsoft Sysinternals Rootkit Revealer**, 35
- Microsoft System Center Configuration Manager (SCCM)**, 86
- MIMO (multiple-input multiple-output)**, 315
- MITB (man-in-the-browser)**, 242, 247
- mitigating vulnerabilities**, 432
- MITM (man-in-the-middle)**, 242, 247
- mobile apps**, securing, 150
- mobile device management (MDM) platforms**, 57
- mobile devices**
- geotagging, 56
  - securing, 50
    - application security*, 54-57
    - botnets*, 52
    - BYOD concerns*, 57-59
    - malware*, 51-52
    - SIM cloning*, 52
    - theft*, 53-54
    - wireless attacks*, 53
- models**
- access control models. *See access control models*
  - authentication models, 345-347
- modems, network design**, 196
- monitoring**, 464-466
- anomaly-based monitoring, 466
  - automated monitoring, 466
  - behavior-based monitoring, 467
  - environments, 432
  - manually monitoring, 466
  - signature-based monitoring, 466
  - summary of methodologies, 467
- monitoring tools**, 467-468
- analytical tools, 475-477
  - Network Monitor, 472-474
  - performance baselining, 468-470
  - protocol analyzers, 470-471
  - SNMP (Simple Network Management Protocol), 474
  - Wireshark, 471-472
- moving folders and files**, 397
- MS-CHAP**, 356
- MSDN (Microsoft Developer Network)**, 94
- Ms-sql-s**, 228
- MTBF (mean time between failure)**, 587
- reliability, 428
- MTTF (mean time to failure)**, 428
- MTTR (mean time to repair)**, 428, 587
- multicast**, 187
- multifactor authentication**, 346
- multiple-input multiple-output**, 315
- 
- ## N
- 
- NAC (network access control)**, 192
- NAS (network attached storage)**, 48, 585
- NAT (network address translation)**, 110
- network design, 185-188
- NAT filtering**, 271
- National Institute of Standards and Technology (NIST)**, 430
- NCAS (National Cyber Awareness System)**, 51
- need-to-know**, 642
- Nessus**, 441
- NetBIOS**, 228
- netstat command**, 233
- network access control (NAC), network design**, 192
- network adapters, redundancy planning**, 586
- network address translation (NAT)**, 110
- network attached storage (NAS)**, 48
- network attacks**
- summary of network attacks, 247
  - wired networks and devices, 303
- network controllers, servers**, 204
- network design**, 178-180
- DMZ (demilitarized zone), 189-190
  - hubs, 182
  - Internet, 189
  - intranets and extranets, 190-191
  - LANs versus WANs, 188-189
  - modems, 196
  - NAC (network access control), 192
  - NAT (network address translation), 185-188
  - network devices, 182
  - network zones and interconnections, 188
  - OSI (Open Systems Interconnection) model, 180-181
  - PBX (private branch exchange) equipment, 197
  - routers, 184-185
  - subnetting, 192-194

switches, 182-184  
 telephony devices, 196  
 VLANs (virtual local area networks), 194-195  
 VoIP (voice over Internet Protocol), 197  
**network devices, network design**, 182  
**network DLP systems**, 45  
**network documentation**, 320, 435  
**network firewalls**, 274  
**network intrusion detection system (NIDS)**. *See NIDS (network intrusion detection system)*  
**network intrusion prevention system**. *See NIPS (network intrusion prevention system)*  
**network mapping**, 435-437  
**Network Monitor**, 472-474  
**network operations center (NOC)**, 196  
**network scanners**, 439  
**network shares**, Windows Server, 487  
**network sniffing**, 441-443  
**Network tab**, Firefox, 143  
**network zones**, network design, 188  
**network-based DLP**, 278  
**networking, redundancy planning**, 586-587  
**NEXT (near end crosstalk)**, 306  
**NIDS (network intrusion detection system)**, 41, 279-280  
 versus NIPS, 282  
 protocol analyzers, 282-283  
**NIPS (network intrusion prevention system)**, 279, 280-282  
 versus NIDS, 282  
 protocol analyzers, 282-283  
**NIST (National Institute of Standards and Technology)**, 430, 517  
 penetration testing, 433  
**Nmap**, 439  
**NNTP (Network News Transfer Protocol)**, 228  
**NOC (network operations center)**, 196  
**nonessential services**, 440  
**non-promiscuous mode**, 470  
**NoSQL**, 160  
**NTFS**, 103  
**NTFS permissions**, 394  
**NTLM hash**, 531

**NTLMv2**, 531  
**null sessions**, 244, 247

## O

---

**offboarding**, 631  
**offline**, 444  
**onboarding**, 631  
**one-time pad**, 523-524  
**one-time passwords (OTPs)**, 532  
**online**, 444  
**OOV (order of volatility)**, 640  
**open ports**, 440  
**Open Source Security Testing Methodology Manual (OSSTMM)**, 433  
**openfiles command**, 475  
**operating systems, hardening**, 82-84  
 group policies, security templates, and configuration baselines, 100-102  
 hotfixes, 96-98  
 patch management, 99-100  
 patches, 96-98  
 removing unnecessary applications and services, 84-92  
 service packs, 92-95  
 Windows updates, patches, and hotfixes, 95-96  
**operational controls**, 430  
**Options dialog box**, Firefox, 142  
**order of volatility (OOV)**, 640  
**organizational policies**, 625  
 AUPs (acceptable usage policies), 629  
 change management, 629-630  
 data sensitivity and classification of information, 626-628  
 disposing of computers and other equipment securely, 634-636  
 due care, 631  
 due diligence, 631  
 due process, 632  
 incident response procedures, 636-642  
 mandatory vacations, 630-631  
 offboarding, 631  
 onboarding, 631  
 personnel security policies, 628  
 privacy policies, 628-629  
 separation of duties, 630  
 user education and awareness, 632-633  
 vendors, dealing with, 633-634

**OS X Server, removing unnecessary applications and services**, 91

**OSI (Open Systems Interconnection) model**, 180-181

layers, 180

**OSSEC**, 42

**OSSTMM (Open Source Security Testing Methodology Manual)**, 433

**OTPs (one-time passwords)**, 532

outbound ports, 226-228

**Outlook**, securing, 149

**OVAL (Open Vulnerability and Assessment Language)**, 434

**OVAL Interpreter**, 434

## P

---

**P2P networks, clouds**, 202-203

**PaaS (platform as a service)**, 199

**packet capture, Wireshark**, 442

**packet capturing programs**, 470

**packet filtering**, 271

**passive optical splitters, fiber-optic networks**, 308-309

**passive security analysis**, 430

**Password Policy**, 400-401

**password recovery**, 444-445

**password-cracking programs**, 445

**passwords**, 397-399

analyzing, 443-445

BIOS, 46-47

clouds, 200-201

complexity and length, 401

hashing, 531-533

LM Hash, 530

NTLM hash, 531

OTPs (one-time passwords), 532

policies, 400

weak passwords, 300-301

**patch management, hardening, operating systems**, 99-100

**patches**, 96-98

hardening operating systems, 95-96

**PayPal**, 133

**PBX (private branch exchange) equipment, network design**, 197

**PDS (protected distribution system)**, 309

**PDUs (protocol data units)**, 181

**PEAP (Protected EAP)**, 350

**penetration testing**, 433-434

NIST (National Institute of Standards and Technology), 433

**people, redundancy planning**, 589-590

**performance baselining**, 468-470

**Performance Monitor in Windows**, 468

**permanent DoS attack**, 238

**permanently installed generators**, 581

**permission inheritance**, 396

**permissions**

access control models, 391-395

IT folder's permissions, 487

**persistent cookies**, 136

**Personal Identity Verification (PIV)**, 343

**personal software firewalls**, 39-41

**personally identifiable information (PII)**, 55, 628-629

**personnel security policies**, 628

summary of, 633

**PGP (Pretty Good Privacy)**, 524-525

**phishing**, 619-621

**phone cloning**, 52

**phone phishing**, 620

**PHP forms**, 155

**physical security**, 340

biometric readers, 344-345

door access, 342-344

general building and server room security, 340-342

**physical tampering, switches**, 183-184

**piggybacking**, 622

**PII (personally identifiable information)**, 55, 628-629

**Ping flood**, 236, 247

**ping of death (POD)**, 238, 247

**PIV (Personal Identity Verification)**, 343

**PKCS (Public-Key Cryptography Standards)**, 520

**PKI (public key infrastructure)**, 550-551

CA (certificate authority), 552-556

certificates, 552

*single-sided and dual-sided*, 556

security protocols, 557

*IPsec*, 561

*L2TP (Layer 2 Tunneling Protocol)*, 560

*PPTP (Point-to-Point Tunneling Protocol), 560*  
*S/MIME, 557*  
*SSH (Secure Shell), 559*  
*SSL/TLS, 558-559*  
 web of trust, 556

**planning**  
 DR (disaster recovery), 594-597  
 patch management, 99

**platform as a service (PaaS), 199**

**plugging into twisted-pair networks, 308**

**PNAC (port-based network access control), 348**

**POD (ping of death), 238, 247**

**policies, 102**  
 access control models, 400-401  
 disaster recovery planning, 596-597  
 implementing for browsers, 129-132  
 Run Only Specified Windows Applications Policy, 147

**POP3, 228, 233**

**pop-up blockers, 43-45**

**pop-up blocking tools, IE (Internet Explorer), 135**

**pop-ups, 132**  
 IE (Internet Explorer), 139

**port numbers, protocols, 232**

**port scanners, 441**

**port zero security, 234-235**

**port-based network access control (PNAC), 348**

**portable gas-engine generators, 581**

**ports, 224**  
 command ports, 232  
 inbound versus outbound, 226-228  
 IP addresses, 232-233  
 open ports, 440  
 port zero security, 234-235  
 protocols, 228-232  
 ranges, 225-226  
 unnecessary ports, closing, 233-234

**power**  
 dirty power, 580  
 long-term power loss, disaster recovery planning, 596  
 redundancy planning, 577-579

**power supplies, redundancy planning, 579**

**power supply failure, 578**

**PPTP (Point-to-Point Tunneling Protocol), 228, 358, 560**

**practice exam, 672**

**preparation for exams, 662-664**

**pretexting, 618**

**Pretty Good Privacy (PGP), 524-525**

**preventative controls, 431**

**preventing**  
 malware, 28, 38  
 rootkits, 35-36  
 spam, 36-38  
 spyware, 33-34  
 viruses, 28-32  
 worms and Trojan horses, 32

**previous logon notification, 402**

**principle of defense in depth, 153**

**principle of least privilege, 153, 389-390**

**prioritizing, vulnerabilities, 432**

**Privacy act of 1974, 627-629**

**privacy options, Firefox, 142**

**privacy policies, 628-629**

**Privacy tab, IE (Internet Explorer), 139**

**private branch exchange (PBX) equipment, network design, 197**

**private clouds, 199**

**private IPv4 ranges, 186**

**private keys, 511-512**

**private versus public IP, network design, 185-188**

**privilege, principle of least privilege, 153**

**privilege de-escalation, 303**

**privilege escalation, 26, 302-303**

**procedures, disaster recovery planning, 596-597**

**process virtual machine, 108**

**programming testing methods, 154-156**

**Programs and Features window, Windows 7, 84**

**Programs tab, IE (Internet Explorer), 139**

**promiscuous mode, 470**

**propagation, 396**

**protected distribution system (PDS), 309**

**protecting**  
 data, clouds, 201  
 routers, 184-185

**protocol analyzers**, 182  
 monitoring tools, 470-471  
 NIDS (network intrusion detection system), 282-283  
 NIPS (network intrusion prevention system), 282-283  
**protocol data units (PDUs)**, 181  
**protocols**, 224  
 EAP (Extensible Authentication Protocol).  
*See* EAP (Extensible Authentication Protocol)  
 exams, 235  
 LDAP (Lightweight Directory Access Protocol), 351-352  
 port numbers, 232  
 port ranges, 226  
 ports, 228-232  
 SNMP (Simple Network Management Protocol), 474  
 wireless protocols, 312  
**proxies**  
 browsers, 133-135  
 Firefox, 144  
**proxy connections**, Firefox, 144  
**proxy servers**, 133-135  
 firewalls, 274-277  
*Internet content filtering*, 276  
**PSTN (public switched telephone network)**, 197  
**public clouds**, 199  
**public key cryptography**, 513-514  
**public key infrastructure**. *See PKI (public key infrastructure)*  
**public keys**, 511  
**public switched telephone network (PSTN)**, 197  
**punch blocks**, connecting to, 308  
**purging, disposing of computers and other equipment securely**, 636

## Q

**QKD (quantum key distribution)**, 522-523  
**qualitative risk assessment**, 425-426, 428  
**quantitative risk assessment**, 426-428  
**quantum cryptography**, 522-523  
**quantum key distribution (QKD)**, 522-523

## R

---

**RA (registration authority)**, 555  
**RACE Integrity Primitives Evaluation Message Digest (RIPEMD)**, 528  
**radio frequency interference (RFI)**, 305  
**RADIUS (Remote Authentication Dial-In User Service)**, 228, 360-361  
**RAID (redundant array of independent disks)**, 583-586  
**RAID 0**, 583  
**RAID 0+1**, 583  
**RAID 1**, 578, 583  
**RAID 5**, 583-585  
**RAID 6**, 583  
**RAID 10**, 583  
**ranges, port ranges**, 226  
**ransomware**, 20-21  
**RAS (Remote Access Service)**, 356-358, 361  
**RATs (remote access Trojans)**, 20, 208  
**RBAC (role-based access control)**, 387, 393  
**RC (Rivest Cipher)**, 518  
**RC4**, 518  
**RC5**, 518  
**RC6**, 518  
**RCE (remote code execution)**, 158  
**RDP (Remote Desktop Protocol)**, 228, 354  
**recovery plans**  
 disaster recovery planning, 596  
 password recovery, 444-445  
**reduced sign-on**, 346  
**reducing risk**, 424  
**redundancy**, 574  
**redundancy planning**, 574-577  
 backup generators, 581-582  
 data, 582-586  
 networking, 586-587  
 people, 589-590  
 power, 577-579  
 power supplies, 579  
 servers, 587-588  
 sites, 588-589  
 UPS (uninterruptible power supplies), 579-581  
**registration authority (RA)**, 555  
**relationships**, 245

- reliability, MTBF (mean time between failure),** 428
  - Remote Access Services (RAS),** 356-358, 361
  - remote access Trojans (RATs),** 20
  - remote authentication technologies,** 356
  - RADIUS (Remote Authentication Dial-In User Service), 360-361
  - RAS (Remote Access Service), 356-358
  - TACACS (Terminal Access Controller Access-Control System), 361
  - VPNs (virtual private networks), 358-360
  - remote code execution, secure programming,** 158
  - Remote Desktop Services,** 354-355
  - remote lockout systems, mobile devices,** 54
  - remote ports, wired networks and devices,** 303
  - remote wipe programs, mobile devices,** 54
  - removable storage, securing,** 47-48
  - removing**
    - temporary files, 104
    - unnecessary applications and services, 84-92
  - replay attacks,** 243, 247
  - residual risk,** 425
  - restoration techniques,** 105
  - reverse proxies,** 276
  - RFI (radio frequency interference),** 305
  - RIPEMD (RACE Integrity Primitives Evaluation Message Digest),** 528
  - risk**
    - avoiding, 424
    - impact assessment, 425
    - reducing, 424
    - residual risk, 425
    - transferring, 424
  - risk acceptance,** 424
  - risk assessments,** 422-425
    - OVAL (Open Vulnerability and Assessment Language), 434
    - penetration testing, 433-434
    - qualitative risk assessment, 425-426
    - quantitative risk assessment, 426-428
    - security analysis, 429-430
    - security controls, 430-431
    - summary of, 428
    - vulnerability management, 431-433
  - risk avoidance,** 424
  - risk reduction,** 424
  - risk retention,** 424
  - risk sharing,** 424
  - risk transference,** 424
  - Rivest Cipher (RC),** 518
  - rogue access points, wireless networks,** 311
  - role-based access control (RBAC),** 387
  - rootkits,** 22
    - preventing and troubleshooting, 35-36
  - routers**
    - network design, 184-185
    - protecting, 184-185
  - RPC,** 228
  - RSA (Rivest, Shamir, and Adleman),** 519-520
  - rule-based access control,** 386
  - rules, firewalls,** 270
  - Run Only Specified Windows Applications Policy,** 147
- 
- ## **S**
- SA (security association),** 561
  - SaaS (software as a service),** 199
  - Safari, securing,** 145-146
  - Safe Mode,** 34
  - sags,** 578
  - sanitizing phones,** 54
  - Sarbanes-Oxley,** 627
  - SCCM (System Center Configuration Manager),** 86
  - schedules**
    - backups
      - 10 tape rotation,* 593
      - grandfather-father-son,* 593
      - Towers of Hanoi,* 593-594
    - full backups, 592
      - for incremental backups, 591
  - screen locks, mobile devices,** 54
  - SDLC (systems development life cycle),** 151-154, 430
    - CIA (confidentiality, integrity, and availability), 152
  - secret keys,** 510
  - secure defaults,** 153
  - Secure Hash Algorithm (SHA),** 527-528

- secure programming, 151**
  - programming testing methods, 154-156
  - systems development life cycle, 151-154
  - vulnerabilities and attacks, 156
    - arbitrary code execution/remote code execution, 158*
    - backdoors, 157*
    - buffer overflows, 157-158*
    - code injection, 159-161*
    - directory traversal, 161*
    - summary of, 162*
    - XSRF (cross-site request forgery), 159*
    - XSS (cross-site scripting), 159*
    - zero day attacks, 161-162*
- Secure Shell, 228**
- secure VPN connectivity, 185**
- securing**
  - applications, 147-149
  - back office applications, 151
  - BIOS, 46-47
  - browsers, 126-129
    - Chrome, 145*
    - Firefox, 141-145*
    - general security procedures, 129*
    - IE (Internet Explorer), 135-140*
    - implementing policies, 129-132*
    - malicious code, 135*
    - proxies and content filters, 133-135*
    - Safari, 145-146*
    - training users, 132-133*
  - Excel, 149
  - log files, 486
  - mobile apps, 150
  - mobile devices, 50
    - application security, 54-57*
    - botnets, 52*
    - BYOD concerns, 57-59*
    - malware, 51-52*
    - SIM cloning, 52*
    - theft, 53-54*
    - wireless attacks, 53*
  - Outlook, 149
  - storage devices, 47
    - HSMs (hardware security modules), 50*
    - NAS (network attached storage), 48*
    - removable storage, 47-48*
    - whole disk encryption, 48-50*
  - USB devices, 48
  - VMs (virtual machines), 110-111
  - wired networks and devices, 298
    - backdoors, 303*
    - cable media vulnerabilities, 304*
    - default accounts, 300*
- interference, 305**
- network attacks, 303**
- privilege escalation, 302-303**
- remote ports, 303**
- tapping into data and conversations, 307-309**
- Telnet, 304**
- vulnerabilities, 300**
- weak passwords, 300-301**
- wireless networks**
  - administration interface, 310*
  - bluejacking, 319*
  - bluesnarfing, 319-320*
  - bluetooth, 318-319*
  - evil twins, 311*
  - rogue access points, 311*
  - SSID (service set identifier) broadcast, 310*
  - VPNs, 314*
  - vulnerabilities, 317-318*
  - WAP (wireless access point), 314-317*
  - weak encryption, 311-313*
  - wireless access point vulnerabilities, 309*
  - WPS (Wi-Fi Protected Setup), 313*
- Word, 149**
- security, 2**
  - AAA (authentication, authorization, and accounting), 5**
  - CIA (confidentiality, integrity, and availability), 2-5**
  - information security, 5-8
  - log file maintenance and, 485-486
  - physical security. *See physical security*
  - port zero security, 234-235
- security analysis, risk assessments, 429-430**
- security applications**
  - DLP (data loss prevention), 45
  - personal software firewalls, 39-41
  - pop-up blockers, 43-45
- security applications HIDS (host-based intrusion detection system), 41-43**
- security association (SA), 561**
- security controls, 430-431**
- Security features, IE (Internet Explorer), 129**
- Security log, 481**
- security logs, Windows, 481**
- Security option, Firefox, 143**
- security permissions, access control models, 394**
- security plans, 6**

- security protocols, PKI (public key infrastructure), 557**
  - IPsec, 561
  - L2TP (Layer 2 Tunneling Protocol), 560
  - PPTP (Point-to-Point Tunneling Protocol), 560
  - S/MIME, 557
  - SSH (Secure Shell), 559
  - SSL/TLS, 558-559
- security templates, hardening, operating systems, 100-102**
- security threats, 16**
  - malicious software, 18
    - delivering, 24*
  - malware threats, 23
  - ransomware, 20-21
  - rootkits, 22
  - spam, 22-23
  - spyware, 21
  - Trojan horses, 20
  - viruses, 18-19
  - worms, 19
- security tools**
  - assessing vulnerabilities, 435
    - network mapping, 435-437*
    - network sniffing, 441-443*
    - password analysis, 443-445*
    - vulnerability scanning, 438-441*
  - summary of, 445
- security zones, IE (Internet Explorer), 135-136**
- separation of duties, 390, 630**
- separation of OS and data, 30**
- server rooms, 578**
  - security, 340-342
- servers**
  - e-mail servers, 204-205
  - file servers, 203-204
  - FTP servers, 207-208
  - network controllers, 204
  - redundancy planning, 587-588
  - web servers, 205-207
- service packs, 28**
  - hardening operating systems, 92-95
- services, stopping, 91**
- session hijacking**
  - blind hijacking, 242
  - MITB (man-in-the-browser), 242
  - MITM (man-in-the-middle), 242
  - session theft, 241
  - TCP/IP hijacking, 241-242
  - watering hole attacks, 242-243
- session theft, 241, 247**
- SFC (System File Checker), 104**
- SHA (Secure Hash Algorithm), 527-528**
- shielded twisted-pair (STP) cable, 616**
- shielding, 616-617**
- shoulder surfing, 621-622**
- SHTTP (Secure HTTP), 559**
- signature-based IDS, 42, 466**
- signature-based monitoring, 466**
- SIM cloning, 52**
- single loss expectancy (SLE), 426**
- single points of failure, redundancy planning, 576**
- single-sided certificates, 556**
- sinkholes, 239-240**
- sites, redundancy planning, 588-589**
- SLA (service-level agreement), 634**
- SLE (single loss expectancy), 426**
- smart cards, 343**
- SMB (Server Message Block, 228**
- S/MIME, 557**
- SMTP, 228**
- smurf attacks, 236, 247**
- SNMP (Simple Network Management Protocol), 228, 474**
- SNMPTRAP, 228**
- social engineering, 6, 617**
  - baiting, 622
  - diversion theft, 619
  - dumpster diving, 622
  - eavesdropping, 622
  - hoaxes, 621
  - malicious insiders, 618-619
  - phishing, 619-621
  - piggybacking, 622
  - pretexting, 618
  - shoulder surfing, 621-622
  - summary of social engineering types, 623
  - tailgating, 622
  - user education and awareness, 624
- social engineering attacks, 52**
- software**
  - anti-malware software, 7
  - antivirus software, 28, 31
  - malicious software, 6, 18
- software as a service (SaaS), 199**
- SOHO 802.11n, 315**

- SOHO routers, Syslog**, 483-484
  - SOX (Sarbanes-Oxley)**, 628
  - spam**
    - preventing and troubleshooting, 36-38
    - security threats, 22-23
  - spam firewalls/filters**, 36
  - spear fishing**, 620
  - special hazard protection systems**, 614-615
  - spectral analyzers**, accessing data emanations, 308
  - SPI (stateful packet inspection)**, 316
  - spikes**, 578
  - splitting twisted-pair connections**, 308
  - spoofing**, 240-241, 247
  - sprinkler systems**, 613-614
  - SPS (standby UPS)**, 580
  - spyware**, 21
    - preventing and troubleshooting, 33-34
    - symptoms of, 33-34
  - SQL**, 160
  - SSH (Secure Shell)**, 228, 559
  - SSID (service set identifier) broadcast**, wireless networks, 310
  - SSL, IE (Internet Explorer)**, 139
  - SSL/TLS**, 558-559
  - SSO (single sign-on)**, 346
    - web-based SSO, 347
  - standardization of programming, clouds**, 201
  - standby UPS (SPS)**, 580
  - stateful packet inspection (SPI)**, 316
  - statistical anomalies, IDS (intrusion detection system)**, 41
  - steganography**, 515-516
  - stopping, services**, 91
  - storage devices, securing**
    - HSMs (hardware security modules), 50
    - NAS (network attached storage), 48
    - removable storage, 47-48
    - whole disk encryption, 48-50
  - storage DLP systems**, 45
  - storage-based DLP**, 278
  - stream ciphers**, 512
  - subnetting, network design**, 192-194
  - surges**, 578
  - surveys**, 316
  - switch spoofing**, 195
  - switches**
    - MAC flooding, 183
    - network design, 182-184
    - physical tampering, 183-184
  - symmetric key algorithms**, 512-513
  - symmetric versus asymmetric key algorithms**, 512
  - symptoms of spyware**, 33-34
  - symptoms of viruses**, 30-31
  - SYN flood**, 237, 247
  - Syslog**, 228, 483
  - System and Application logs**, 482
  - System Center Configuration Manager (SCCM)**, 86
  - system failures**, 6
  - system files, checking**, 104
  - System Monitor**, 470
  - system security settings, auditing**, 486-489
  - system virtual machines**, 108
  - System window, Windows 7**, 93
  - systeminfo**, 94-96
  - systems development life cycle**. *See SDLC (systems development life cycle)*
- 
- ## T
- TACACS (Terminal Access Controller Access-Control System)**, 361
  - TACACS+ (Terminal Access Controller Access-Control System Plus)**, 228, 361
  - tailgating**, 622
  - tape backups**, 590-591. *See also backups*
  - tapping into data and conversations**, 307-309
  - Task Manager**, 91
  - taskkill command**, 91
  - TCP/IP hijacking**, 241-242
  - TDSSKiller**, 35
  - teardrop attacks**, 238, 247
  - technical controls**, 431
  - technical growth**, 670
  - telephony devices, network design**, 196
  - Telnet**, 87, 228
    - wired networks and devices, 304

**TEMPEST**, 617  
**tempoar**, removing, 104  
**Terminal Access Control Access-Control System (TACACS)**, 361  
**Terminal Services**, 354  
**TermService**, 354  
**testing**  
  black-box testing, 154  
  fuzz testing (fuzzing), 156  
  gray-box testing, 155  
  patch management, 99  
  penetration testing, 433-434  
  programming testing methods, 154-156  
  white-box testing, 154  
**TFTP (Trivial File Transfer Protocol)**, 88, 228  
*The Orange Book*, MAC (mandatory access control), 386  
**theft**  
  disaster recovery planning, 596  
  mobile devices, 53-54  
**think like a hacker**, 8-10  
**threat modeling**, 153  
**threats**. *See security threats*  
**time-based OTP (TOTP)**, 532  
**time-of-day restrictions**, access control models, 393  
**tips for test taking**, 667-670  
**TKIP (Temporal Key Integrity Protocol)**, 312, 518  
**tools**, monitoring tools, 467  
  analytical tools, 475-477  
  Network Monitor, 472-474  
  performance baselining, 468-470  
  protocol analyzers, 470-471  
  SNMP (Simple Network Management Protocol), 474  
  Wireshark, 471-472  
**TOTP (time-based OTP)**, 532  
**Towers of Hanoi**, 593-594  
**TPM (trusted platform module)**, 49, 520  
**tracking cookies**, 138  
**training users**, 37-38  
  browser security, 132-133  
**transfer switches**, 581  
**transferring risk**, 424  
**transitive access attacks**, 244, 247  
**transparent testing**, 154

**Trend Micro, OSSEC**, 42  
**Triple DES (3DES)**, 516  
**Tripwire**, 42  
**Trivial File Transfer Protocol (TFTP)**, 88  
**Trojan horses**, 20  
  preventing, 32  
**troubleshooting**  
  malware, 28  
  rootkits, 35-36  
  spam, 36-38  
  spyware, 33-34  
  Trojan horses, 32  
  viruses, 28-32  
  worms, 32  
**trusted platform module (TPM)**, 49  
  web of trust, 556  
**tunneling protocols, VPNs (virtual private networks)**, 358  
**twisted-pair**, 304  
**twisted-pair connections**, splitting wires, 308  
**twisted-pair networks**, plugging into, 308  
**Twofish**, 518  
**Type 1: Native, hypervisor**, 109  
**Type 2: Hosted, hypervisor**, 109  
**types of**  
  clouds, 199-200  
  virtualization, 107-109

## U

---

**UAC (User Account Control)**, 147, 403-404  
**UDP flood attacks**, 237  
**unauthorized access**, 6  
**unauthorized zone transfers**, 246-247  
**unicast**, 187  
**Unified Threat Management (UTM)**, 283, 360  
**uninterruptible power supplies**. *See UPS (uninterruptible power supplies)*  
**unnecessary applications and services**, removing, 84-92  
**unnecessary ports**, closing, 233-234  
**UPS (uninterruptible power supplies)**, 579-581  
**URL spoofing**, 240

**USB devices, securing**, 48  
**User Account Control (UAC)**, 147, 403-404  
**user awareness**, 7  
**user education and awareness**  
  organizational policies, 632-633  
  social engineering, 624  
**user error**, 24  
**user rights, access control models**, 392  
**usernames**, 397-399  
**users**  
  access control models, 391-395  
  training, 37-38  
  *browser security*, 132-133  
**UTM (Unified Threat Management)**, 283, 360

**V**


---

**vacations, organizational policies**, 630-631  
**vendors, dealing with, organizational policies**, 633-634  
**verbose logging**, 485  
**VeriSign certificates**, 553  
**VeriSign-issued certificates**, 553  
**Verisys**, 42  
**vertical privilege escalation**, 302  
**virtual appliances**, 108  
**virtual local area networks. *See* VLANs (virtual local area networks)**  
**virtual machines. *See* VMs (virtual machines)**  
**virtual systems**, 82  
**virtualization**  
  defined, 107  
  hypervisor, 109-110  
  securing, VMs (virtual machines), 110-111  
  types of, 107-109  
**viruses**, 18-19  
  boot sector viruses, 31  
  preventing, 28-32  
  symptoms of, 30-31  
  troubleshooting, 28-32  
**vishing**, 620  
**VLAN hopping**, 195, 247  
**VLANs (virtual local area networks), network design**, 194-195

**VMs (virtual machines)**, 107  
  process virtual machine, 108  
  securing, 110-111  
  system virtual machines, 108  
**VoIP (voice over Internet Protocol), network design**, 197  
**VPNs (virtual private networks)**, 358-360, 560  
  secure VPN connectivity, 185  
  tunneling protocols, 358  
  wireless networks, 314  
**vulnerabilities**  
  assessing with security tools  
  *network mapping*, 435-437  
  *network sniffing*, 441-443  
  *password analysis*, 443-445  
  *vulnerability scanning*, 438-441  
  cable media vulnerabilities, 304  
  Firefox, 128  
  mitigating, 432  
  prioritizing, 432  
  RDP (Remote Desktop Protocol), 354  
  secure programming, 156  
    *arbitrary code execution/remote code execution*, 158  
    *backdoors*, 157  
    *buffer overflows*, 157-158  
    *code injection*, 159-161  
    *directory traversal*, 161  
    *XSRF (cross-site request forgery)*, 159  
    *XSS (cross-site scripting)*, 159  
    *zero day attacks*, 161-162  
  wired networks and devices, 300  
  wireless access point vulnerabilities, 309  
  wireless networks, 317-318  
**vulnerability assessments**, 422  
**vulnerability management**, 431-433  
**vulnerability scanning**, 438-441

**W**


---

**WANs (wide area networks), network design**, 188-189  
**WAP (wireless access point)**, 318  
  wireless networks, 314-317  
**warm sites**, 589  
**watering hole attacks**, 242-243, 247  
**weak encryption, wireless networks**, 311-313  
**weak passwords**, 300-301

**web of trust**, 556  
**web servers**, 205-207  
**web-based SSO**, 347  
**websites**, redundancy planning, 588-589  
**well-maintained computers**, keeping, 105-107  
**WEP (Wired Equivalent Privacy)**, 312  
**whaling**, 620  
**white hats**, 9  
**white-box testing**, 154, 433  
**whitelists**, 37  
**whole disk encryption**, 48-50, 105  
**Windows**  
  Performance Monitor, 468  
  security logs, 481  
**Windows 7**  
  Programs and Features window, 84  
  System window, 93  
**Windows Encrypting File System (EFS)**, 517  
**Windows Firewall**, 39-40, 89  
**Windows log files**, 482  
**Windows Server**, 147-149  
  backups, 592  
  network shares, 487  
**Windows Server Security Log Properties dialog box**, 485  
**Windows Update feature**, IE (Internet Explorer), 135  
**Windows updates**, hardening, operating systems, 95-96  
**Windows XP**, 86-87  
**winver command**, 94  
**wired networks and devices**, securing, 298  
  backdoors, 303  
  cable media vulnerabilities, 304  
  default accounts, 300  
  interference, 305  
  network attacks, 303  
  privilege escalation, 302-303  
  remote ports, 303  
  tapping into data and conversations, 307-309  
  Telnet, 304  
  vulnerabilities, 300  
  weak passwords, 300-301  
**wireless access point vulnerabilities**, 309

**wireless attacks**, mobile devices, 53  
**wireless networks**, securing  
  administration interface, 310  
  bluejacking, 319  
  bluesnarfing, 319-320  
  bluetooth, 318-319  
  evil twins, 311  
  rogue access points, 311  
  SSID (service set identifier) broadcast, 310  
  VPNs, 314  
  vulnerabilities, 317-318  
  WAP (wireless access point), 314-317  
  weak encryption, 311-313  
  wireless access point vulnerabilities, 309  
  WPS (Wi-Fi Protected Setup), 313  
**wireless point-to-multipoint layout**, 315  
**wireless protocols**, 312  
**Wireshark**, 441, 471-472  
**WLANs**, 315  
**Word**, securing, 149  
**World Wide Name (WWN)**, 241  
**worms**, 19  
  preventing, 32  
**WPA (Wi-Fi Protected Access)**, 312  
**WPA2 (Wi-Fi Protected Access Version 2)**, 312  
**WPS (Wi-Fi Protected Setup)**, 313  
**WWN (World Wide Name)**, 241

## X-Y

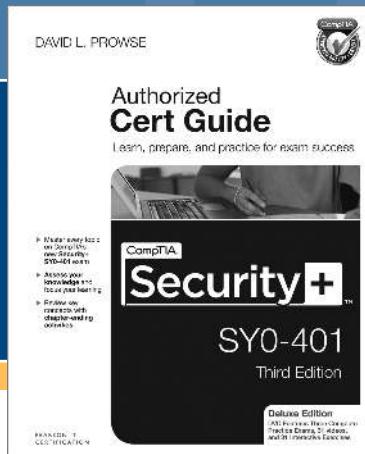
---

**X.509**, certificates, 552  
**Xmas attack**, 238  
**XML injection**, 160  
**XSRF (cross-site request forgery)**, secure programming, 159  
**XSS (cross-site scripting)**, 138, 243  
  secure programming, 159

## Z

---

**zero day attacks**, secure programming, 161-162  
**ZeroAccess botnet**, 26  
**zombies**, 25-26  
**zone transfers**, 246  
**ZoneAlarm**, 40



# FREE Online Edition

Your purchase of **CompTIA Security+ SY0-401 Authorized Cert Guide, Deluxe Edition** includes access to a free online edition for 45 days through the Safari Books Online subscription service. Nearly every Pearson IT book is available online through Safari Books Online, along with thousands of books and videos from publishers such as Addison-Wesley Professional, Cisco Press, Exam Cram, IBM Press, O'Reilly Media, Prentice Hall, Que, Sams, and VMware Press.

Safari Books Online is a digital library providing searchable, on-demand access to thousands of technology, digital media, and professional development books and videos from leading publishers. With one monthly or yearly subscription price, you get unlimited access to learning tools and information on topics including mobile app and software development, tips and tricks on using your favorite gadgets, networking, project management, graphic design, and much more.

**Activate your FREE Online Edition at  
[informit.com/safarifree](http://informit.com/safarifree)**

**STEP 1:** Enter the coupon code: WTXCIWH.

**STEP 2:** New Safari users, complete the brief registration form.  
Safari subscribers, just log in.

If you have difficulty registering on Safari or accessing the online edition,  
please e-mail [customer-service@safaribooksonline.com](mailto:customer-service@safaribooksonline.com)



Adobe Press



Cisco Press



Microsoft  
Press



O'REILLY



Peachpit  
Press



PRENTICE  
HALL



SAMS



vmware PRESS



WILEY



*This page intentionally left blank*

# View Recommended Resources

This document shows all of the links from each chapter plus some extra resources that you might find useful. Keep in mind that Internet links can change over time, and resources can be removed from the Internet without notice. If the link does not work, try searching within your search engine for the resource in question, or a similar resource to take its place.

## Chapter 1

AAA RFC documents:  
<http://tools.ietf.org/wg/aaa/>

## Chapter 2

For readers who want to brush up on their CompTIA A+ topics:

- Prowse, David L. *CompTIA A+ Exam Cram*:  
<http://www.pearsonitcertification.com/store/comptia-a-plus-220-801-and-220-802-authorized-exam-9780789749710>
- Prowse, David L. *CompTIA A+ Exam Cram Practice Questions*:  
<http://www.pearsonitcertification.com/store/comptia-a-plus-220-801-and-220-802-authorized-practice-9780789749741>

Links to anti-malware products:

- McAfee Total Protection:  
<http://home.mcafee.com/store/total-protection>
- Norton Internet Security:  
<http://us.norton.com/internet-security/>
- Kaspersky Anti-Virus:  
<http://usa.kaspersky.com/products-services/home-computer-security/anti-virus/>

Windows Firewall with Advanced Security Tutorial:  
<http://www.davidlprowse.com/articles/?p=896>

ZoneAlarm Firewall:

<http://www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm>

Knoppix Live Linux CD:

<http://knoppix.net/>

Windows Defender:

<http://windows.microsoft.com/en-us/windows7/products/features/windows-defender>

Barracuda Networks:

<http://www.barracuda.com>

Windows Sysinternals RootkitRevealer (for Windows systems):

<http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx>

chkrootkit (for UNIX-based systems):

<http://www.chkrootkit.org/>

Microsoft: “Windows BitLocker Drive Encryption Step-by-Step Guide”:

[http://technet.microsoft.com/en-us/library/cc766295\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc766295(WS.10).aspx)

National Cyber Alert System links:

- <http://www.us-cert.gov/cas/tips/ST05-017.html>
- <http://www.us-cert.gov/cas/tips/ST04-020.html>

Trend Micro OSSEC:

<http://www.ossec.net>

Verisys:

<http://www.ionx.co.uk/products/verisys>

Tripwire:

<http://www.tripwire.com/it-security-software/scm/file-integrity-monitoring/>

Adblock Plus (add-on):

<https://adblockplus.org/en/chrome>

IronKey:

<http://www.ironkey.com/>

Microsoft Malicious Software Removal Tool:

<http://www.microsoft.com/security/pc-security/malware-removal.aspx>

TrendMicro HouseCall:

<http://housecall.trendmicro.com/>

Malwarebytes Anti-Malware:

<http://www.malwarebytes.org/>

Microsoft Safety Scanner:

<http://www.microsoft.com/security/scanner/en-us/default.aspx>

Spybot Search & Destroy:

<http://www.safer-networking.org/private/>

Combofix:

<http://www.combofix.org/>

Microsoft Virtual PC 2007:

<http://www.microsoft.com/en-us/download/details.aspx?id=4580>

Microsoft Virtual PC 2007 SP1:

<http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=24439>

Windows Virtual PC:

<http://www.microsoft.com/en-us/download/details.aspx?id=3702>

Oracle VM VirtualBox:

<http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html?ssSourceSiteId=ocomcz>

## Chapter 3

Linux MAN pages:

- <http://www.linuxmanpages.com/>
- <http://linux.die.net/man/>

Microsoft Virtual PC 2007:

<http://www.microsoft.com/en-us/download/details.aspx?id=4580>

Microsoft Virtual PC 2007 SP1:

<http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=24439>

Windows Virtual PC:

<http://www.microsoft.com/en-us/download/details.aspx?id=3702>

Oracle VM VirtualBox:

<http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html?ssSourceSiteId=ocomcz>

VMware:

<http://www.vmware.com/>

Microsoft: “Hyper-V Security Guide”:

<http://technet.microsoft.com/en-us/library/dd569113.aspx>

Using and securing VMware:

<http://www.vmware.com/products/vsphere/resources.html>

## Chapter 4

Firefox add-on links:

- Adblock Plus Firefox add-on:

<https://addons.mozilla.org/en-US/firefox/addon/1865/>

- NoScript Firefox add-on:

<https://addons.mozilla.org/en-US/firefox/addon/722/>

FileZilla Server download:

[https://filezilla-project.org/download.php?show\\_all=1&type=server](https://filezilla-project.org/download.php?show_all=1&type=server)

FileZilla Client download:

[https://filezilla-project.org/download.php?show\\_all=1](https://filezilla-project.org/download.php?show_all=1)

CERT As-if Infinitely Ranged (AIR) integer model download:

<http://www.cert.org/secure-coding/tools/integral-security.cfmhttp://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9299>

## Chapter 5

For readers who wish to brush up on their networking topics:

- Comer, Douglas. *Computer Networks and Internets* (Sixth Edition). Prentice Hall. 2014.

- Video: “OSI Model Primer”:

<http://www.davidlprowse.com/articles/?p=905>

- Cisco: “Internetworking Basics”:

<http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-Internet.html>

Trend Cloud Security Blog:

<http://cloudsecurity.trendmicro.com/>

FreeNAC:

<http://freenac.net/>

Pure-FTPd:

<http://www.pureftpd.org>

FileZilla:

<http://filezilla-project.org/>

GRC's ShieldsUP!:

<http://www.grc.com>

More information on SYN flood attacks:

<http://tools.ietf.org/html/rfc4987>

Rackspace Cloud Knowledge Center:

[http://www.rackspace.com/knowledge\\_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas](http://www.rackspace.com/knowledge_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas)

Microsoft Security Bulletin: "Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930)":

<http://technet.microsoft.com/en-us/security/bulletin/ms11-013>

**NOTE** For more vulnerabilities to IIS (and other Microsoft software), visit the Security TechCenter, and bookmark the following link:

<http://technet.microsoft.com/en-US/security/bb291012>

**NOTE** A list of common vulnerabilities and exposures (CVE) to Apache HTTP Server (and the corresponding updates) can be found at the following link:

[http://httpd.apache.org/security/vulnerabilities\\_22.html](http://httpd.apache.org/security/vulnerabilities_22.html)

Netcraft Automated Vulnerability Scanning:  
<http://www.netcraft.com/security-testing/audited/>

## Chapter 6

Port numbers:

<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

Video: "TCP, UDP, and Ports Refresher":

<http://www.davidlprowse.com/articles/?p=911>

Nmap:

<http://nmap.org/>

ShieldsUP!:

<http://www.grc.com>

## Chapter 7

Video: “Setting up virtual servers and port forwarding on a typical SOHO router/firewall”:

<http://www.davidlprowse.com/articles/?p=916>

Adding firewall rules with netsh.exe:

[http://technet.microsoft.com/en-us/library/dd734783\(v=ws.10\).aspx#BKMK\\_3\\_add](http://technet.microsoft.com/en-us/library/dd734783(v=ws.10).aspx#BKMK_3_add)

iptables MAN page:

<http://ipset.netfilter.org/iptables.man.html>

## Chapter 8

NetStumbler:

<http://www.netstumbler.com/>

Some decent security websites (there are many more!):

- SecurityFocus: <http://www.securityfocus.com/>
- CERT: <http://www.cert.org/>

The Password Meter:

<http://www.passwordmeter.com/>

Microsoft Password Checker:

<https://www.microsoft.com/security/pc-security/password-checker.aspx>

D-Link wireless router emulator:

<http://support.dlink.com/Emulators/dir655/index.html>

## Chapter 9

Recommended reading:

Harper, Jim. “Identity Crisis: How Identification is Overused and Misunderstood.” Cato Institute. 2006.

HID door access control systems:

<http://www.hidglobal.com/products/readers>

Microsoft Trust Transitivity:

[http://technet.microsoft.com/en-us/library/cc739693\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc739693(v=ws.10).aspx)

#### 802.1X links:

- Official IEEE 802.1X PDF download:  
<http://standards.ieee.org/getieee802/download/802.1X-2004.pdf>
- Intel: “Wireless Networking” (802.1X overview):  
<http://www.intel.com/support/wireless/wlan/sb/cs-008413.htm>
- Cisco: “Deploying 802.1X Technology with Cisco Integrated Services Routers”:  
[http://www.cisco.com/en/US/prod/collateral/routers/ps5853/prod\\_white\\_paper0900aecd806c6d65.html](http://www.cisco.com/en/US/prod/collateral/routers/ps5853/prod_white_paper0900aecd806c6d65.html)
- Open1X:  
<http://open1x.sourceforge.net/>

#### LDAP links:

- IETF Technical Specifications (RFC 4510):  
<http://tools.ietf.org/html/rfc4510>
- OpenLDAP:  
<http://www.openldap.org/>
- Microsoft: “How to enable LDAP over SSL with a third-party certification authority”:  
<http://support.microsoft.com/kb/321051>

#### Kerberos links:

- Microsoft: “Kerberos Explained”:  
<http://technet.microsoft.com/en-us/library/bb742516.aspx>
- “Kerberos: The Network Authentication Protocol”:  
<http://web.mit.edu/Kerberos/>
- MIT Kerberos Consortium:  
<http://www.kerberos.org/>

#### RAS links:

- Microsoft: “RAS Security”:  
<http://technet.microsoft.com/en-us/library/cc751466.aspx>
- List of Microsoft dial-up and VPN error codes:  
<http://support.microsoft.com/kb/824864>

#### RADIUS and TACACS+ links:

- Microsoft: “RADIUS Protocol Security and Best Practices”:  
<http://technet.microsoft.com/en-us/library/bb742489.aspx>

- Free GNU RADIUS:  
<http://www.gnu.org/software/radius/>
- The FreeRADIUS Project:  
<http://freeradius.org/>
- Cisco: “TACACS+ and RADIUS Comparison”:  
[http://www.cisco.com/en/US/tech/tk59/technologies\\_tech\\_note09186a0080094e99.shtml](http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml)

## Chapter 10

“Department of Defense Trusted Computer System Evaluation Criteria” (TCSEC), aka The Orange Book:

<http://csrc.ncsl.nist.gov/publications/secpubs/rainbow/std001.txt>

Department of Defense Directive 8500.01E (replacement for the TCSEC):  
<http://dodcio.defense.gov/Portals/0/Documents/DIEA/850001p.pdf>

“An Introduction to Role-Based Access Control” (NIST/ITL bulletin):

[http://csrc.nist.gov/groups/SNS/rbac/documents/design\\_implementation/Intro\\_role\\_based\\_access.htm](http://csrc.nist.gov/groups/SNS/rbac/documents/design_implementation/Intro_role_based_access.htm)

Password checking resources:

- Microsoft: “Password Best Practices”:  
<http://technet.microsoft.com/en-us/library/cc784090.aspx>
- Microsoft: “User Account Control Step-by-Step Guide”:  
<http://technet.microsoft.com/en-us/library/cc709691%28WS.10%29.aspx>

## Chapter 11

ISO 31000:2009: “Risk Management—Principles and Guidelines” download:  
[http://www.iso.org/iso/catalogue\\_detail.htm?csnumber=43170](http://www.iso.org/iso/catalogue_detail.htm?csnumber=43170)

Open Source Security Testing Methodology Manual (OSSTMM) download:  
<http://www.isecom.org/research/osstmm.html>

NIST Special Publication 800-12: “An Introduction to Computer Security: The NIST Handbook”:

<http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter1.html>

NIST Special Publication 800-115: “Technical Guide to Information Security Testing and Assessment”:

<http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>

Link to all NIST Special Publication 800 Series documents (SP800):  
<http://csrc.nist.gov/publications/PubsSPs.html>

Open Vulnerability and Assessment Language repository website:  
<http://oval.mitre.org/>

Open Vulnerability and Language Assessment (OVAL) download:  
<http://oval.mitre.org/language/version5.7/>

Network Topology Mapper trial download:  
<http://www.solarwinds.com/lansurveyor-to-network-topology-mapper-2013.aspx>

Microsoft Visio trial:  
<http://office.microsoft.com/en-us/visio/>

Spiceworks:  
<http://www.spiceworks.com/app/>

PRTG Network Monitor  
<http://www.paessler.com/prtg>

Nessus Vulnerability Scanner:  
<http://www.tenable.com/products/nessus/nessus>

Nmap:  
<http://nmap.org/>

McAfee SuperScan:  
<http://www.mcafee.com/us/downloads/free-tools/superscan.aspx>

Angry IP Scanner:  
<http://angryip.org/>

Wireshark protocol analyzer:  
<http://www.wireshark.org/>

NetTool Inline Network Tester:  
<http://www.flukenetworks.com/enterprise-network/network-testing/NetTool-Series-II-Inline-Network-Tester>

Cain & Abel password recovery tool:  
<http://www.oxid.it/cain.html>

John the Ripper password recovery tool:  
<http://www.openwall.com/john/>

## Chapter 12

Windows Server 2008: Windows Reliability and Performance Monitor:  
<http://technet.microsoft.com/en-us/library/cc755081%28WS.10%29.aspx>

Wireshark download:  
<http://www.wireshark.org/download.html>

Wireshark tutorial:  
<http://www.wireshark.org/news/20060714.html>

Microsoft: “How to capture network traffic with Network Monitor”:  
<http://support.microsoft.com/kb/148942>

Microsoft Systems Management Server (SMS) 2003 information:  
<http://technet.microsoft.com/en-us/library/cc181833.aspx>

Microsoft System Center Configuration Manager (SCCM) 2007:  
<http://www.microsoft.com/systemcenter/en/us/configuration-manager.aspx>

Net-SNMP:  
<http://www.net-snmp.org/>

Windows Server “Event Logging and Viewing”:  
<http://technet.microsoft.com/en-us/library/bb726966.aspx>

Microsoft “How to create and delete hidden or administrative shares on client computers”:  
<http://support.microsoft.com/kb/314984>

Microsoft Network Monitor for Windows Server 2008:  
<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=4865>

## Chapter 13

Recommended books:

*Introduction to Modern Cryptography: Principles and Protocols.* Katz, Lindell. Chapman and Hall, 2007.

*Applied Cryptograph: Protocols, Algorithms, and Source Code in C.* Schneier, Bruce. Wiley, 1996.

*Cryptography Demystified.* Hershey. McGraw-Hill Professional, 2002.

*Practical Cryptography.* Ferguson. Wiley, 2003.

*Hiding in Plain Sight.* Cole. Wiley, 2003.

*Malicious Cryptography: Exposing Cryptovirology.* Young, Yung. Wiley, 2004.

*Privacy on the Line: The Politics of Wiretapping and Encryption.* Diffie, Landau. The MIT Press, 2010.

*Schneier on Security.* Schneier. Wiley, 2008.NIST: “Data Encryption Standard (DES)”:  
<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>

NIST: “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher”:

<http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf>

NIST: “Advanced Encryption Standard (AES)”:

<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

Microsoft: “Configure Server Authentication and Encryption Levels”: Concerns RDS Encryption:

<http://technet.microsoft.com/en-us/library/cc770833.aspx>

RSA Public Key Cryptography Standards (PKCS):

<http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm>

RSA Laboratories: RC6 Block Cipher:

<http://www.emc.com/emc-plus/rsa-labs/historical/rc6-block-cipher.htm>

Disabling the storage of LM hashes in Windows:

<http://support.microsoft.com/kb/299656>

Bruce Schneier Blog:

<http://www.schneier.com/>

## Chapter 14

Microsoft: “Configuring the Key Recovery Agent Certificate”:

<http://technet.microsoft.com/en-us/library/cc780525%28WS.10%29.aspx>

## Chapter 15

Thermaltake redundant power supply:

<http://www.thermaltakeusa.com/store/ProductPrint.aspx?C=1016&ID=2221>

APC enterprise-level UPS devices:

<http://www.apc.com/products/family/index.cfm?id=163>

Gillette Generators:

<http://www.gillettegenerators.com/>

Generac generators:

<http://www.generac.com/Commercial/>

Intel PRO/1000 MT Dual Port Server Adapter:

<http://www.intel.com/products/server/adapters/pro1000mt-dualport/pro1000mt-dualport-overview.htm>

Microsoft: “How multiple adapters on the same network are expected to behave”:  
<http://support.microsoft.com/kb/175767>

Microsoft: “Data Backup and Recovery”:

<http://technet.microsoft.com/en-us/library/bb727010.aspx>

DuPont FM-200 web page:

[http://www2.dupont.com/FE/en\\_US/products/FM200.html](http://www2.dupont.com/FE/en_US/products/FM200.html)

## Chapter 16

ISO/IEC 27002:2005: “Information technology—Security techniques—Code of practice for information security management”:

[http://www.iso.org/iso/catalogue\\_detail?csnumber=50297](http://www.iso.org/iso/catalogue_detail?csnumber=50297)

ISO/IEC 27002:2013:

[http://www.iso.org/iso/home/store/catalogue\\_ics/catalogue\\_detail\\_ics.htm?csnumber=54533](http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533)

ISO 9001:2008: “Quality management systems – Requirements”:

[http://www.iso.org/iso/catalogue\\_detail?csnumber=46486](http://www.iso.org/iso/catalogue_detail?csnumber=46486)

Privacy Act of 1974:

[http://epic.org/privacy/laws/privacy\\_act.html](http://epic.org/privacy/laws/privacy_act.html) and <http://www.justice.gov/opcl/privacyact1974.htm>

SpinRite data recovery software:

<http://www.grc.com/sr/spinrite.htm>

Kroll Ontrack data recovery software:

<http://www.ontrackdatarecovery.com/file-recovery-software/>

Journal of Digital Forensics, Security and Law:

<http://www.jdfsl.org/>

The International Journal of Forensic Computer Science:

<http://www.ijofcs.org/>

Shon Harris: “CISSP Video Mentor”:

<http://www.pearsonitcertification.com/store/product.aspx?isbn=0789740303>

*This page intentionally left blank*

# Master List of Key Topics

**Table 1-1** Key Topics for Chapter 1

| <b>Key Topic Element</b> | <b>Description</b>                                           | <b>Page Number</b> |
|--------------------------|--------------------------------------------------------------|--------------------|
| Figure 1-1               | The CIA of computer security                                 | 4                  |
| Bulleted list            | Definitions of confidentiality, integrity, and availability  | 4                  |
| Bulleted list            | Definitions of authentication, authorization, and accounting | 5                  |
| Bulleted list            | Definitions of the different types of hacker “hats”          | 9                  |

**Table 2-4** Key Topics for Chapter 2

| <b>Key Topic Element</b> | <b>Description</b>                       | <b>Page Number</b> |
|--------------------------|------------------------------------------|--------------------|
| Bulleted list            | Types of viruses                         | 19                 |
| Table 2-1                | Summary of malware threats               | 23                 |
| Table 2-2                | Summary of malware prevention techniques | 38                 |
| Figure 2-3               | BIOS and drive lock passwords            | 46                 |
| Table 2-3                | Summary of mobile device security        | 59                 |

**Table 3-2** Key Topics for Chapter 3

| <b>Key Topic Element</b> | <b>Description</b>                                               | <b>Page Number</b> |
|--------------------------|------------------------------------------------------------------|--------------------|
| Figure 3-2               | Services window in Windows XP                                    | 87                 |
| Figure 3-3               | Telnet Properties dialog box                                     | 88                 |
| Figure 3-4               | Stopping and disabling a service in the Windows 7 Command Prompt | 89                 |
| Table 3-1                | Summary of ways to stop services                                 | 92                 |
| Bulleted list            | Windows Update options                                           | 96                 |
| Figure 3-7               | <code>systeminfo</code> command in Windows                       | 97                 |
| Bulleted list            | Patch management four steps                                      | 99                 |
| Figure 3-9               | Local Group Policy Editor in Windows 7                           | 100                |
| Figure 3-10              | Windows Server 2012 Import Policy From window                    | 101                |
| Bulleted list            | Maintaining a hard disk                                          | 104                |
| Numbered list            | Keeping a well-maintained computer                               | 105                |
| Bulleted list            | Types of hypervisors                                             | 109                |

**Table 4-3** Key Topics for Chapter 4

| <b>Key Topic Element</b> | <b>Description</b>                                               | <b>Page Number</b> |
|--------------------------|------------------------------------------------------------------|--------------------|
| Figure 4-1               | Internet Explorer Security Features in the Local Computer Policy | 130                |
| Figure 4-3               | Internet Explorer policies in the Marketing-Policy GPO           | 132                |
| Figure 4-4               | Configuring the proxy server connection in Internet Explorer     | 134                |
| Figure 4-5               | Internet Options dialog box—Security zones                       | 136                |
| Figure 4-6               | Internet Options dialog box—Privacy tab                          | 137                |
| Figure 4-10              | Firefox Privacy options                                          | 142                |
| Figure 4-11              | Firefox Security options                                         | 143                |
| Figure 4-12              | Firefox proxy connection                                         | 144                |
| Table 4-2                | Summary of programming vulnerabilities and attacks               | 162                |

**Table 5-5** Key Topics for Chapter 5

| <b>Key Topic Element</b> | <b>Description</b>                                 | <b>Page Number</b> |
|--------------------------|----------------------------------------------------|--------------------|
| Bulleted list            | Description of MAC flooding and defense techniques | 183                |
| Table 5-2                | Private IPv4 ranges (as assigned by the IANA)      | 186                |
| Figure 5-1               | Example of public and private IPv4 addresses       | 187                |
| Figure 5-2               | 3-leg perimeter DMZ                                | 190                |
| Table 5-4                | Types of VLAN hopping                              | 195                |

**Table 6-4** Key Topics for Chapter 6

| <b>Key Topic Element</b> | <b>Description</b>                                   | <b>Page Number</b> |
|--------------------------|------------------------------------------------------|--------------------|
| Table 6-2                | Ports and their associated protocols                 | 228                |
| Figure 6-2               | IP addresses and ports                               | 232                |
| Table 6-3                | Summary of network attacks and mitigation techniques | 247                |

**Table 7-2** Key Topics for Chapter 7

| <b>Key Topic Element</b> | <b>Description</b>                          | <b>Page Number</b> |
|--------------------------|---------------------------------------------|--------------------|
| Bulleted list            | Types of firewalls                          | 271                |
| Figure 7-2               | Back-to-back firewall/DMZ configuration     | 272                |
| Bulleted list            | Types of proxies                            | 274                |
| Figure 7-4               | Illustration of an HTTP proxy in action     | 275                |
| Figure 7-5               | Illustration of NIDS placement in a network | 280                |
| Table 7-1                | Summary of NIDS versus NIPS                 | 282                |

**Table 8-3** Key Topics for Chapter 8

| <b>Key Topic Element</b> | <b>Description</b>                               | <b>Page Number</b> |
|--------------------------|--------------------------------------------------|--------------------|
| Table 8-1                | Weak, strong, and stronger passwords             | 301                |
| Bulleted list            | Privilege escalation types                       | 302                |
| Bulleted list            | Cable types                                      | 304                |
| Bulleted list            | Interference types                               | 305                |
| Table 8-2                | Wireless protocols                               | 312                |
| Figure 8-1               | Wireless security configuration on a typical WAP | 313                |
| Figure 8-2               | Wireless point-to-multipoint layout              | 315                |
| Figure 8-3               | Final network documentation                      | 320                |

**Table 9-3** Key Topics for Chapter 9

| <b>Key Topic Element</b> | <b>Description</b>                                      | <b>Page Number</b> |
|--------------------------|---------------------------------------------------------|--------------------|
| Bulleted list            | Authentication methods                                  | 340                |
| Figure 9-2               | Example of an 802.1X-enabled network adapter in Windows | 349                |
| Figure 9-3               | Components of a typical 802.1X authentication procedure | 349                |
| Figure 9-4               | Example of Active Directory showing user objects        | 352                |
| Figure 9-5               | Results of the netstat -an command on a Windows Server  | 353                |
| Figure 9-6               | MS-CHAP enabled on a dial-up connection                 | 357                |
| Table 9-1                | VPN tunneling protocols                                 | 358                |
| Table 9-2                | Summary of authentication technologies                  | 362                |

**Table 10-2** Key Topics for Chapter 10

| <b>Key Topic Element</b> | <b>Description</b>                           | <b>Page Number</b> |
|--------------------------|----------------------------------------------|--------------------|
| Figure 10-1              | Example of discretionary access in Windows   | 385                |
| Table 10-1               | Summary of access control models             | 388                |
| Figure 10-2              | Example of implicit deny on a Windows folder | 389                |
| Figure 10-4              | User account expiration date                 | 392                |
| Figure 10-5              | Time-of-day restrictions for a standard user | 393                |
| Bulleted list            | Password compliance                          | 400                |

**Table 11-4** Key Topics for Chapter 11

| <b>Key Topic Element</b> | <b>Description</b>                      | <b>Page Number</b> |
|--------------------------|-----------------------------------------|--------------------|
| Table 11-1               | Example of quantitative risk assessment | 427                |
| Table 11-2               | Summary of risk assessment types        | 428                |
| Bulleted list            | NIST security controls                  | 430                |
| Bulleted list            | Event-based security controls           | 431                |
| Numbered list            | Five steps of vulnerability management  | 431                |
| Figure 11-3              | Network vulnerability scan with Nessus  | 439                |
| Figure 11-4              | Port scan with Nmap                     | 440                |
| Figure 11-5              | Packet capture with Wireshark           | 442                |
| Figure 11-6              | Password cracking with Cain & Abel      | 443                |
| Bulleted list            | Password-cracking methods               | 444                |
| Table 11-3               | Summary of Chapter 11 security tools    | 446                |

**Table 12-2** Key Topics for Chapter 12

| <b>Key Topic Element</b> | <b>Description</b>                                                     | <b>Page Number</b> |
|--------------------------|------------------------------------------------------------------------|--------------------|
| Table 12-1               | Summary of monitoring methodologies                                    | 467                |
| Figure 12-1              | Performance Monitor in Windows                                         | 469                |
| Figure 12-2              | Wireshark showing a captured TLS Version 1.0 packet                    | 472                |
| Figure 12-3              | Network Monitor showing a captured FTP packet with clear-text password | 473                |
| Figure 12-5              | Audit Policy within the Local Computer Policy of a Windows computer    | 479                |
| Figure 12-7              | Security log in Windows                                                | 481                |
| Figure 12-9              | Syslog program running in Windows                                      | 484                |
| Figure 12-10             | Windows Server Security Log Properties dialog box                      | 486                |

**Table 13-5** Key Topics for Chapter 13

| <b>Key Topic Element</b> | <b>Description</b>                          | <b>Page Number</b> |
|--------------------------|---------------------------------------------|--------------------|
| Table 13-1               | Black book phone number encryption          | 508                |
| Figure 13-1              | Illustration of public key cryptography     | 514                |
| Table 13-3               | Summary of symmetric algorithms             | 519                |
| Table 13-4               | Summary of RSA Public and Private Key Usage | 520                |
| Figure 13-2              | Illustration of the hashing process         | 526                |
| Figure 13-3              | LM hash in the Local Group Policy           | 530                |

**Table 14-1** Key Topics for Chapter 14

| <b>Key Topic Element</b> | <b>Description</b>                                         | <b>Page Number</b> |
|--------------------------|------------------------------------------------------------|--------------------|
| Figure 14-1              | Example of a secure connection, shown in Internet Explorer | 553                |
| Figure 14-2              | Example of a secure connection, shown in Firefox           | 553                |
| Figure 14-3              | Details of a typical VeriSign certificate                  | 554                |
| Bulleted list            | IPsec protocols                                            | 561                |

**Table 15-5** Key Topics for Chapter 15

| <b>Key Topic Element</b> | <b>Description</b>                   | <b>Page Number</b> |
|--------------------------|--------------------------------------|--------------------|
| Bulleted list            | Power failures                       | 578                |
| Table 15-1               | RAID descriptions                    | 583                |
| Figure 15-1              | RAID 1 illustration                  | 585                |
| Figure 15-2              | RAID 5 illustration                  | 585                |
| Bulleted list            | Server cluster types                 | 588                |
| Bulleted list            | Types of redundant sites             | 589                |
| Bulleted list            | Backup types                         | 590                |
| Table 15-2               | Example incremental backup schedule  | 591                |
| Table 15-3               | Example differential backup schedule | 592                |
| Bulleted list            | Backup rotation schemes              | 593                |

**Table 16-6** Key Topics for Chapter 16

| <b>Key Topic Element</b> | <b>Description</b>                                    | <b>Page Number</b> |
|--------------------------|-------------------------------------------------------|--------------------|
| Bulleted list            | Fire extinguisher types                               | 612                |
| Table 16-1               | Summary of social engineering types                   | 623                |
| Table 16-4               | Acts passed concerning the disclosure of data and PII | 627                |
| Table 16-5               | Summary of policy types                               | 633                |
| Numbered list            | Seven steps of incident response process              | 637                |
| Bulleted list            | Forensic procedures                                   | 639                |

*This page intentionally left blank*

# CompTIA Security+ Acronyms

This list of acronyms comes directly from the CompTIA Security+ Certification Exam Objectives: SY0-401 v.6. It is unaltered from that source. You can find the latest objectives on the CompTIA web site.

3DES – Triple Digital Encryption Standard

AAA – Authentication, Authorization, and Accounting

ACL – Access Control List

AES – Advanced Encryption Standard

AES256 – Advanced Encryption Standards 256bit

AH – Authentication Header

ALE – Annualized Loss Expectancy

AP – Access Point

API – Application Programming Interface

ASP – Application Service Provider

ARO – Annualized Rate of Occurrence

ARP – Address Resolution Protocol

AUP – Acceptable Use Policy

BAC – Business Availability Center

BCP – Business Continuity Planning

BIA – Business Impact Analysis

BIOS – Basic Input / Output System

BPA – Business Partners Agreement

BYOD – Bring Your Own Device

CA – Certificate Authority

CAC – Common Access Card

CAN – Controller Area Network

CAPTCHA – Completely Automated Public Turing Test to Tell Computers and Humans Apart

CAR – Corrective Action Report

CCMP – Counter-Mode/CBC-Mac Protocol

CCTV – Closed-circuit television

CERT – Computer Emergency Response Team

CHAP – Challenge Handshake Authentication Protocol

CIO – Chief Information Officer

CIRT – Computer Incident Response Team

COOP – Continuity of Operation Planning

CP – Contingency Planning

CRC – Cyclical Redundancy Check

CRL – Certification Revocation List

CSR – Control Status Register

CSU – Channel Service Unit

CTO – Chief Technology Officer

DAC – Discretionary Access Control

DBA – Database Administrator

DDOS – Distributed Denial of Service

DEP – Data Execution Prevention

DES – Digital Encryption Standard

DHCP – Dynamic Host Configuration Protocol

DHE – Data-Handling Electronics

DHE – Diffie-Hellman Ephemeral

DLL – Dynamic Link Library

DLP – Data Loss Prevention

DMZ – Demilitarized Zone

DNAT – Destination Network Address Translation

DNS – Domain Name Service (Server)

DOS – Denial of Service

DRP – Disaster Recovery Plan  
DSA – Digital Signature Algorithm  
DSL – Digital Subscriber line  
DSU – Data Service Unit  
EAP – Extensible Authentication Protocol  
ECC – Elliptic Curve Cryptography  
ECDHE – Elliptic Curve Diffie-Hellman Ephemeral  
EFS – Encrypted File System  
EMI – Electromagnetic Interference  
ESN – Electronic Serial Number  
ESP – Encapsulated Security Payload  
FACL – File System Access Control List  
FDE – Full Disk Encryption  
FTP – File Transfer Protocol  
FTPS – Secured File Transfer Protocol  
GPG – Gnu Privacy Guard  
GPO – Group Policy Object  
GPS – Global Positioning System  
GPU – Graphic Processing Unit  
GRE – Generic Routing Encapsulation  
HDD – Hard Disk Drive  
HIDS – Host Based Intrusion Detection System  
HIPS – Host Based Intrusion Prevention System  
HMAC – Hashed Message Authentication Code  
HOTP – HMAC based One Time Password  
HSM – Hardware Security Module  
HTML – HyperText Markup Language  
HTTP – Hypertext Transfer Protocol  
HTTPS – Hypertext Transfer Protocol over SSL  
HVAC – Heating, Ventilation Air Conditioning

IaaS – Infrastructure as a Service

ICMP – Internet Control Message Protocol

ID – Identification

IDS – Intrusion Detection System

IKE – Internet Key Exchange

IM – Instant messaging

IMAP4 – Internet Message Access Protocol v4

IP – Internet Protocol

IPSEC – Internet Protocol Security

IR – Incident Response

IRC – Internet Relay Chat

IRP – Incident Response Procedure

ISA – Interconnection Security Agreement

ISP – Internet Service Provider

ISSO – Information Systems Security Officer

ITCP – IT Contingency Plan

IV – Initialization Vector

JBOD – Just a Bunch of Disks

KDC – Key Distribution Center

L2TP – Layer 2 Tunneling Protocol

LAN – Local Area Network

LDAP – Lightweight Directory Access Protocol

LEAP – Lightweight Extensible Authentication Protocol

MaaS – Monitoring as a Service

MAC – Mandatory Access Control / Media Access Control

MAC – Message Authentication Code

MAN – Metropolitan Area Network

MBR – Master Boot Record

MD5 – Message Digest 5

MOU – Memorandum of Understanding

MPLS – Multi-Protocol Layer Switch

MSCHAP – Microsoft Challenge Handshake Authentication Protocol

MTBF – Mean Time Between Failures

MTTR – Mean Time to Recover

MTTF – Mean Time to Failure

MTU – Maximum Transmission Unit

NAC – Network Access Control

NAT – Network Address Translation

NDA – Non-Disclosure Agreement

NFC – Near Field Communication

NIDS – Network Based Intrusion Detection System

NIPS – Network Based Intrusion Prevention System

NIST – National Institute of Standards & Technology

NOS – Network Operating System

NTFS – New Technology File System

NTLM – New Technology LANMAN

NTP – Network Time Protocol

OCSP – Online Certificate Status Protocol

OLA – Open License Agreement

OS – Operating System

OVAL – Open Vulnerability Assessment Language

P2P – Peer to Peer

PAC – Proxy Auto Configuration

PAM – Pluggable Authentication Modules

PAP – Password Authentication Protocol

PAT – Port Address Translation

PBKDF2 – Password Based Key Derivation Function 2

PBX – Private Branch Exchange

PCAP – Packet Capture

PEAP – Protected Extensible Authentication Protocol

PED – Personal Electronic Device

PGP – Pretty Good Privacy

PII – Personally Identifiable Information

PIV – Personal Identity Verification

PKI – Public Key Infrastructure

POTS – Plain Old Telephone Service

PPP – Point to point Protocol

PPTP – Point to Point Tunneling Protocol

PSK – Pre-Shared Key

PTZ – Pan-Tilt-Zoom

RA – Recovery Agent

RAD – Rapid application development

RADIUS – Remote Authentication Dial-in User Server

RAID – Redundant Array of Inexpensive Disks

RAS – Remote Access Server

RBAC – Role Based Access Control

RBAC – Rule Based Access Control

RC4 – RSA Variable Key Size Encryption Algorithm

RIPEMD – RACE Integrity Primitives Evaluation Message Digest

ROI – Return of Investment

RPO – Recovery Point Objective

RSA – Rivest, Shamir, & Adleman

RTO – Recovery Time Objective

RTP – Real-Time Transport Protocol

S/MIME – Secure / Multipurpose Internet Mail Extensions

SAML – Security Assertions Markup Language

SaaS – Software as a Service

SAN – Storage Area Network

SCADA – System Control and Data Acquisition

SCAP – Security Content Automation Protocol

SCEP – Simple Certificate Enrollment Protocol  
SCSI – Small Computer System Interface  
SDLC – Software Development Life Cycle  
SDLM – Software Development Life Cycle Methodology  
SEH – Structured Exception Handler  
SHA – Secure Hashing Algorithm  
SFTP – Secured File Transfer Protocol  
SHTTP – Secure Hypertext Transfer Protocol  
SIEM – Security Information and Event Management  
SIM – Subscriber Identity Module  
SLA – Service Level Agreement  
SLE – Single Loss Expectancy  
SMS – Short Message Service  
SMTP – Simple Mail Transfer Protocol  
SNMP – Simple Network Management Protocol  
SOAP – Simple Object Access Protocol  
SONET – Synchronous Optical Network Technologies  
SPIM – Spam over Internet Messaging  
SQL – Structured Query Language  
SSD – Solid State Drive  
SSH – Secure Shell  
SSL – Secure Sockets Layer  
SSO – Single Sign On  
STP – Shielded Twisted Pair  
TACACS+ – Terminal Access Controller Access Control System  
TCP/IP – Transmission Control Protocol / Internet Protocol  
TGT – Ticket Granting Ticket  
TKIP – Temporal Key Integrity Protocol  
TLS – Transport Layer Security  
TOTP – Time-Based One-Time Password

TPM – Trusted Platform Module  
TSIG – Transaction Signature  
UAT – User Acceptance Testing  
UEFI – Unified Extensible Firmware Interface  
UDP – User Datagram Protocol  
UPS – Uninterruptable Power Supply  
URI – Uniform Resource Identifier  
URL – Universal Resource Locator  
USB – Universal Serial Bus  
UTM – Unified Threat Management  
UTP – Unshielded Twisted Pair  
VDI – Virtualization Desktop Infrastructure  
VLAN – Virtual Local Area Network  
VoIP – Voice over IP  
VPN – Virtual Private Network  
VTC – Video Teleconferencing  
WAF – Web-Application Firewall  
WAP – Wireless Access Point  
WEP – Wired Equivalent Privacy  
WIDS – Wireless Intrusion Detection System  
WIPS – Wireless Intrusion Prevention System  
WPA – Wireless Protected Access  
WPA2 – WiFi Protected Access 2  
WPS – WiFi Protected Setup  
WTLS – Wireless TLS  
XML – Extensible Markup Language  
XSRF – Cross-Site Request Forgery  
XSS – Cross-Site Scripting

*This page intentionally left blank*

# Case Studies

## Case Studies for Chapter 2

The case studies offer generic scenarios for you to read through and answer according to your own technology and experiences. Your solutions will vary in comparison, but both can certainly be valid. Many case study solutions also point to hands-on videos and simulations which can be found on the book's disc.

### Case Study 2-1: Using Free Malware Scanning Programs

**Scenario:** As a security administrator, your task is to select a free malware scanning program and scan a computer system.

An anti-malware solution is extremely important when securing a computer's operating system. There are plenty to choose from that will have a price tag attached, but a good security person should also be able to use free tools online. Plus, using a free tool provides us with an easy way to practice without expending any hard-earned capital.

You can select from the following list or search for an alternative using your favorite search engine. These could be programs that are downloadable; if so, be sure that you are downloading the files from a reputable source. There are also online scanners that run directly from within a website. In this case, make sure that the website is secured via some kind of website scanning system.

Keep in mind that links may change over time, and software that is free (at the writing of this book) may incur a charge as time goes by.

Once you have selected a tool, scan your computer for malware. This is best done on a test computer if you have one available. Write down the results of your scans.

- Malicious Software Removal Tool  
<http://www.microsoft.com/security/pc-security/malware-removal.aspx>
- Trend Micro HouseCall <http://housecall.trendmicro.com/>
- Malwarebytes Anti-Malware <http://www.malwarebytes.org/>

- Microsoft Safety Scanner  
<http://www.microsoft.com/security/scanner/en-us/default.aspx>
- Spybot Search & Destroy <http://www.safer-networking.org/private/>
- Combofix <http://www.combofix.org/>

### **Case Study 2-2: Securing the BIOS**

**Scenario:** Your boss asks you to secure the BIOS on a desktop computer. Your job is to modify the BIOS boot order, disable unnecessary devices such as floppy drives, and configure a supervisory password.

The BIOS boots before the operating system. It can be configured to boot from optical discs and removable media. This change is fairly simple to make as long as a person can log in to the BIOS setup program. If no password is configured, this is even easier. You can imagine the amount of havoc that can be wreaked upon a machine if a malicious individual were to gain access to the BIOS.

Try securing the BIOS program on a test computer, or try securing the virtual BIOS that is included within virtual machine software such as Virtual PC 2007, Windows Virtual PC, or VirtualBox. When you are finished, return all settings back to normal.

### **Case Study 2-3: Securing Mobile Devices**

**Scenario:** You have purchased a couple of different mobile devices and are concerned about their out-of-the-box level of security. Implement some basic security measures on the devices.

Take a look at the mobile device(s) that you own or attempt to borrow one. What kind of security measures could you take (or have already taken) to make the device(s) less vulnerable. If you can't get access to one, use the content in this chapter to help with some ideas for security measures that you can implement. Write down your list of security implementations and compare them with the case study solution.

### **Case Study 2-4: Filtering and Screening E-mail**

**Scenario:** You are the security administrator for a midsized organization. One of your many tasks is to train users to filter and/or screen their e-mails.

E-mail vetting (screening) has become increasingly necessary over the past decade. This is due to the amount of spam that dominates the Internet. Imagine how you might reduce the amount of spam (which everyone gets at some point) within Out-

look e-mail accounts and within free web-based e-mail accounts such as Gmail. Write down your answers and compare with the case study solution.

## Case Study Solutions

### Case Study 2-1 Solution

In this example solution we use the free Trend Micro HouseCall scanning program to analyze a computer for viruses. This should be performed on a test computer, but a virtual machine is also acceptable. The steps are as follows:

- Step 1.** Download Trend Micro's HouseCall software from  
<http://housecall.trendmicro.com/>
- Step 2.** When it finishes downloading, install the program.
- Step 3.** The program should run automatically; use it to scan your computer for malware. You can click settings to select different partitions or folders. If you find any malware, quarantine it!
- Step 4.** Consider downloading and utilizing other tools in the list to get a firmer understanding of how these type of scanning tools operate.
- Step 5.** When you finish working with the free malware scanning programs, uninstall each of them from the computer and clear the cache on the system.

**Video Solution:** Watch the video solution “2-1: Using Free Malware Scanning Programs” on the accompanying disc.

**Simulation:** Complete the simulation “2-1: Identifying Malware Types.”

### Case Study 2-2 Solution

For this example solution we use the virtual BIOS in Microsoft Virtual PC 2007 to make some configuration changes, thus securing the BIOS. The steps are as follows:

- Step 1.** Download and install Microsoft Virtual PC 2007.
- Step 2.** Run the Virtual PC program; this should display the Virtual PC console.

**Step 3.** Create a new virtual machine.

**Step 4.** Access the VM BIOS.

**Step 5.** Change the Boot device priority order.

**Step 6.** Disable the floppy drive.

**Step 7.** Configure a complex supervisor password.

**Step 8.** Return the virtual BIOS settings to normal.

**Video Solution:** Watch the video solution “2-2: Securing the BIOS” on the accompanying disc for in-depth details of each step.

**Simulation:** Complete the simulation “2-2: Securing the BIOS.”

### Case Study 2-3 Solution

Some of the security measures you can implement on a mobile device include: configuring screen locks utilizing either a password, PIN, or gesture; installing (or simply configuring) antivirus software; disabling wireless and GPS; using encryption; and installing/configuring backup and remote wipe programs.

**Video Solution:** Watch the video solution “2-3: Securing Mobile Devices” on the accompanying disc.

### Case Study 2-4 Solution

Spam and other junk mail is very prevalent in today’s e-mail communications. There are so many sources of this junk mail that it is impossible to stop altogether. However, through filtering and user education (screening of e-mail) it can be reduced to a level that is manageable.

One of the ways to do this is to increase the level of security for junk e-mail. E-mail applications such as Outlook offer this feature. Another way is to set up filters either through third-party software locally, at the e-mail server (be it in-house or on the Internet), or by using a filtering appliance, such as the Barracuda devices mentioned earlier in the chapter. The use of blacklisting (and/or whitelisting) can help with re-occurring spam. But the best method is to train users to scan their e-

mails carefully, deleting any that appear suspicious, and by all means to not open any attachments from an unknown source. While deleting the e-mail, the domain it came from can be marked as blacklisted as well. So any e-mails originating from that domain (any e-mail address on that domain) will be automatically blocked.

**Simulation:** Complete the simulation “2-4: Filtering E-mails.”

## Case Studies for Chapter 3

### Case Study 3-1: Discerning and Updating the Service Pack Level

**Scenario:** You have been tasked with finding out the service pack level of a Windows 7 computer and updating it if necessary. You must also configure the Windows Update program in such a way that you will be notified of new updates but they will not be downloaded until you decide to do so, in keeping with your company’s policies.

Usually an organization will choose to have the latest service packs installed for every Windows system, and the latest patches for other operating systems. It’s important to be able to recognize whether a computer is up to date. Try and locate the service pack level for your version of Windows, and attempt to find out the version numbers for any other computing devices you might possess. Enter your results in Table 3-3. Afterward, define how you would go about configuring Windows Update, and what option you would choose.

**Table 3-3** Operating System and Version Responses

| Operating System   | Version                         |
|--------------------|---------------------------------|
| Example: Windows 7 | Example: SP1 (version 6.1.7601) |
|                    |                                 |
|                    |                                 |
|                    |                                 |
|                    |                                 |
|                    |                                 |

### **Case Study 3-2: Securing a Virtual Machine**

**Scenario:** Now that you have installed virtual machine software, and created a new VM, you are required to secure it. Your task is to disable unnecessary virtual hardware and secure the virtual BIOS.

Virtual machines that are contained within a Type 2 host are sort of like a computer within a computer. Consider writing down exactly what you are configuring. Try to do this in an illustrative nature. Or, consider using a network documentation program such as Visio. As you progress in the virtual world, you will be using more and more virtual computers, and will connect to them in a variety of remote ways. The more you document what it is that you are doing, the better you will understand your virtual environments.

Within your virtual software, disable the sound card, COM ports, LPT ports, and floppy disks (if any exist). This is done in the properties (or settings) of the virtual machine. Secure the BIOS by modifying the BIOS boot order, disabling unnecessary hardware, and setting an administrative (supervisor) password.

### **Case Study 3-3: Stopping Services in the Command-Line**

**Scenario:** You have found that working in the GUI is good, but working in the command-line can be better. Besides, you almost always have a CLI (command-line interface) open, and you can type quickly, so it makes sense to use the CLI as often as possible. You know that unnecessary services can be vulnerabilities to your systems, so you decide to reduce the size of the attack surface by stopping and disabling services—and do this from the CLI.

Demonstrate that you can stop services in the Windows Command Prompt (such as the Windows Firewall), as well as services in the Linux CLI (such as an Apache web server if installed). Specific commands and syntax will vary depending on the version of the operating system you are working in.

## **Case Study Solutions**

### **Case Study 3-1 Solution**

To find out the service pack level of Windows 7, navigate to Start, then right-click Computer and select Properties. This displays the System window and should show the Windows edition, as well as the service pack level. If no service pack is listed, then none is installed, and is known as service pack 0. Other versions of Windows use similar navigation to find out the service pack level. To update to the latest service pack for a given Windows operating system, go to

<http://support.microsoft.com/> and search the relevant phrase, such as “Windows 7 SP1.” Latest service packs can be downloaded directly from the website. An organization might also use an optical disc to update individual computers or, if there are a lot of computers, stream the service pack update over the network.

Service packs are large groups of patches and updates. But they are static, meaning after one is released, it remains the same. So, additional updates are always necessary. By default this is taken care of by Windows Update. To modify the Windows Update settings, choose Start > All Programs > Windows Update. Then click the Change Settings link. Click the drop-down menu under Important Updates to select the correct setting. In this scenario it was “Check for updates but let me choose whether to download and install them.” This is a good solution for an individual computer, giving the user a good amount of control over what is installed. However, it probably wouldn’t be the best solution in an organization, and it is more likely that updates would be streamed across the network with a centralized solution such as SCCM.

Keep in mind that some computers will need to be updated beyond the service pack, *and* beyond what is automatically downloaded from Windows Update. Patches for specific problems are known as hotfixes. It is important to know how to acquire these hotfixes (also known as update rollups). They are usually found at the Microsoft Support website and are listed by Knowledge Base (KB) number. For example, one hotfix that repairs a memory leak in Windows 7 SP1 can be found at the following link:

<http://support.microsoft.com/kb/2911106>.

It is article number 2911106 in the Microsoft Knowledge Base. It actually fixes a lot of documented issues, and can be an important fix for various Windows operating systems in addition to Windows 7 SP1. Over time, these hotfixes are gathered together in automatically downloaded Windows Update groups (if it is deemed necessary), and ultimately are added to newer service packs.

**Video Solution:** Watch the video solution “3-1: Discerning and Updating the Service Pack Level” on the accompanying disc for in-depth details of each step, plus content on Linux, OS X, Android, and iOS.

### Case Study 3-2 Solution

Virtualization security is vital. VMs should be secured the same way that a regular operating system is secured. However, the VM itself (and the virtual hosting software) can be further secured by disabling virtual hardware, both within the virtual machine settings and within the virtual machine BIOS.

This solution utilizes a Windows 7 hosting computer and assumes that you have already downloaded and installed Microsoft Virtual PC 2007, created a virtual machine, and installed an OS. Basic steps follow below. Be sure to watch the accompanying video solution as well.

- Step 1.** Check the Microsoft Virtual PC 2007 software SP level from Control Panel > Programs > Programs and Features. If necessary, upgrade to the latest SP from the following link:  
[www.microsoft.com/download/en/details.aspx?displaylang=en&id=24439](http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=24439)
- Step 2.** Set security options in the Virtual PC console from File > Options > Security.
- Step 3.** Disable unnecessary hardware within the Virtual PC console for the VM in question. For example, the sound card, COM ports, LPT ports, and floppy disks.
- Step 4.** Start the virtual machine and secure the virtual BIOS. Modify the BIOS boot order, disable unnecessary devices, and configure an administrative password.
- Step 5.** Start the virtual machine and check the SP level of the virtual OS.
- Step 6.** Disable unnecessary hardware in the Device Manager of the VM.
- Step 7.** Remove any network sharing connections between the VM and the physical host.
- Step 8.** (Optional) Exit the VM and secure the folder on the host OS that contains the VM files.

**Video Solution:** Watch the video solution “3-2: Securing a Virtual Machine” on the accompanying disc for in-depth details of each step.

### Case Study 3-3 Solution

Stopping services is an extremely important skill for a security administrator (not to mention for the Security+ exam). As an IT person, you should feel at home in the command-line. Running commands, scripting, and testing network connections are all part of a day’s work in the computer world. From a security standpoint, some things that cannot be accomplished in the GUI *can* be performed in the command-line.

To stop a service such as the Windows Firewall in Windows, use the following syntax:

```
net stop mpssvc
```

or

```
sc stop mpssvc
```

To stop a service in Linux (for example, stopping the udevmonitor service in Ubuntu), use the following syntax:

```
sudo stop udevmonitor
```

Be prepared to enter the administrator password because you have invoked the `sudo` option.

**Video Solution:** Watch the video solution “3-3: Working with Services in Windows and Linux” on the accompanying disc. This goes into a bit more depth, showing a few more commands, and deals with processes as well.

**Simulation:** Complete the simulation “3-3: Stopping Services in the Command-Line.”

## Case Studies for Chapter 4

### Case Study 4-1: Securing Web Browsers

**Scenario:** Your organization uses Internet Explorer version 10 as its main web browser. Your job as the security administrator is to secure Internet Explorer in as many ways as possible.

Take a look at the configuration settings for your version of IE. Write down some of the ways that IE can be secured.

(Optional) Take a look at any other browsers you might have running (Firefox, Chrome, Safari, Opera, etc.) and define the types of security they have as well.

### Case Study 4-2: Whitelisting and Blacklisting Applications in a Windows Server Policy

**Scenario:** You have been employed as a consultant to set up a couple of policies in Windows Server. The first of these is to configure which applications can, and can't, be executed by employees.

Explain in your own words how you would accomplish your goal in Windows Server. If you have access to a Windows Server (for testing purposes), attempt to do this configuration within the operating system. If you don't, consider downloading an evaluation copy of Windows Server and loading it into a virtual machine.

## Case Study Solutions

### Case Study 4-1 Solution

Internet Explorer can be secured in many ways. The first thing you might do is to update to the newest version (if your organization's policy permits) and make sure that version is fully patched. Test the new version thoroughly before deployment. Otherwise, the following is a short list of some of the best ways to secure the browser:

1. Turn on automatic website checking with the phishing filter or SmartScreen filter.
2. Increase the security of the browser's "zones" such as the Internet zone.
3. Increase security for cookies.
4. Empty temporary Internet files on exit.
5. Set up whitelisting and blacklisting by configuring trusted and restricted websites.
6. (Optional) Set up a proxy connection.

**Video Solution:** Watch the video solution "4-1: Securing Web Browsers" on the accompanying disc.

**Simulation:** Complete the simulation "4-1: Securing Web Browsers."

### Case Study 4-2 Solution

Whitelisting means that you give users access to specific applications *only*—for example, Microsoft Word (winword.exe) or Internet Explorer (iexplore.exe).

Blacklisting means that you deny users access to specific applications. Both of these are possible within the same Group Policy object (GPO) in Windows Server. To

create this GPO and modify it correctly, it is assumed that you have promoted the Windows Server to a domain controller, and that you have created an organizational unit (OU) to work with. It also assumes that you have an MMC to use as your workspace. The video solution (4-2) shows how to create the OU. The following shows the basic steps involved with configuring the GPO:

**NOTE** The following solution is based on Windows Server 2008. However, Windows Server 2012 will be similar.

**Step 1.** Create a new policy based off the OU and add it to the MMC:

- A. Go to File > Add/Remove Snap-in. This displays the Add/Remove Snap-ins dialog box.
- B. Scroll down to Group Policy Management Editor, highlight it, and click Add. This displays the Select Group Policy Object window.
- C. In the Select Group Policy Object dialog box, click Browse.
- D. Double-click the name of the OU folder (for example, accounting.dpro3.com). Yours might differ in OU name and domain name.
- E. On the upper-right side of the window, click the middle icon, which is called Create New Group Policy Object.
- F. Click the New button. Name the policy (for purposes of this example, use acct-policy) and press Enter. Then click OK. This creates a standard policy within the Accounting OU.
- G. Click Finish in the Select Group Policy Object window and click OK in the Add or Remove Snapins window. This should add the new policy to the MMC.

**Step 2.** Configure the policy:

- A. Expand the acct-policy.
- B. Navigate to User Configuration > Policies > Administrative Templates > System.
- C. Double-click Don't Run Specified Windows Applications.
- D. Click the Enabled radio button.
- E. Click Show.

- F. Click Add and add an application (for example, winword.exe, the executable for Microsoft Word). Then click OK. Be sure to reset this at the end of the lab if it will affect any computers or users.
- G. Click OK for the policy's Properties window. This brings you back to the MMC. The policy will now be enabled.
- H. Double-click the Run Only Specified Windows Applications policy.
- I. Enable the policy; then click Show.
- J. Add an application by clicking the Add button, typing the name of an application (for example, excel.exe, the executable for Microsoft Excel), and clicking OK.
- K. Click OK for the policy's Properties window. This brings you back to the MMC. The policy will now be enabled.

**Step 3.** Save your MMC.

**Step 4.** Test whether or not your new policy works by logging in to a client computer with one of the user accounts that is part of the OU.

**Video Solution:** Watch the video solution “4-2: Whitelisting and Blacklisting Applications with a Windows Server Policy” on the accompanying disc.

## Case Studies for Chapter 5

### Case Study 5-1: Creating a DMZ

**Scenario:** Your organization’s network has all of its servers running directly within the LAN. The new IT director knows this is quite insecure, and so instructs you to develop a 3-leg firewall scheme.

Your task is to create a network diagram (either handwritten or with a program such as Microsoft Visio) that shows the LAN, Internet, firewall, and DMZ areas. Give examples of the IP addresses that might be used for all three connections to the firewall.

## Case Study 5-2: Subnetting a Network

**Scenario:** The organization you work for has several departments. There is a lot of unnecessary traffic flowing between the Human Resources, Accounting, and Marketing departments. Each department has 10 to 15 computers running within it. Your task is to implement subnetting so that each of the three departments' computers are placed on separate subnets, thus reducing overall traffic, as well as securing the connections between the departments.

In this scenario you will use the 192.168.100.0 network. The current subnet mask is 255.255.255.0. You will need to modify this. Plan the network so that there are eight subnets in total. Specify which subnet ID each department uses, and what the usable ranges of IP addresses for those subnets are. Your answers may vary from the case study solution.

## Case Study 5-3: Defending against the Web Shell

**Scenario:** One of your associate's websites was hacked into. The associate contacted you to see if you knew anything about a "Web Shell." The person had found that name within the syntax of one of the "new" files on his web server. Your task is to explain what is going on to your associate, and recommend a solution.

Question 1: What is the Web Shell?

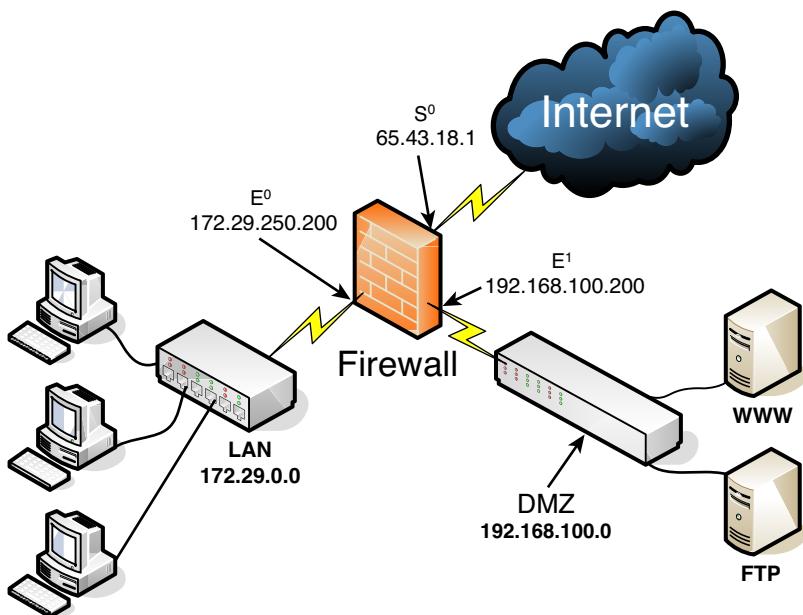
Question 2: How did it get there?

Question 3: What should your recommendations be?

# Case Study Solutions

## Case Study 5-1 Solution

As shown in Figure 5-6, the 3-leg firewall scheme has a firewall in the center with three connections to the Internet, the LAN, and the DMZ. The LAN is using a Class B private IP network. The DMZ is on a separate Class C IP network. And the Internet connection uses a public IP address so that the firewall can connect directly to other systems and networks on the Internet.



**Figure 5-6** DMZ with 3-Leg Firewall Scheme

This 3-leg solution is an excellent way (though not the only method) of separating web servers, FTP servers, and mail servers from the rest of the LAN. A separate set of rules (ACLs) can be configured for the DMZ connection and the LAN connection. In this way, the DMZ can be accessed by users on the Internet (and by users on the LAN), but the resources on the LAN are fully protected from users on the Internet. A 3-leg firewall of this sort can be accomplished by using a hardware-based firewall with an Internet connection and two LAN connections (most common), or a server with three network adapters running special firewalling software.

**Simulation:** Complete the simulation “5-1: Creating a DMZ” on the accompanying disc.

### Case Study 5-2 Solution

Subnetting is an excellent way of compartmentalizing the network. It reduces broadcast traffic between the various computers on the network, and secures different departments. This is because many types of traffic now cannot pass from one subnet to the next (without an expressed routing rule). So it is an effective security method.

In the scenario we were given the 192.168.100.0 Class C network to work with. To end up with eight subnets, we would need to use the 255.255.255.224 subnet mask. This can be represented as 192.168.100.0/27 because the subnet mask will have 27 masked bits (1s). Table 5-7 shows the eight possible subnets and their ranges. Though they are usable, in many cases, a network engineer will opt to not use the first and last subnets, so subnet IDs 1 to 6 become fair game.

**Table 5-7** List of Subnets for 192.168.100.0/27 (255.255.255.224 Subnet Mask)

| Subnet ID | Mathematical IP Range           | Usable IP Range                 |
|-----------|---------------------------------|---------------------------------|
| ID 0      | 192.168.100.0–192.168.100.31    | 192.168.100.1–192.168.100.30    |
| ID 1      | 192.168.100.32–192.168.100.63   | 192.168.100.33–192.168.100.62   |
| ID 2      | 192.168.100.64–192.168.100.95   | 192.168.100.65–192.168.100.94   |
| ID 3      | 192.168.100.96–192.168.100.127  | 192.168.100.97–192.168.100.126  |
| ID 4      | 192.168.100.128–192.168.100.159 | 192.168.100.129–192.168.100.158 |
| ID 5      | 192.168.100.160–192.168.100.191 | 192.168.100.161–192.168.100.190 |
| ID 6      | 192.168.100.192–192.168.100.223 | 192.168.100.193–192.168.100.222 |
| ID 7      | 192.168.100.224–192.168.100.255 | 192.168.100.225–192.168.100.254 |

Each subnet has 30 usable IP addresses. (Remember that you can't use the first or the last because they are reserved for the subnet IP and the broadcast IP.) So, for example, we could use subnet ID 1 for the Human Resources department, subnet ID 2 for the Accounting department, and subnet ID 3 for the Marketing department.

The computers within each of those networks would then need to be configured properly. There are a lot of ways to do this. Automation is the best way. For example, set up three DHCP scopes configured on a DHCP server (be it a Microsoft server or a router), each of which corresponds to the appropriate subnet-work within a router. The key is to make sure that the DHCP server hands out the correct subnet ID addresses to each department. This requires additional config-uring that goes beyond the extent of this case study. However, for more information on defining DHCP scopes in Windows Server, see the following link:  
<http://technet.microsoft.com/en-us/library/dd759218.aspx>

For more information about DHCP subnet configuration on Cisco routers, see the following link:

[http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/admin/8\\_5\\_1/ccmefg/bccm-851-cm/b02dhsu.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/8_5_1/ccmefg/bccm-851-cm/b02dhsu.html)

Or simply search for “Cisco DHCP subnet configuration.”

**Video Solution:** Watch the video solution “5-2: Subnetting a Network” on the accompanying disc. This reviews subnet masks and shows an example of subnetting.

### Case Study 5-3 Solution

These web shells are programs (known under several permutations: C99, C Shell, Web Shell, Web Shell by Orb, and others) that are installed on the web server by an attacker, and are used to remotely access and reconfigure the server without the owner’s consent. They are *remote access Trojans*, but are also referred to as backdoors because they offer an alternative way of accessing the website for the attacker.

Most likely, the hacker stole the associate’s FTP password. Once the hacker had the password, it was just a matter of uploading the shell. Then the hacker could log in through the new web shell, and do just about anything they wanted to the web server. Many of these web shells allow the operator to access them through a proxy, thus hiding the location of the operator. Also, the shell can be bound to specific ports, and the information can be encrypted and hashed.

First, you should recommend increasing password security for all important FTP accounts. Make the passwords as complex as the web server would allow. Remove any unnecessary FTP accounts. Delete the original RAT files and run a full scan of the system, or at worst, restore data from an older backup. Have the associate verify the web host’s scanning techniques, or scan web files manually.

**Simulation:** Complete the simulation “5-3: Defending against the Web Shell.”

## Case Studies for Chapter 6

### Case Study 6-1: Scanning Ports

**Scenario:** Your organization has some concerns about the attack surface of its servers. It is unknown what the vulnerabilities to the servers are at this point. Your task is to find out what ports are open on a web server and an FTP server. If any are unnecessary, you are to close or shield them.

Question 1: Which command-line tools can you use to find out which ports are open?

Question 2: Where would you go in Windows to secure the unnecessary ports?

Question 3: What is an example of a deprecated and most likely unnecessary port?

## Case Study 6-2: Identifying Network Attacks

**Scenario:** You are interviewing for a job with a marketing company. The company's servers have been victims of various DoS attacks and other malicious network attacks over the past year. The company wants to employ a resourceful server technician who can quickly identify the different types of network attacks common today.

Your task is to research the three types of DoS attacks listed below and give a few examples of how they can be prevented.

- Smurf attack
- 
- 
- 

- SYN flood
- 
- 
- 

- Teardrop attack
- 
- 
- 

## Case Study Solutions

### Case Study 6-1 Solution

There are many command-line tools available that can be used to scan for open ports on a computer. For example, in Windows you could use the `netstat` command, or download the `TCPView.exe` or `PortQry.exe` tools from Microsoft's website. A third-party tool, `Nmap`, is very popular and can be used on Windows and Linux platforms. A common way to use this tool is to type the following syntax:

```
nmap -sS [IP address]
```

You can also scan Internet-facing network adapters with syntax such as:

```
nmap -P0 [public IP address]
```

If there are nonessential ports open, turn off their corresponding unnecessary services. For instance, if the web server shows port 21 is open but doesn't need FTP running, stop the service (and disable it) in the services console window (Run > services.msc), or by using the net and sc commands in the Command Prompt. You could also configure the Windows Firewall (best option is with Advanced Security) to block or shield the appropriate ports, and create filters and rules.

An example of a deprecated port is port 23, used by Telnet. This utility is insecure and should be avoided. Windows XP was the last Microsoft operating system to use it, but you could easily find that operating system in use, in addition to the fact that some routers might have the Telnet protocol installed as well. You never know exactly what you might find on a network, even your own network. Port scanning allows you to find the open doorways.

**Video Solution:** Watch the video solution “6-1: Scanning Ports” on the accompanying disc.

**Simulation:** Complete the simulation “6-1: Understanding Port Numbers” Parts A, B, and C.

### Case Study 6-2 Solution

DoS (and DDoS) attacks can harm routers and other various hosts, but are most commonly used to flood servers, causing them to only give intermittent data to clients, or fail altogether.

The Smurf attack sends large amounts of ICMP packets to multiple targets on a network in an attempt to flood their network interfaces, and the network in general. The most obvious defense is to filter ICMP traffic at the router or firewall. However, you could also use a NIDS solution, filter for spoofed IP addresses, or utilize subnetworking.

The SYN flood is when large amounts of SYN packets are sent to a server, rendering it inoperable. One way to prevent this is to implement flood control at the firewall (which can also help with Smurf and other DoS attacks). Another is to use an IDS.

The teardrop attack sends broken IP packets (fragments) in an attempt to crash the computer. To prevent this, utilize filtering and update and harden the OS.

Try to memorize the various network attacks covered in this chapter. This will undoubtedly help you on the job interview, as well as on the job itself. To help you remember them, run the following simulation from the disc.

**Simulation:** Complete the simulation “6-2: Identifying Network Attacks” Parts A, B, C, and D.

## Case Studies for Chapter 7

### Case Study 7-1: Configuring a Firewall’s Rule Set

**Scenario:** You are the security administrator for a company with 200 computers, five of which are servers. Your company wants you to devise a firewall rule set for a specific client computer and allow it specific access to a server.

**Details:**

Server IP: 10.18.255.101

Client IP: 10.18.255.16

Access needed to server: HTTPS

In Table 7-3, fill out the required information given the previous details.

**Table 7-3** Firewall Rule Set

| Source IP | Destination IP | Port Number | TCP/UDP | Allow/Deny |
|-----------|----------------|-------------|---------|------------|
|           |                |             |         |            |

### Case Study 7-2: Configuring Packet Filtering and NAT

**Scenario:** You are consulting for a small company that has seven computers connected to an all-in-one SOHO router (also known as a multifunction network device). The owner is concerned whether data passed through the device is being inspected and/or filtered properly. The owner is also not sure how the internal IP addresses of his computers are being protected from the Internet properly. Your tasks are to make sure packet filtering is functioning, and explain to the owner how NAT works on this device.

Consider your options when it comes to packet filtering for a device such as this. Make a recommendation based on today's SOHO routers. If the owner wanted to take packet filtering further, what could you suggest?

---



---



---

In your own words, explain to the owner (as if you were actually speaking to the person) how NAT functions within a SOHO router.

---



---



---

### Case Study 7-3: Configuring an Inbound Filter

**Scenario:** Your boss is concerned with the repeated intrusion attempts from a group of IP addresses on the Internet. They are all part of a single IP network and range between 12.46.14.66 and 12.46.14.100. The main concern is that they are trying to insert unwanted packets into the network. Your public IP address is 65.13.82.14.

Your job is to block these IP addresses at the firewall. What can you implement that will filter out the unwanted IP addresses? How would this work from a logical standpoint?

## Case Study Solutions

### Case Study 7-1 Solution

In this scenario you created a basic rule allowing HTTPS access from a client computer to a server. Table 7-4 has the solution for the proper configuration.

**Table 7-4** Firewall Rule Set Solution

| Source IP    | Destination IP | Port Number | TCP/UDP | Allow/Deny |
|--------------|----------------|-------------|---------|------------|
| 10.18.255.16 | 10.18.255.101  | 443         | TCP     | Allow      |

The client is the source IP and the server is the destination IP as it is the device that runs the service. The port number is 443, the one used by HTTPS. HTTPS,

like HTTP, uses TCP as its transport mechanism; it is a guaranteed packet delivery system, otherwise known as connection-oriented. Finally, the rule is that connections are allowed.

Consider practicing with hardware- and software-based firewalls. If you can't get access to a Cisco, Check Point, or similar device, try working with Windows or Linux in the command-line. For Windows, configure the Windows Firewall with Advanced Security using the Command Prompt and netsh.exe. For more information on how to add rules with netsh.exe, see the following link:

[http://technet.microsoft.com/en-us/library/dd734783\(v=ws.10\).aspx#BKMK\\_3\\_add](http://technet.microsoft.com/en-us/library/dd734783(v=ws.10).aspx#BKMK_3_add)

For Linux, use `iptables` or `nftables` in the command-line. For more information on `iptables`, see the following MAN page link:

<http://ipset.netfilter.org/iptables.man.html>

Try to practice working with firewall rules. You are bound to get questions on this topic when you take the exam. Plus, it is a necessary skill for the security administrator.

**Simulation:** Complete the simulation “7-1: Configuring a Firewall’s Rule Set.”

## Case Study 7-2 Solution

First, you should make sure that stateful packet inspection (SPI) is being implemented. SPI keeps track of the individual sessions running through the router. It can differentiate between good and bad packets to a small extent. Small office/home office (SOHO) routers usually have the ability to run SPI, at least at a basic level. However, you should test this ability. How much does it slow down communications?—for example, VPN or remote connectivity connections. If the difference in communication speed between SPI being enabled and being disabled is great, you might recommend a newer SOHO router.

If the owner requires a greater level of packet filtering, you can suggest a NIDS/NIPS solution that sits inline on the network, and perhaps a proxy server of sorts.

Your explanation of NAT to the owner should include a description of how it translates the private internal IP addresses of the network to the public external IP address. This, you can tell the owner, protects the internal IP addresses from discovery. The public IP address is connected to the Internet, but if firewalled properly, it should be virtually invisible.

Most small four- and eight-port SOHO routers also offer NAT filtering that can filter out TCP and UDP traffic in a variety of ways depending on the IP address

and port in question. This is something you should also examine, and see if the filtering capability can be increased without undue slowdown of the network.

**Video Solution:** Watch the video solution “7-2: Configuring Packet Filtering and NAT” on the accompanying disc.

### Case Study 7-3 Solution

Intrusion attempts to a network are extremely common. A public IP address can expect to be scanned and have intrusion attempts multiple times every day. This is because of the plethora of bots and automatic scanning systems on the Internet.

The first and most obvious defense is to make sure the firewall is on, and test it by scanning it with an online program or with a command-line program such as Nmap. If at all possible, make sure all ports are closed and shielded.

Next, recommend creating an inbound filter for the IP addresses in question. This firewall rule will block all attempts by those IP addresses to access the network. This is often done graphically, but can also be done in the command-line. In essence what you are trying to accomplish can be represented as the following:

```
deny TCP/UDP 12.46.14.66 - 12.46.14.100 65.13.82.14 all ports
```

In this example, you are denying all TCP and UDP port connections for computers with the IP range of 12.46.14.66 to 12.46.14.100. Again, this is just a representation. The actual syntax for how this is implemented will vary from one system to the next. Or it might simply be done within the GUI of the firewall. That will depend on a variety of factors, including the level of complexity of your hardware and software.

Whatever the case is, keep track of your firewall rules. Too many rules and you can end up blocking access to known good IP addresses. Finally, if you are worried that external attackers are trying to insert unwanted packets on your network, you should strongly consider a NIDS or NIPS solution, and possibly a honeypot. These might be implemented as individual technologies or as a part of the overall UTM solution.

**Video Solution:** Watch the video solution “7-3: Configuring an Inbound Filter” on the accompanying disc.

## Case Studies for Chapter 8

### Case Study 8-1: Securing a Wireless Device

**Scenario:** You have a new client, a small marketing office with six computers and a SOHO router/WAP. The client wants you to secure the device so that the internal computers will be safe and so that the wireless network will be difficult to attack.

Define eight ways that you can protect this wireless network.

---

---

---

---

---

---

---

---

### Case Study 8-2: Enabling MAC Filtering

**Scenario:** As part of the previous scenario, you decide to enable MAC filtering on the client's WAP. Your task is to allow access only to specific MAC addresses for three Windows computers, a Linux computer, and a Mac computer. Explain how you would find out the MAC addresses for those computers, and give an example of a MAC address. Then, describe how MAC filtering can be enabled given this setting.

### Case Study 8-3: War-driving...and the Cure

**Scenario:** Your boss has heard of these “war-drivers” and has obvious concerns of unauthorized access to your wireless network. He wants to have proof that it will be difficult for a war-driver to access the network, and that there are no jamming devices or other interference-based devices within the perimeter of the building.

Your job is to scan the building, make any configurations necessary, and explain how you have configured the wireless network to be war-driver-proof.

---

---

---

---

---

---

---

### Case Study 8-4: Planning Network Security

**Scenario:** You have been given a new assignment at your organization's newly built sister office. You have been tasked with installing several security technologies to protect the LAN and WLAN.

Take a look at Table 8-4, which includes a list of problems that you need to tackle. In the Your Solution column, enter the device, technology, or other solution that you would employ for each situation. Be concise and brief in your answers. This Case Study spans the content within Chapters 5 through 8.

**Table 8-4** LAN and WLAN Security Issues

| Issue                                                                                                                                                        | Your Solution |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| E-mail and web servers need to be separated from the LAN.                                                                                                    |               |
| The WAP is not running any encryption.                                                                                                                       |               |
| Your boss wants additional authentication for the wireless network above and beyond the WAP's inherent ability.                                              |               |
| You have discovered that several computers' wired connections suffer from EMI. They have confidential information and are potential victims for wiretapping. |               |
| The firewall is not configured for the proper type of packet filtering.                                                                                      |               |
| Users on the network need to be protected from malicious content on websites.                                                                                |               |
| You are concerned about anomalous packets and want them to be removed from the network if they are found.                                                    |               |
| There is a long distance wired connection between the firewall and the extranet.                                                                             |               |
| There are areas of the building that are not particularly secure and could be accessed by malicious insiders who could possibly attempt wiretapping.         |               |

## Case Study Solutions

### Case Study 8-1 Solution

There are a host of things you can do to secure a wireless network. The following eight-step list should be incorporated into most plans to secure a WAP, but you will undoubtedly add your own zest to the mix!

- Step 1.** Update firmware. Download the latest firmware, install it, and test it before implementation. Any hotfixes and updates (if the device accepts those) should be installed as well. Check for updates automatically, and have the device's manufacturer e-mail you if new updates are released.
- Step 2.** Set passwords! Enter separate, complex passwords for the administrator and the user accounts.
- Step 3.** Disable remote administration. If it is not necessary, remove this functionality by disabling it. Or, if it is necessary, consider changing the port from the commonly used 8080 to something less well-known.
- Step 4.** Disable SSID broadcasting. Once all computers have been connected, make the wireless network invisible by disabling the SSID. Computers can still connect, in a manual, step-by-step fashion, but at least it will be more difficult to scan for the SSID.

**NOTE** Before anyone ever connects to the WAP, change the SSID from the default name to something less common.

- Step 5.** Enable encryption. As of the writing of this book, WPA2 and AES are the best options. (But anything is better than nothing.) Select a complex preshared key. If possible, use a RADIUS server for authentication.
- Step 6.** Reduce the output transmitting power of the WAP. Sometimes, the wireless network is too powerful and reaches far beyond the physical perimeter of the office. Antennas are set to a specific output power by default (for example, 90 mW). This can be reduced on some WAPs, which will ultimately reduce the range of the wireless network.
- Step 7.** Enable MAC filtering. This configuration allows you to allow or deny specific MAC addresses.
- Step 8.** Configure other rules and ACLs. This might include inbound filters, access control policies, application rules, and so on. Depending on your organization's

function, you might decide to implement other options such as captive portals and secure VPN.

In Steps 7 and 8, be sure that you don't lock down your WAP too tightly, or you might end up restricting access to clients that legitimately need to access your wireless network.

**Video Solution:** Watch the video solution: "8-1: Securing a Wireless Device" on the accompanying disc.

### Case Study 8-2 Solution

MAC addresses are groups of six hexadecimal numbers, separated by hyphens or by colons.

Example: 00-1C-C0-A1-54-1B

Find out the MAC address of a Windows computer by accessing the Command Prompt and typing `ipconfig /all`.

Find out the MAC address of a Linux or Mac computer by opening the Terminal and typing `ifconfig`.

Write down all MAC addresses that are to be given access to the WAP. Then, access the WAP's firmware, usually from your web browser.

**NOTE** Consider a secure web browser such as Firefox when doing this type of work. Regardless, make sure the browser is updated, and verify that no one is attempting to shoulder surf your computer while you access the WAP!

Access the MAC filter configuration area (sometimes also called *network filter*). Select the Allow Only These Computers option, or similar name. Add each individual MAC address and save the settings. Then test the system to make sure the computers in question can access the wireless network.

**Video Solution:** Watch the video solution: "8-2: Enabling MAC Filtering" on the accompanying disc.

### Case Study 8-3 Solution

The first step is to scan the area to find out what wireless networks are visible. This can be done in several ways. For example, you could use just about any mobile device with Wi-Fi enabled, and search for wireless networks. From that you can glean the name of the wireless network, the connection speed/type, and whether encryption is used. Or, you could do this from a wireless-enabled desktop or laptop computer by using the built-in wireless network finding software, either by Microsoft, by another OS manufacturer, or by a network adapter manufacturer. But, one of the best ways is to use a third-party program such as NetStumbler. This can give very detailed information about the wireless networks that are available. In fact, it is the type of tool that war-drivers would use, so it makes sense for you, as the security administrator, to use it as well, and see what your enemy sees.

Next, based on your wireless scans and physical inspections, you want to locate and shut down any unauthorized WAPs, rogue devices, or evil twins, and remove any devices causing interference or jamming.

Then, for the authorized WAPs, reduce the power level of the antennas until you can scan them from inside the perimeter of the office but not from the outside. This may take several attempts to get it just right, but it pretty much eliminates the attacker's ability to scan for your network. This is a common method, especially if you are using 802.11n or 802.11ac, which have powerful ranges. Of course, this does not address malicious insiders, but other solutions such as authentication, NIDS/NIPS, and so on can be used to deal with them.

If possible, disable the SSID to make it invisible. The SSID broadcast is not the only way that a WAP can be located, but disabling it is a good first step.

Finally, secure the authorized WAPs in the manner you did during Case Studies 1 and 2. Update the device, set complex passwords, use strong encryption, and consider MAC filtering.

**Video Solution:** Watch the video solution: "8-3: War-driving...and the Cure" on the accompanying disc.

### Case Study 8-4 Solution

As you can see, being in charge of the security for a network can be a lot of work—a full-time job perhaps, given the size of a network. Remember that you are attempting to do the following:

- Ensure that *confidential* files remain secret.
- Keep the *integrity* of your data intact.
- Make sure that data is still *available* to the appropriate persons.

Use the CIA approach to help govern your actions as a security administrator. Add layers of security so that you end up with a solid defense-in-depth plan, ultimately protecting your network and data on multiple levels. See Table 8-5 for some possible solutions to the issues you face.

**Table 8-5** LAN and WLAN Security Issues and Solutions

| Issue                                                                                                                                                                                                                                    | Your Solution                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| E-mail and web servers need to be separated from the LAN.                                                                                                                                                                                | Implement a DMZ.                                                                                        |
| The WAP is not running any encryption.                                                                                                                                                                                                   | Configure WPA2 and AES.                                                                                 |
| Your boss wants additional authentication for the wireless network above and beyond the WAP's inherent ability.                                                                                                                          | Utilize a RADIUS server or similar external authentication device.                                      |
| You have discovered that several computers' wired connections suffer from EMI. They have confidential information and are potential victims for wiretapping.                                                                             | Replace unshielded twisted-pair (UTP) connections with shielded twisted-pair (STP).                     |
| The firewall is not configured for the proper type of packet filtering.                                                                                                                                                                  | Implement SPI, and increase the level of NAT filtering if necessary.                                    |
| Users on the network need to be protected from malicious content on websites.                                                                                                                                                            | Use a proxy server with a content filter.                                                               |
| You are concerned about anomalous packets and want them to be removed from the network if they are found.                                                                                                                                | Install an inline NIPS between the firewall and the Internet or in between the firewall and the switch. |
| There is a long distance wired connection between the firewall and the extranet.<br>There are areas of the building that are not particularly secure and could be accessed by malicious insiders who could possibly attempt wiretapping. | Use fiber-optic connections between the firewall and extranet. Install a CCTV system.                   |

**Simulation:** Complete the simulation: “8-4: Planning Network Security.”

## **Case Studies for Chapter 9**

## Case Study 9-1: Choosing Physical Security Methods

**Scenario:** You are the security administrator for Prowse Inc., a technology research firm that has 20 users in the main office, several offsite computers, a data center, and an unsecured computer lab. Your task is to use physical methods to secure these computers.

Name eight types of physical security methods and define them in Table 9-4. The solution to Case Study 9-1 may have different answers than yours.

**Table 9-4** Types of Physical Security Methods

## Case Study 9-2: Selecting the Correct Authentication Technology

**Scenario:** There are many types of authentication technologies. Your organization employs two localized authentication technologies and two remote authentication technologies. Your organization uses a Microsoft Windows Server that runs Active

Directory. Also, your organization uses the PPTP protocol. Finally, the remote authentication technology uses UDP as the transport mechanism.

Your task is to identify the four types of authentication technologies your organization uses, describe each one briefly, and specify the inbound port for each. Enter that information in Table 9-5.

**Table 9-5** Authentication Technologies Your Organization Uses

| Authentication Technology | Brief Description | Port Number Used |
|---------------------------|-------------------|------------------|
|                           |                   |                  |
|                           |                   |                  |
|                           |                   |                  |
|                           |                   |                  |

### Case Study 9-3: Understanding 802.1X

**Scenario:** You are in charge of implementing an 802.1X solution. Your job is to first define the three main elements of an 802.1X authentication scheme. Next, you must specify the exact technologies you will use for each of those three main elements.

In Table 9-6, describe the three main elements of 802.1X. Then, use the Internet to research actual types of 802.1X-compliant network adapters and components that you can use to create an actual working 802.1X authentication scheme.

**Table 9-6** 802.1X Authentication Elements

| <b>802.1X Element</b> | <b>Description</b> | <b>Actual Component</b> |
|-----------------------|--------------------|-------------------------|
|                       |                    |                         |
|                       |                    |                         |
|                       |                    |                         |
|                       |                    |                         |

### Case Study 9-4: Setting Up a Secure VPN

**Scenario:** Your boss wants to enable remote access for several people who will be working from home. You are now in charge of implementing a secure VPN solution for the data commuters.

Name a couple of vendors that offer secure VPN solutions. Describe the two main protocols that are used with VPN connections and specify their port numbers.

---



---



---

## Case Study Solutions

### Case Study 9-1 Solution

There are many types of physical security methods. Table 9-7 gives eight examples and basic descriptions for them based on the scenario in Case Study 9-1.

**Table 9-7** Types of Physical Security Methods—Solution

| <b>Physical Security Method</b> | <b>Description</b>                                                                                                  |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------|
| CCTV                            | Closed-circuit television, used to monitor and record images from server rooms and data centers.                    |
| Cable locks                     | Used to physically lock down computers and monitors; for example, computers in an otherwise unsecured computer lab. |

---

### **Physical Security Description**

#### **Method**

|                   |                                                                                                                                                                                                                                                                                                    |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cipher lock       | A type of door lock that uses a basic cipher mechanism where the numbers of the code have to be entered sequentially—often push button operated. Used in server rooms, data centers, and even for entrances to offices.                                                                            |
| Proximity badges  | Basic swiping cards used to allow access to an office or to a server room. The card (or badge) need only be in close proximity to the sensor for the door in question.                                                                                                                             |
| Safe              | A wonderful way to protect items such as optical discs, backup tapes, USB flash drives, application and development discs, and so on.                                                                                                                                                              |
| <b>Mantrap</b>    | A secure area that can be used to hold a person until that person is authenticated to the area ahead. Often used as entrances to server rooms and data centers (and even offices), while still allowing a means of egress in the case of an emergency.                                             |
| Biometric scanner | Often a type of scanner that can be used on laptops and other mobile devices. It connects via USB and will usually scan a thumbprint. This type of physical security works great for computers that are located outside the office; for example, computers used by salespersons or data commuters. |
| Smart cards       | Like proximity badges, something a person <i>has!</i> For example, a Common Access Card, which has an embedded chip that can authenticate a user. Excellent choice for highly secure areas such as server rooms and data centers.                                                                  |

Your organization’s physical security methods will vary. They will be based on the IT security budget as well as the level of confidentiality of your data. Consider researching additional methods of physical security on the Internet.

**Simulation:** Complete the simulation “9-1: Choosing Physical Security Methods.”

### **Case Study 9-2 Solution**

This chapter contains many types of authentication technologies, but this particular Case Study scenario was asking for four: Kerberos and LDAP, which are used by Active Directory on Microsoft Windows Server domain controllers; a Remote Access Service—namely VPN—in this case utilizing PPTP; and RADIUS server, which uses UDP as its transport mechanism. See Table 9-8 for the rest of the solution.

**Table 9-8** Authentication Technologies Your Organization Uses—Solution

| <b>Authentication Technology</b>       | <b>Brief Description</b>                                                                                           | <b>Port Number Used</b>                         |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| Kerberos                               | Authenticates users in an Active Directory environment.                                                            | 88                                              |
| LDAP                                   | Controls access for users and computers in an Active Directory environment.                                        | 389                                             |
| Remote Access Service (VPN using PPTP) | Allows remote access for computers outside the LAN.                                                                | 1723                                            |
| RADIUS                                 | A powerful remote authentication technology used in conjunction with VPN. It utilizes the UDP transport mechanism. | 1812 and 1813<br>(sometimes port 1645 and 1646) |

**Simulation:** Complete the simulation “9-2: Selecting the Correct Authentication Technology.”

### Case Study 9-3 Solution

The three main elements of an 802.1X authentication scheme include the supplicant, the authenticator, and the authentication server. There are several companies that offer products that comply with 802.1X secure authentication. See Table 9-9 for descriptions and examples of companies that offer solutions.

**Table 9-9** 802.1X Authentication Elements—Solution

| <b>802.1X Element</b> | <b>Description</b>                                                                         | <b>Actual Component</b>                                                               |
|-----------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Supplicant            | A software client running on a workstation. This is also known as an authentication agent. | Many network adapters (wired and wireless) from Intel and Cisco are 802.1X compliant. |
| Authenticator         | A wireless access point or switch.                                                         | Cisco and D-Link have options for 802.1X-compliant WAPs and switches.                 |
| Authentication server | An authentication database.                                                                | Microsoft Windows RADIUS Server.                                                      |

**Video Solution:** Watch the video solution “9-3: Understanding 802.1X” on the accompanying disc.

**Simulation:** Complete the simulation “9-3: Understanding 802.1X.”

### Case Study 9-4 Solution

A couple of vendors that offer secure VPN solutions for small offices include D-Link and Cisco (through its subsidiary Linksys), among other manufacturers of SOHO routers. For larger environments you would look to companies such as Cisco, Microsoft, Juniper, and so on. The two main protocols that can be used in a secure VPN solution include PPTP (port 1723) and L2TP (port 1701). L2TP requires specialized certificate services, whereas PPTP does not.

Use the Internet to further research the variety of VPN solutions available.

**Video Solution:** Watch the video solution “9-4: Setting Up a Secure VPN” on the accompanying disc.

## Case Studies for Chapter 10

### Case Study 10-1: Configuring Complex Passwords

**Scenario:** You are not only the security administrator for your organization, but also the IT trainer! Teach your users how to set passwords in Windows, Linux, and OS X. But more importantly, show them how to check if their passwords are complex enough to meet today’s standards. Finally, show the junior network admins how to enforce complex passwords.

In Table 10-3, describe the following:

- How you would set passwords in Windows, Linux, and OS X
- How to check the complexity of passwords online
- What method should be used to enforce complex passwords

**Table 10-3** Configuring Complex Passwords

| Task                                                   | Your Solution |
|--------------------------------------------------------|---------------|
| Configure Windows password                             |               |
| Configure Linux password                               |               |
| Configure OS X password                                |               |
| Identify where to check complexity of passwords online |               |
| Choose method to enforce complex passwords             |               |

### Case Study 10-2: Configuring Password Policies and User Account Restrictions

**Scenario:** As the network security administrator of a company with 5000 users, you are required to enforce complex passwords, and make sure that user access to the network is restricted to specific times. More importantly, you *must* employ a certain level of automation. Let's face it, even the fastest computer operator wouldn't be able to keep up with all of the password requests and timeframe configurations for users on an individual basis. Your organization has a Windows domain with three domain controllers.

In your own words, describe how you would enforce complex passwords and user account restrictions. Explain how you would automate the process, utilize templates, and work with organizational units.

### Case Study 10-3: Understanding Access Control Models

Access control can deal with a lot of different things, but in technology what we are most concerned with is the access to data and how it is controlled.

Use the Internet to research the three main types of access control, and in Table 10-4 give a description of each and an example of technology environments for each.

**Table 10-4** Access Control Models

| Access Control Model | Description | Example |
|----------------------|-------------|---------|
| DAC                  |             |         |
| MAC                  |             |         |
| RBAC                 |             |         |

## Case Study 10-4: Configuring User and Group Permissions

**Scenario:** You are required to configure permissions for users on your network. To simplify the process, also create user groups that will allow you to group the users together (most likely by the department of your organization) and apply permissions to multiple users within the group at one time.

Using this book and the Internet, research how you would apply permissions to users, and how you can create groups on a Windows computer.

## Case Study Solutions

### Case Study 10-1 Solution

Training users is one of the best ways to increase the security of your IT environment. It can be difficult to keep some users' attention, so you have to make it interesting. Appeal to their curiosity, and have the users practice, practice, practice to make things stick. Remember that users are not techies (usually), and might learn in a different way and at a different pace.

Remember too that users might work with Windows, Linux, OS X, iOS, Android, or other operating systems, each with its own way of configuring passwords and passcodes. Also keep in mind that there are many ways to accomplish something in Windows and other operating systems. Table 10-5 gives a few examples.

**Table 10-5** Configuring Complex Passwords Solution

| Task                                                    | Possible Solution                                                                                       |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Windows password configuration                          | Press Ctrl+Alt+Del and select Change Password.<br>Change the password in Control Panel > User Accounts. |
| Linux password configuration                            | Open Terminal, then type passwd.                                                                        |
| OS X password configuration                             | Open Terminal, then type passwd.<br>Change the password in System Preferences > Users & Groups.         |
| Where to check complexity of passwords                  | Use online password checkers such as the Microsoft Password Checker or The Password Meter.              |
| What method should you use to enforce complex passwords | Implement well-written password policies to enforce the use of complex passwords.                       |

**Video Solution:** Watch the video solution “10-1: Configuring Complex Passwords” on the accompanying disc.

**Simulation:** Complete the simulation “10-1: Password Strength.”

### Case Study 10-2 Solution

A network security administrator will have far too much work to do to have to worry about individual password requests, or to deal with configuring users one at a time.

So, the smart admin will utilize password policies that are based on individual organizational units (OUs) in Windows or other similar grouping structures in other operating systems. These policies will default to a self-reset mode, where the users change the passwords themselves, when prompted by the system. And the policy will make sure that the user meets the complexity requirements.

User account restrictions can be configured through policies and also by creating a basic user template, from which other user accounts are based off of, effectively copying any restrictions from the template to the new user.

By automating as much as possible, the admin reduces the amount of time required on basic configurations, and can spend more time researching the latest CVEs and installing their updates.

**Video Solution:** Watch the video solution “10-2: Configuring Password Policies and User Account Restriction” on the accompanying disc.

**Simulation:** Complete the simulation “10-2: Configuring Logon Hours.”

### Case Study 10-3 Solution

There is some overlap when it comes to access control models. That is partially true because the functional definitions of the various access models have changed over time, and the software that uses them has changed over time as well. For example, you might see that FreeBSD is considered to be either MAC-based or RBAC-based depending on its implementation.

Table 10-6 gives sample descriptions and examples of the three main access control models.

**Table 10-6** Access Control Models—Solution

| Access Control Model | Description                                                                                                                           | Examples                                                                                   |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| DAC                  | Access control policy generally determined by the owner. Objects such as files and printers can be created and accessed by the owner. | Windows domains<br>Linux Red Hat networks                                                  |
| MAC                  | Access control policy determined by a computer system, not by a user or owner.                                                        | Military<br>Government                                                                     |
|                      | Defines sensitivity labels that are assigned to <i>subjects</i> (users) and <i>objects</i> (files and folders).                       | SELinux<br>Multilevel secure (MLS) systems; for example, NSA, Boeing, Honeywell, and so on |
| RBAC                 | Controlled by the system, but works with sets of permissions known as roles.                                                          | Solaris<br>SAP<br>Active Directory (server roles)                                          |

**Simulation:** Complete the simulation “10-3: Understanding Access Control Models.”

### Case Study 10-4 Solution

One great resource on the Internet for details about configuring permissions is Microsoft TechNet (<http://technet.microsoft.com>). It has all kinds of step-by-step instructions that show you how to do just about anything in Windows operating systems. Case in point: working with users and groups, whether on a Windows client or server. Practice working with users and groups and watch the video on this subject on the disc.

**Video Solution:** Watch the video solution “10-4: Configuring User and Group Permissions” on the accompanying disc.

## Case Studies for Chapter 11

### Case Study 11-1: Understanding Risk and Vulnerability

Risk is the possibility of an attack or threat compromising your IT infrastructure. It is normally accomplished by exploiting vulnerabilities in computers, networks, and even people.

**Scenario:** You work for a medium-sized business with 200 computers and users. The company has experienced extremely fast growth, and until now, has not been concerned with risk. Your task is to define risk to your company, and develop plans to deal with it effectively. The board of directors is interested in finding out the annualized loss expectancy for the company's servers. The board also wishes to have some kind of management plan in place that includes the analyzing of network documentation, and the mitigating of threats and potential compromise.

Question 1: What type of risk assessment should you recommend?

Question 2: Because you don't know exactly what will happen to your company's servers in the future, it is impossible to predict exactly what will happen to them, and when, and how much it will cost. What concept, in addition to your risk assessment method, can aid in this?

Question 3: What kind of management plan should you implement? What basic steps does it entail?

(View the solution to this case study before moving on to the next case study.)

### Case Study 11-2: Mapping and Scanning the Network

**Scenario:** Now that you have developed plans for risk assessment and vulnerability assessment, it's time to get your hands dirty and find out what's actually happening on your network. Your job is to use utilities that will help you identify the servers and other computers on the network, and scan for vulnerabilities on those computers.

Warning: The following should be performed on a closed, test network.

Access the Internet and locate two network mapping programs and two network scanning programs. Look for free utilities, or utilities that have free trials. Download and install those programs, then create a basic map of the network, and define some of the vulnerabilities such as open ports on your computers.

### Case Study 11-3: Defending Against Password Cracking

It's been said over and over again—weak passwords can easily be cracked. There are plenty of free tools available on the Internet that can crack a weak password in a matter of seconds.

**Scenario:** You are in charge of a small peer-to-peer Windows network where people configure their own passwords on computers that have no other configured security than the out-of-the-box security that comes with the operating system. Your task is to test the users' passwords, and set up a way to enforce the usage of complex passwords. You are not allowed to know the current user passwords (unless of course you can crack them!).

Use freely downloadable tools to test accounts (and their passwords). Then define what a complex password is. Finally, explain how you can enforce whether people use complex passwords.

## Case Study Solutions

### Case Study 11-1 Solution

Remember, solutions to these types of scenarios will vary. The following is one possible solution to the needs of your company.

First, you should recommend a *quantitative* risk assessment. This uses exact monetary values: SLE × ARO = ALE (the aforementioned annualized loss expectancy).

The problem with quantitative risk assessments is that they are based on the past history of your actual organization. To go beyond this, and perhaps predict the future with a bit more certainty, consider using concepts such as mean time between failures (MTBF). This information can be obtained from the manufacturer of a device. It consists of data gathered from many customers that ultimately shows the average failure time of the device in question. Instead of relying solely on your own data and how costly failures were, you can utilize the data of other customers (anonymous of course) to better find the median, or average, for failures, and predict the future with more clarity.

Finally, you should implement a vulnerability management plan. This means documenting the network, testing the attack surface of servers, scanning systems internally and remotely, mitigating any vulnerabilities you find, and monitoring carefully.

**Simulation:** Complete the simulations 11-1a, 11-1b, and 11-1c on the accompanying disc.

## Case Study 11-2 Solution

*Remember to perform these types of tests on a closed network that you are allowed to have access to.*

A couple examples of network scanning programs include Network Topology Mapper (previously LANsurveyor) and Spiceworks, but there are others as well. Use what works best for you. Two examples of port scanners are Nessus and Nmap (though these are actually full-blown vulnerability scanners). On a Windows client computer, type in the command `netstat -an`. In the left-hand column you will more than likely find that ports 135 and 139 are open (among many others). Some ports such as these need to be open so the computer can be “networkable.” But other ports might need to be closed. From a remote system, scan the same computer with the Nessus and Nmap programs to find out what ports are visible from the network.

**Video Solution:** Watch the video solution “11-2: Mapping and Scanning the Network” on the accompanying disc.

## Case Study 11-3 Solution

*Remember to perform these types of tests on a closed network that you are allowed to have access to.*

Passwords can be very insecure out-of-the-box. An account is generally configured with no password by default. In addition, different operating systems have different ways of *hashing* the password. In fact, in Windows there are multiple ways of hashing, depending on the Windows version and several other factors. (We’ll discuss more about hashing later in the book.) Aside from the lack of default security, users often select very simple passwords such as *love*, *secret*, or the best one, *password*. Those passwords are just about as good as using no password at all. For example, a four-character password can be cracked by today’s password-cracking programs in a matter of seconds.

There are plenty of tools out there that you can download for free and use to check the quality of users’ passwords; for example, Cain & Abel, ophcrack, and Rainbow-Crack. Try out some of these programs on a closed network (and a clean machine) and see how they function. You will see that they are designed to use various password-cracking methods (brute force, for example) that are very good at breaking LM and NTLM password hashes in Windows.

In many networks, the chances are you will find a lot of non-complex passwords—ones that can be cracked very easily. How to fix this? Do the following:

- Give the administrator account a complex password. (Also consider making a secondary administrator account—with a complex password—and disabling the original admin account.)
- Disable generic accounts and give them a complex password.
- Set up a policy that governs the type of password that is chosen by users.

Now, that last bullet will vary depending on the type of network. In a small peer-to-peer network that has, say, five or six Windows computers, the policy would have to be configured on one machine, then exported, and imported to the rest of the computers. In this scenario you would go to Run and type `secpol.msc`. That displays the Local Security Policy, and from there you would access Account Policies > Password Policy, where you would enforce complexity and a minimum password length. In a larger network, such as a Windows domain, you would configure the policy based on the OU in question, and/or use the `gpedit.msc` utility.

**Video Solution:** Watch the video solution “11-3: Defending Against Password Cracking” on the accompanying disc.

## Case Studies for Chapter 12

### Case Study 12-1: Capturing and Analyzing Packets

**Scenario:** You are doing work for a medium-sized business with several servers. There is concern that one of the servers is running a non-secured FTP service, and is possibly being used for non-work purposes. Your task is to analyze the traffic coming in and out of the server.

What technology should you use to analyze the traffic?

What are a couple of examples of this technology?

Which layer of the OSI model will tell you about the ports being used by applications?

### Case Study 12-2: Deciphering Log Files

**Scenario:** The same organization used in Case Study 12-1 has concerns about its firewall. The IT director thinks that an attacker on the Internet is attempting (and

possibly succeeding) in bypassing the firewall, but doesn't know how it is potentially being done or what port is being used to do it.

What application/protocol can you use to easily analyze the firewall logs from your workstation?

How would you configure this on the firewall and at your workstation?

Describe a typical log message with attempted communication and the two main components of it.

If you see a message such as the one listed below, what does it tell you?

```
Tues Apr 21 12:36:01 2014 Cisco Firewall System Log: Blocked incoming
TCP packet
```

```
From 64.58.137.211:23475 65.82.117.241:23 as SYN:ACK received but
there is no active connection.
```

### Case Study 12-3: Auditing Files

**Scenario:** You've analyzed packets, checked Syslogs, and checked for vulnerabilities on the firewall. As a final precaution you want to make sure that no one is accessing your file server and compromising the integrity of your data files.

You decide to enable auditing on the server. What steps are involved to accomplish this?

## Case Study Solutions

### Case Study 12-1 Solution

It's a good idea to periodically analyze the traffic that is sent and received by servers. This can help when you are concerned about a potential compromise, or just think that the server is being used incorrectly.

There are lots of technologies used to analyze traffic, but the best for this scenario is the protocol analyzer, otherwise known as a network sniffer or packet sniffer. Examples of these tools include Wireshark, Network Monitor, NetScout, TCPdump and snoop (command-line only), WinDump, Network Observer, and so on. Wireshark is extremely common and (as of the writing of this book) is a free download. It's the transport layer of the OSI model that tells all. It defines the port number being used on the source computer and the destination. It also describes the transport mechanism being used (TCP or UDP). The network layer is also important as this shows the IP addresses being used by the communicating systems. The application layer shows what program is being used, but many network and security admins will jump right to the transport layer and glean that information (and much more info) from the port numbers.

**Video Solution:** Watch the video solution “12-1: Capturing and Analyzing Packets” on the accompanying disc.

**Simulation:** Complete the simulation “12-1: Capturing and Analyzing Packets” on the accompanying disc.

### Case Study 12-2 Solution

Use the Syslog protocol. There are many Syslog programs available, such as SolarWinds Kiwi Syslog Server. This can pull the logs from a firewall and other network devices so that you can watch them in real time from your workstation.

The firewall would need to have Syslogging enabled and configured to stream log messages to the IP address of your workstation. A typical log message will be generated by the firewall when someone on the Internet attempts to connect to it. It will have the source IP address and port as well as the destination IP address and port; for example:

S=207.50.135.54:53 – D=10.1.1.80:1

In the Case Study’s Syslog message listed, you are told a lot of information, including the potential attacker’s IP address and the port used, as well as the IP address of your firewall and the port that was attempted for access; in this case port 23 Telnet. The important part here is that the TCP packet was *blocked*. So the firewall succeeded in blocking the potential attack and remained secure. However, devices will fail sometimes. The key is to fail securely. An example of a secure failure would be if a firewall let a packet through (which *will* happen) but the result was that the firewall was shut off immediately after by an automated mechanism. Another example would be if an IPS blocked a packet that was legitimate. This is a failure, but a secure one, albeit an inefficient one. Another example is if a WAP let a potential attacker through but redirected the person to a honeypot, or if the WAP shut down altogether.

If you believe that an attacker is possibly getting through the firewall, then some active scanning will be appropriate. Connect to the firewall from the public side and use a port scanner such as Nmap or a vulnerability scanner such as Nessus (or both) to find out what (if any) open ports there are and if any of these are substantial vulnerabilities.

**Video Solution:** Watch the video solution “12-2: Deciphering Log Files” on the accompanying disc.

**Simulation:** Complete the simulation “12-2: Deciphering Log Files” on the accompanying disc.

### Case Study 12-3 Solution

Auditing is an excellent way to check for data integrity issues, check for breach of permissions, or to simply make sure that your files are being accessed exactly the way you want!

For example, auditing can be enabled on a Windows Server and you can review who tried to access what, and whether they succeeded or failed. What you are most interested in is the attempted deletion or modification of data. The basic steps involved with auditing include enabling auditing in a policy, turning on auditing for a data folder (or other resource) in question, and finally, reviewing the Security log often.

**Video Solution:** Watch the video solution “12-3: Auditing Files” on the accompanying disc.

## Case Studies for Chapter 13

### Case Study 13-1: Understanding Symmetric and Asymmetric Algorithms

**Scenario:** You have been tasked with selecting cryptographic algorithms for internal storage and for Internet-based transmissions. Select the strongest symmetric and asymmetric algorithms possible for each situation.

What algorithm should you select for encrypting an entire hard drive on a laptop?

What asymmetric algorithm should you select for the key exchange during a login to a secure website (using HTTPS)?

What symmetric algorithm should you select for the data exchange during a secure web session?

### Case Study 13-2: Disabling the LM Hash

**Scenario:** Your organization is concerned with the current level of password security. Your task is to make sure that a strong cryptographic hash is used.

If you find that the organization is currently using the LANMAN hash, what should you upgrade to?

In what two ways can you disable the LM Hash?

## Case Study Solutions

### Case Study 13-1 Solution

It's a fact—there are lots of cryptographic algorithms to choose from, but the ones that are the most secure make up a pretty short list. The key here (pun intended) is to select algorithms that will secure data as best possible, while working quickly to do so. The answers below are examples. You might find other answers that better suit your needs, and of course, new algorithms are released periodically.

The most common algorithm used for whole disk encryption (such as BitLocker) is AES. AES 256-bit is preferred. This is a symmetric algorithm that uses a block cipher.

There are three excellent answers for secure key exchange over the Internet; they are all asymmetric. First is RSA 2048-bit. It is commonly used by websites, but it has a massive key length, so elliptic curve technologies are also used: The Diffie-Hellman version ECDH (or ephemeral version ECDHE), and the DSA version (ECDSA). These use less computational power because the elliptic curve method uses a shorter key length.

The best symmetric algorithm for data exchange during a secure web session is AES. However, you might also see RC4 used. In fact, some websites will offer AES connections, until too many users are connected simultaneously; at that point, the additional users will receive RC4-based certificates.

**Video Solution:** Watch the video solution “13-1: Understanding Symmetric and Asymmetric Algorithms” on the accompanying disc.

**Simulation:** Complete the simulation “13-1: Understanding Symmetric and Asymmetric Algorithms” on the accompanying disc.

## Case Study 13-2 Solution

You should upgrade to the NTLMv2 cryptographic hash. Make sure that is running and that the LM hash has been disabled. This can be done by turning it off in the local security policy—OU or domain policy if configuring it for a Microsoft domain—and by disabling it in the Registry.

**Video Solution:** Watch the video solution “13-2: Disabling the LM Hash” on the accompanying disc.

## Case Studies for Chapter 14

### Case Study 14-1: Understanding PKI

**Scenario:** Your boss wants you to set up a new website for customers that will allow for a secure login directly on the home page. Your task is to locate two vendors of SSL certificates that have up to 256-bit AES encryption and also offer RSA encryption for key exchange.

Identify two SSL certificate vendors and describe their services.

Define what an SLA is.

Explain what happens if more than a certain level of users connect simultaneously.

### Case Study 14-2: Making an SSH Connection

**Scenario:** A company you consult for wants to make secure connections to two Linux systems so that they can be remotely controlled in the command-line. The company does not want to use the deprecated Telnet utility. You decide to recommend the SSH protocol because of its known security advantages over Telnet.

What is SSH?

What port does it use, and which computers should have that port open?

What kind of secure algorithm does it support?

What program(s) can you use to remotely control the Linux systems from the command-line?

## Case Study Solutions

### Case Study 14-1 Solution

There are plenty of Secure Sockets Layer (SSL) certificate providers. Examples include VeriSign, Comodo, GoDaddy, DigiCert, and Thwate. The more trusted providers (such as VeriSign) use that trust to increase the price of their products.

A typical SSL certificate from VeriSign will offer RSA 2048-bit asymmetric key exchange with SHA1 hashing, as well as variable symmetric session encryption. As of the writing of this book, it would be common to have 256-bit AES for a certain number of users, and any users that connect beyond that would get 128-bit AES or RC4 connections.

An SLA is a service-level agreement, which is effectively a contract defining the terms of service. We'll discuss this more later in the book.

It's important to note that this technology changes quickly. Encryption methods are often considered uncrackable—that is until they are cracked, and then there is a complete paradigm shift in the technology once again. It's unavoidable. For example, in 2009, a lot of websites used Triple DES (168-bit) for the session data. AES was still gaining traction, but now (as of the writing of this book), just five years later, AES is the standard, and Triple DES is all but extinct. Chances are, the algorithm of choice will be completely different every five years or so. Make sure you don't sign SLAs that have a span of more than two years. Keep the contracts short, review your technology (and the PKI used) often, and reconsider your options as time goes on.

**Video Solution:** Watch the video solution “14-1: Understanding PKI” on the accompanying disc.

### Case Study 14-2 Solution

SSH stands for Secure Shell, and is a cryptographic protocol used to secure communications and command-line-based remote login. It uses port 22 by default. The computer that will be logged in to needs to have SSH installed and inbound port 22 open. SSH2 (as of the writing of this book) is the more secure version of SSH. It supports public key authentication using certificates (X.509), RSA, and DSA. File transfer can be secured by using SFTP. The copying of files can also be secured using SCP. By default these use TCP as the transport mechanism, but can also use

STCP. For these file transfers it supports the 3DES, AES, and Blowfish symmetric algorithms.

The most commonly used program to remotely control Linux systems in the command-line is the PuTTy program. It is an open source terminal emulator that allows control over the remote computer, and network file transfer. It has support for a wide variety of operating systems. Other SSH clients include Open SSH, Dropbear, and Tera Term, though their support for operating systems will vary.

**Video Solution:** Watch the video solution “14-2: Making an SSH Connection” on the accompanying disc.

## Case Study for Chapter 15

### Case Study 15-1: Configuring RAID

**Scenario:** You have a mission-critical server that cannot be allowed to fail completely. And this time you have some IT budget to work with. You must make sure that the operating system, applications, *and* the data does not fail.

What type of RAID should you use to make sure the OS and applications are available all of the time?

What type of RAID should you implement to ensure that data will be accessible, even in the event of a failure? For the fault tolerance of the data, should you opt for a hardware solution or a software solution? Should it be internal or external?

## Case Study Solution

### Case Study 15-1 Solution

You should strongly consider **RAID 1** (mirroring) with disk duplexing to protect the OS and the applications. This is the type of solution that will mirror the C: drive. If one drive fails, the other will continue to work with no downtime. You can replace the drive during off-hours.

For the data, **RAID 5**, 6, and possibly 10, are highly recommended. With **RAID 5**, if one drive fails, the data remains accessible. In RAID 6, two drives can fail and the data remains accessible. And of course, the data can be rebuilt from the parity data when you are ready. If you have the budget backing you, the best option is to use external hard drive boxes with hot-swappable capabilities.

**Video Solution:** Watch the video solution “15-1: Configuring RAID” on the accompanying disc.

**Simulation:** Complete the simulation “15-1: Configuring RAID” on the accompanying disc.

## Case Studies for Chapter 16

### Case Study 16-1: Identifying Social Engineering Attacks

**Scenario:** As an IT professional, you realize that your job spans much more than just computers. For instance, it deals with the intangible world of social engineering. You have recently taken over the position of security administrator for a company with 200 users, but prior to your new appointment there was little if any security. You are concerned with people that were previously allowed access to the building and how those people might try to infiltrate your company in the future through social engineering techniques.

Conduct research on the Internet and give one example each of pretexting, hoaxes, and malicious insiders. Then, define ways that you would protect your company, data, and employees from these social engineering methods.

### Case Study 16-2: Imaging a Hard Drive and Live Data for Forensic Purposes

**Scenario:** You work for a small organization and wear multiple hats: network administrator, cable installer, security administrator, and digital forensic analyst, when required. Upper management is concerned that an employee (who left work suddenly and didn’t return) might have been attempting to compromise the organization’s secret data. Your task is to document the potential crime scene (the ex-employee’s workstation), analyze the data on the computer, and see if there is any merit to the organization’s concerns.

Name a couple forensically acceptable software tools you can use to image the hard drive.

Name a forensically acceptable software tool you can use to copy the live data.

Name a couple LiveCDs that you can use to image the drive (which may or may not be forensically acceptable).

## Case Study Solutions

### Case Study 16-1 Solution

You can read all kinds of stories about social engineering experts, and the cons they have pulled off. They might be true, they might not. What matters is this: Does it sound feasible? And if so, how would you protect against it? For example, Kevin Mitnick is one of the most well-known masters of social engineering (as well as a top-notch hacker). Supposedly, in his early days, he found out from a bus driver where he could get his own ticket punch, and therefore ride the city bus for free. How did he do this? Probably through the grooming of trust, or the bus driver simply liked him, but effectively there was some kind of pretexting going on somewhere along the way. People who are good at employing social engineering techniques are usually very knowledgeable of psychology in one way or another. They can relate to the person they are attempting to con. So, in the case study scenario, can you think of anyone who used to work for the company that fits this image? Could your company withstand a sweet-talking impersonator? To protect against this, identification and authorization become your best friends.

One common example of a hoax is the virus hoax. These come in many shapes and sizes, but are usually either received through e-mail or show up on a website that a user has been redirected to. The hoax might state that the user's computer will catch on fire in 10 minutes, or perhaps that the computer's files have all been encrypted. (Be careful here, though, because there is actual ransomware attacks that will do just this.) The real problem with virus hoaxes is not that they cause computers to fail, but that they decrease productivity: people discuss the hoax, and they forward it (as requested) to friends and co-workers. To defend against this from a technical standpoint, implementing e-mail filters, updating firewalls, IDS/IPS, and updating AV software are all recommended. To protect from a user standpoint, you should train your users what to be on the lookout for. Give actual examples on a computer screen. Explain that it is very unlikely that a computer will catch fire from a virus. Train users to screen their e-mails carefully and to not open or accept unknown attachments. In the case they do get a display that says their computer is doomed, or to pay a ransom immediately, the best thing to do is shut off the computer and notify the IT personnel.

Malicious insiders are among the deadliest, because they already have access to a certain extent, and getting full access is just one step away. Examples of victims and their respective malicious insiders include USB PaineWebber and Roger Duronio (logic bomb); the DoD and Bradley Manning (release of classified documents to WikiLeaks); and the city of San Francisco and Terry Childs (network tampering)—the examples go on and on. More often than not, these people are disgruntled and perhaps want some kind of revenge. But there are plenty of cases in which the

person was simply in it for the money. But the motive doesn't really matter to a security administrator, because the end result is increased chaos, decreased productivity, and loss of money for the company. So it is a matter of protection, but how? Here are some tips. First, remember your *lessons learned*. Learn from past attacks, whether you have read about them or they have happened to your company. Understand how the attack occurred, and what security control could have prevented it. Next, protect the most important data first. For example, work on patents, the design schematics for a new computer, the code for an unreleased computer program, the secret ingredient in your latest and greatest barbecue sauce—whatever it is, use all of your security power to protect that all-important data first and foremost. Watch for suspect behavior. Human Resources will probably keep a file on people with suspect attitudes, so you should interface with HR often. Watch for quick terminations and resignations. It's good manners for an employee to give two weeks' notice so as to gracefully transition work to other employees. Quick resignations are a red flag. But all this is commentary—the real way to protect against these threats is to have strong policies, well-planned permissions, tough physical security, strong authentication, and enforcement of principles such as need-to-know and least privilege.

**Simulation:** Complete the simulations “16-1: Identifying Social Engineering Attacks” Parts A and B on the accompanying disc.

### Case Study 16-2 Solution

The key with a potentially compromised computer is to document everything you see (and can't see). Take photos, write down what you encounter, and of course, use software and hardware tools to *image* the machine.

For example, to image a hard drive you might use AccessData's Forensic Toolkit, or Guidance Software's EnCase. These are commonly used tools that are usually accepted by the courts as forensically sound applications. Of course, these tools come with a price tag attached (a hefty one), and so in some cases a smaller company will go with simply imaging the drive bit by bit, which could be done with cloning software, or with a LiveCD (or LiveDVD) such as Knoppix or BackTrack. The question here is whether these tools (and the resulting hard drive images) will be acceptable to a court of law. Also, you have to be very careful not to disturb the original drive when making the image, something that can easily be done when using a tool not designed specifically for the job.

If you were to use a LiveCD—and there are many options—it would be derived from Linux, and so a solid knowledge of the command-line would be necessary.

For example, if you were to image a drive, you would need to understand the syntax of the dd and nc commands. Plus, you would need to copy the data from one system to another. Many forensic analysts will use a Linux OS (such as Ubuntu) as the destination computer for the copied image. That system would have a secondary drive that could either be analyzed or booted off of if necessary.

For live data—and we are talking about the RAM and other volatile areas of the computer—you could use Live Response, which might run off of a USB key, and Helix software. That is only if the computer is already powered up when you encounter it. If the computer is off, then volatile areas of storage will most likely be cleared.

## Case Study for Chapter 17

### Case Study 17-1: Analyzing Test Questions

If you want to do well on the real exam, you must analyze questions carefully. Getting the answer right is only half the battle. You also need to be able to identify why the incorrect answers are wrong. If there are any concepts that you don't understand in a question, review them, even if they were part of a listed answer that was incorrect. Work on your comprehension of the concepts from a theoretical standpoint as well as a hands-on standpoint. Ultimately, this combination of knowledge will enhance your test-taking skills.

Practice as much as you can. Use the Practice Test software on the disc that accompanies this book. That software emulates the look of the real exam. By practicing in that environment, you will feel much more comfortable when it comes time to take the real test.

Going further, consider accessing the CompTIA website. As I often say: “Go to the source!” CompTIA often has sample practice questions you can go through to gauge your readiness. They are usually listed directly on the main Security+ page, but if not, search around a little bit, or run a search for “Security+ sample questions.” If they are available, you should be able to find them on CompTIA’s website.

In summary, practice as much as you can, know the correct answers, understand why the incorrect answers are wrong, and then practice some more! The harder you push yourself, the better you will do on the exam.

**Video Solution:** Watch the video solution “17-1: Analyzing Test Questions” on the accompanying disc.

**Table 6-2** Ports and Their Associated Protocols

| <b>Port Number</b> | <b>Associated Protocol (or Keyword)</b> | <b>TCP/UDP Usage</b> | <b>Full Name</b>                                      | <b>Usage</b>                                                                                                                                                      |
|--------------------|-----------------------------------------|----------------------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7                  | Echo                                    | TCP or UDP           | Echo                                                  | Testing round-trip times between hosts.                                                                                                                           |
| 19                 | CHARGEN                                 | TCP or UDP           | Character Generator                                   | Testing and debugging.                                                                                                                                            |
| 21                 | FTP                                     | TCP                  | File Transfer Protocol                                | Transfers files from host to host.                                                                                                                                |
| 22                 | SSH                                     | TCP or UDP           | Secure Shell                                          | Remotely administers network devices and Unix/Linux systems. Also used by Secure Copy (SCP) and Secure FTP (SFTP), which both use TCP as the transport mechanism. |
| 23                 | Telnet                                  | TCP or UDP           | TERminaL NETwork                                      | Remotely administers network devices (deprecated).                                                                                                                |
| 25                 | SMTP                                    | TCP                  | Simple Mail Transfer Protocol                         | Sends e-mail.                                                                                                                                                     |
| 49                 | TACACS+                                 | TCP                  | Terminal Access Controller Access-Control System Plus | Remote authentication. Can also use UDP, but TCP is the default. Compare with RADIUS.                                                                             |
| 53                 | DNS                                     | TCP or UDP           | Domain Name System                                    | Resolves hostnames to IP addresses and vice-versa.                                                                                                                |
| 69                 | TFTP                                    | UDP                  | Trivial File Transfer Protocol                        | Basic version of FTP.                                                                                                                                             |
| 80                 | HTTP                                    | TCP                  | Hypertext Transfer Protocol                           | Transmits web page data.                                                                                                                                          |
| 88                 | Kerberos                                | TCP or UDP           | Kerberos                                              | Network authentication, uses tickets.                                                                                                                             |
| 110                | POP3                                    | TCP                  | Post Office Protocol Version 3                        | Receives e-mail.                                                                                                                                                  |

Table 6-2 2

| <b>Port Number</b> | <b>Associated Protocol (or Keyword)</b> | <b>TCP/UDP Usage</b> | <b>Full Name</b>                                           | <b>Usage</b>                                                                                                                                                             |
|--------------------|-----------------------------------------|----------------------|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 119                | NNTP                                    | TCP                  | Network News Transfer Protocol                             | Transports Usenet articles.                                                                                                                                              |
| 135                | RPC/epmap/dcom-scm                      | TCP or UDP           | Microsoft End Point Mapper/DCE Endpoint Resolution         | Used to locate DCOM ports. Also known as RPC (Remote Procedure Call).                                                                                                    |
| 137–139            | NetBIOS                                 | TCP or UDP           | NetBIOS Name, Datagram, and Session Services, respectively | Name querying, sending data, NetBIOS connections.                                                                                                                        |
| 143                | IMAP                                    | TCP                  | Internet Message Access Protocol                           | Retrieval of e-mail, with advantages over POP3.                                                                                                                          |
| 161                | SNMP                                    | UDP                  | Simple Network Management Protocol                         | Remotely monitor network devices.                                                                                                                                        |
| 162                | SNMPTRAP                                | TCP or UDP           | Simple Network Management Protocol Trap                    | Traps and InformRequests are sent to the SNMP Manager on this port.                                                                                                      |
| 389                | LDAP                                    | TCP or UDP           | Lightweight Directory Access Protocol                      | Maintains directories of users and other objects.                                                                                                                        |
| 443                | HTTPS                                   | TCP                  | Hypertext Transfer Protocol Secure                         | Secure transfer of hypertext through web pages (uses TLS or SSL).                                                                                                        |
| 445                | SMB                                     | TCP                  | Server Message Block                                       | Provides shared access to files and other resources.                                                                                                                     |
| 514                | Syslog                                  | UDP                  | Syslog Protocol                                            | Used for computer message logging, especially for router and firewall logs.<br><br>A secure version (Syslog over TLS) uses TCP as the transport mechanism and port 6514. |

| <b>Port Number</b> | <b>Associated Protocol (or Keyword)</b> | <b>TCP/UDP Usage</b> | <b>Full Name</b>                                     | <b>Usage</b>                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------|----------------------|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 636                | LDAP over TLS/SSL                       | TCP or UDP           | Lightweight Directory Access Protocol (over TLS/SSL) | Secure version of LDAP.                                                                                                                                                                                                                                                              |
| 860                | iSCSI                                   | TCP                  | Internet Small Computer System Interface             | IP-based protocol used for linking data storage facilities.<br>Also uses port 3260 for the iSCSI target.                                                                                                                                                                             |
| 989/990            | FTPS                                    | TCP or UDP           | FTP Secure                                           | Uses SSL/TLS to secure FTP transmissions. 990 is the control port and 989 is the data port.                                                                                                                                                                                          |
| 1433               | Ms-sql-s                                | TCP                  | Microsoft SQL Server                                 | Opens queries to SQL server.                                                                                                                                                                                                                                                         |
| 1701               | L2TP                                    | UDP                  | Layer 2 Tunneling Protocol                           | VPN protocol with no inherent security. Often used with IPsec.                                                                                                                                                                                                                       |
| 1723               | PPTP                                    | TCP or UDP           | Point-to-Point Tunneling Protocol                    | VPN protocol with built-in security.                                                                                                                                                                                                                                                 |
| 1812/1813          | RADIUS                                  | UDP                  | Remote Authentication Dial-In User Service           | An AAA protocol used for authentication (port 1812), authorization, and accounting (port 1813) of users that connect to networks and network services. UDP is the default but as of 2012 can use TCP as well. Compare with TACACS+.<br><br>Other common ports include 1645 and 1646. |

Table 6-2 4

| <b>Port Number</b> | <b>Associated Protocol (or Keyword)</b> | <b>TCP/UDP Usage</b> | <b>Full Name</b>                                    | <b>Usage</b>                                                                                                                                                                               |
|--------------------|-----------------------------------------|----------------------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3225               | FCIP                                    | TCP or UDP           | Fibre Channel over Internet Protocol                | Encapsulates Fibre Channel frames within TCP/IP packets.<br><br>Contrast with Fibre Channel over Ethernet (FCoE), which relies on the data link layer and doesn't rely on TCP/IP directly. |
| 3389               | RDP                                     | TCP or UDP           | Remote Desktop Protocol (Microsoft Terminal Server) | Remotely views and controls other Windows systems.                                                                                                                                         |



The 100 multiple-choice questions provided here help you to determine how prepared you are for the actual exam and which topics you need to review further. Write down your answers on a separate sheet of paper so that you can take this exam again if necessary. Compare your answers against the answer key that follows this exam. Following the answer key are detailed explanations for each question.

# Practice Exam 2: SY0-401

1. Which of the following access control methods is not logical?
  - A. Biometrics
  - B. Software token
  - C. Access control list
  - D. Group Policy
  
2. When should hardware devices' default passwords be changed?
  - A. Once per month
  - B. When the hardware vendor requires it
  - C. When the device is first powered on
  - D. If a threat becomes known
  
3. Which of the following defines the main difference between identification and authentication?
  - A. Authentication verifies the identity of a user requesting credentials, whereas identification verifies a set of credentials.
  - B. Authentication verifies a set of credentials, whereas identification verifies the identity of the network.
  - C. Authentication verifies a user ID that belongs to a specific user, whereas identification verifies the identity of a user group.
  - D. Authentication verifies a set of credentials, whereas identification verifies the identity of a user requesting credentials.
  
4. Which of the following is the rarest type of authentication method?
  - A. Username and password
  - B. Three-factor authentication
  - C. Key cards
  - D. Biometrics

5. Your network is an Active Directory domain controlled by a Windows Server domain controller. The Finance group has read permission to the Reports and History shared folders and other shared folders. The Accounting group has read-and-write permissions to the Reports, AccountRecs, and Statements shared folders. Several users are members of both the Finance and Accounting groups. All the folders are located on a file server. The Everyone group is granted the Full Control NTFS permission for each folder through inheritance, but nonadministrative users do not have the right to log on locally at the server. Access to the shared folders is managed through share permissions. It is determined that the Finance group should no longer have read access to the Reports folder. This change should not affect access permissions granted through membership in other groups. What is the best solution to the problem?
  - A. Deny the read permission to the Finance group for the Reports folder.
  - B. Deny the read permission individually for each member of the Finance group for the Reports folder.
  - C. Remove the read permission from the Finance group for the Reports folder.
  - D. Delete the Finance group.
6. Your network is a Windows domain controlled by a Windows Server domain controller. Your goal is to configure user access to file folders shared to the network. In your organization, directory access is dependent upon a user's role in the organization. You need to keep to a minimum the administrative overhead needed to manage access security. You need to be able to quickly modify a user's permissions if that user is assigned to a different role. A user can be assigned to more than one role within the organization. What solutions should you implement? (Select the two best answers.)
  - A. Create security groups and assign access permissions based on organizational roles.
  - B. Place users in OUs based on organizational roles.
  - C. Create an OU for each organizational role and link GPOs to each OU.
  - D. Place users' computers in OUs based on user organizational roles.
  - E. Assign access permission explicitly by user account.
7. Your organization hires temporary users to assist with end-of-year resources and calculations. All the temporary users need access to the same domain

resources. These “temps” are hired for a specific period of time with a set completion date. Users log on to a Windows domain controlled by a Windows Server domain controller.

Your job is to make sure that the accounts can be used only during the specific period of time for which the temps are hired. The solution you select should require minimal administrative effort and upkeep. Of the following, what is the best solution?

- A. Configure expiration dates for the temp user accounts.
  - B. Configure password expiration dates for temp user accounts.
  - C. Configure a domain password policy for the temp accounts.
  - D. Configure a local password policy on the computers used by temp accounts.
  - E. Delete the temp user’s accounts at the end the work period.
8. Which of the following concepts best describes the mandatory access control model?
- A. Bell-La Padula
  - B. Clark-Wilson
  - C. Biba
  - D. Lattice
9. Which of following statements regarding authentication protocols is false?
- A. MS-CHAPv1 is capable of mutual authentication.
  - B. CHAP is more secure than PAP.
  - C. PAP is insecure because passwords are sent in clear text.
  - D. RADIUS provides authentication and authorization for dial-up access.
10. Which of the following authentication protocols makes use of a supplicant, authenticator, and authentication server?
- A. Kerberos
  - B. 802.1X
  - C. RADIUS
  - D. LDAP

- 11.** Which of the following password management systems will best provide for a network with a large number of users?
  - A.** A multiple access method management system
  - B.** A synchronized password management system
  - C.** A self-service password reset management system
  - D.** A locally saved password management system
- 12.** Which of the following log files identifies when a computer was last shut down?
  - A.** System
  - B.** Security
  - C.** Application
  - D.** Directory Services
- 13.** Which of following log files would be the most useful in determining which internal user was the source of an attack that compromised another computer on the same network?
  - A.** Directory Services logs
  - B.** The attacking computer's audit logs
  - C.** The firewall logs
  - D.** The target computer's audit logs
- 14.** Which of the following methods is the most closely associated with DLL injection?
  - A.** Penetration testing
  - B.** Vulnerability assessment
  - C.** Performance monitoring
  - D.** Auditing
- 15.** You are logging a server. What security measures should you implement? (Select the two best answers.)
  - A.** Perform CRCs.
  - B.** Perform hashing of the log files.
  - C.** Apply retention policies on the log files.
  - D.** Collect temporary files.

- 16.** Which of the following anomalies can a protocol analyzer detect?
- A.** Disabled network adapters
  - B.** Decryption of encrypted network traffic
  - C.** Passive sniffing of network traffic
  - D.** Malformed or fragmented packets
- 17.** When is it appropriate to use vulnerability scanners to identify any potential holes in your security design?
- A.** When testing disaster mitigation planning
  - B.** When testing to identify known potential security risks inherent to your design
  - C.** When testing the network's response to specific attacks
  - D.** When testing the automatic detection and alerts of your network
- 18.** What kind of monitoring methodology does an antivirus program use?
- A.** Anomaly-based
  - B.** Behavior-based
  - C.** Signature-based
  - D.** Statistical-based
- 19.** An IDS looks for patterns to aid in detecting attacks. What are these patterns known as?
- A.** Anomalies
  - B.** Viruses
  - C.** Malware
  - D.** Signatures
- 20.** You have collected login information, file access information, security log files, and unauthorized security violations. What is this collection known as?
- A.** Audit trail
  - B.** Audit
  - C.** Access control list
  - D.** Security log

- 21.** The IT director asks you to determine if weak passwords are used by any of the users on your network. You run a password-cracking program to determine this. What is this an example of?
  - A.** Antivirus scanning
  - B.** Vulnerability assessment
  - C.** Fingerprinting
  - D.** Baselining
- 22.** You need to protect passwords. Which of the following protocols is not recommended because it can supply passwords over the network?
  - A.** DNS
  - B.** ICMP
  - C.** SNMP
  - D.** Kerberos
- 23.** Network utilization is the ratio of current network traffic to the maximum amount of traffic that a network adapter or specific port can handle. Which of the following can help you to determine whether current network utilization is abnormal?
  - A.** Security log
  - B.** Vulnerability assessment
  - C.** Penetration testing
  - D.** Performance baseline
- 24.** A user receives an encrypted message that was encrypted using asymmetric cryptography. What does this recipient need to decrypt the message?
  - A.** Recipient's private key
  - B.** Recipient's public key
  - C.** Sender's private key
  - D.** Sender's public key
- 25.** An employee has been terminated from your organization. What can ensure that the organization continues to have access to the employee's private keys?
  - A.** Store the keys in a CRL.
  - B.** Store the keys in escrow.

- C. Delete the employee's user account.
  - D. Retain the employee's token.
26. What is the greatest benefit of using S/MIME?
- A. You can send e-mails with a return receipt.
  - B. You can send anonymous e-mails.
  - C. It expedites the delivery of your e-mails.
  - D. You can encrypt and digitally sign e-mail messages.
27. What is it called when a hashing algorithm creates the same hash from two different messages?
- A. Collision
  - B. Birthday attack
  - C. Rainbow tables
  - D. MD5
28. MD5 can be manipulated by creating two identical hashes using two different messages, resulting in a collision. This is difficult (if impossible) to do with SHA-1. Why is this?
- A. SHA-1 has greater collision strength.
  - B. MD5 has greater collision resistance.
  - C. MD5 has greater collision strength.
  - D. SHA-1 has greater collision resistance.
29. Which of the following is a disadvantage of PGP?
- A. Weak encryption can be easily broken.
  - B. A recipient must trust a public key that is received.
  - C. Private keys can be compromised.
  - D. Man-in-the-middle attacks are common.
30. What is the main difference between a secure hash and secure encryption? (Select the two best answers.)
- A. A secure hash can be reversed.
  - B. A secure hash cannot be reversed.

- C.** Secure encryption can be reversed.
  - D.** Secure encryption cannot be reversed.
- 31.** Which of the following is used to implement an unencrypted tunnel between two networks?
- A.** HTTPS
  - B.** PPTP
  - C.** AES
  - D.** L2TP
- 32.** Which of the following algorithms depends on the inability to factor large prime numbers?
- A.** AES
  - B.** RSA
  - C.** Elliptic curve
  - D.** Diffie-Hellman
- 33.** Which of the following technologies uses a PSK?
- A.** TPM
  - B.** CRL
  - C.** PGP
  - D.** DES
- 34.** Which of the following can be used to encrypt and decrypt files?
- A.** RC5
  - B.** NTLM
  - C.** SHA-1
  - D.** MD5
- 35.** A user connects to a website, and the session is encrypted through the use of SSL. Which of the following types of keys will be used between the client computer and the web server? (Select the two best answers.)
- A.** Remote entry key
  - B.** Key logger

- C. Public key
  - D. Session key
36. You are in charge of the disaster recovery plan for your organization. What can you do to make sure that the DRP can be implemented quickly and correctly?
- A. Run a test of the recovery plan.
  - B. Send the plan to management for approval.
  - C. Distribute copies of the plan to key personnel.
  - D. Store the recovery plan in a secure area.
37. You are in charge of your organization's backup plan. You need to make sure that the data backups are available in case of a disaster. However, you need to keep the plan as inexpensive as possible. Which of the following solutions should you implement?
- A. Implement a hot site.
  - B. Implement a cold site.
  - C. Back up data to removable media and store a copy offsite.
  - D. Implement a remote backup solution.
38. You are contracted with a customer to protect its user data. The customer requires the following:
- Easy backup of all user data
  - Minimizing the risk of physical data theft
  - Minimizing the impact of failure on any one file server
- Which of the following solutions should you implement?
- A. Back up user files to USB hard disks attached to the customer's systems. Store the USB hard disks in a secure area after hours.
  - B. Use file servers with removable hard disks. Secure the hard disks in a separate area after hours.
  - C. Use internal hard disks installed in file servers. Lock the file servers in a secure area.
  - D. Use file servers attached to a NAS. Lock the file servers and NAS in a secure area.

- 39.** Your company needs to have a backup plan in case power is lost for more than a few hours. Which of the following solutions should you implement?
- A.** UPS
  - B.** Generator
  - C.** Warm site
  - D.** Redundant power supplies
- 40.** You are in charge of decreasing the chance of social engineering. Which of the following should you implement? (Select the two best answers.)
- A.** A two-factor authentication scheme
  - B.** Vulnerability assessment
  - C.** Security awareness training
  - D.** Risk assessment
- 41.** One of your users complains that he received an e-mail from a mortgage company asking for personal information. The user does not recognize this mortgage company as the company with which he first applied for a mortgage for his house. What is the best way to describe this e-mail?
- A.** Hoax
  - B.** Spam
  - C.** Denial of service
  - D.** Phishing
- 42.** You are in charge of recycling computers. Some of the computers have hard drives that contain personally identifiable information (PII). What should be done to the hard drive before it is recycled?
- A.** The hard drive should be sanitized.
  - B.** The hard drive should be reformatted.
  - C.** The hard drive should be destroyed.
  - D.** The hard drive should be stored in a safe area.
- 43.** When you arrive at work in the morning, you discover that the server room has been the victim of a fire, and all the servers have been rendered useless. Which of the following is the most important item to have to ensure that your organization can recover from this disaster?
- A.** Warm site

- B. Offsite backup
  - C. Disaster recovery plan
  - D. Fault-tolerant servers
44. The IT director asks you to protect a server's data from unauthorized access and disclosure. What is this an example of?
- A. Integrity
  - B. Confidentiality
  - C. Availability
  - D. Non-repudiation
45. Which of the following programming techniques can stop buffer overflow attacks?
- A. SQL injection attack
  - B. Input validation
  - C. Sandbox
  - D. Backdoor analysis
46. You have been asked by an organization to help correct problems with users unknowingly downloading malicious code from websites. Which of the following should you do to fix this problem?
- A. Install a network-based intrusion detection system.
  - B. Disable unauthorized ActiveX controls.
  - C. Implement a policy to minimize the problem.
  - D. Use virtual machines.
47. What is it known as when an attacker provides falsified information? (Select the *best* answer.)
- A. Aliasing
  - B. Flooding
  - C. Redirecting
  - D. Spoofing
48. Your LAN is isolated from the Internet by a perimeter network. You suspect that someone is trying to gather information about your LAN. The IT director asks you to gather as much information about the attacker as possible while

preventing the attacker from knowing that the attempt has been detected. What is the best method to accomplish this?

- A.** Deploy a DMZ.
  - B.** Deploy a proxy server in the perimeter network.
  - C.** Deploy a NIPS outside the perimeter network.
  - D.** Deploy a honeypot in the perimeter network.
- 49.** Which of the following methods can possibly identify when an unauthorized access has occurred?
- A.** Session lock mechanism
  - B.** Session termination mechanism
  - C.** Two-factor authentication
  - D.** Previous logon notification
- 50.** You have been contracted to determine if network activity spikes are related to an attempt by an attacker to breach the network. The customer wants you to identify when the activity occurs and what type of traffic causes the activity. Which type of tool should you use?
- A.** Network mapper
  - B.** Protocol analyzer
  - C.** System Monitor
  - D.** Performance Monitor
- 51.** Of the following, what is the service provided by message authentication code?
- A.** Confidentiality
  - B.** Fault tolerance
  - C.** Integrity
  - D.** Data recovery
- 52.** The IT director asks you to set up a system that will encrypt credit card data. She wants you to use the most secure symmetric algorithm with the least amount of CPU usage. Which of the following algorithms should you select?
- A.** AES
  - B.** SHA-1
  - C.** 3DES
  - D.** RSA

- 53.** Your high-tech server room needs a quality fire suppression system. What is the most appropriate type of fire suppression system to install?
- A.** Dry chemical suppression
  - B.** Gaseous fire suppression
  - C.** Wet chemical suppression
  - D.** Dry-pipe sprinkler system
- 54.** Virtualization is a broad term that includes the use of virtual machines and the extraction of computer resources. Which of the following is the best security reason for using virtualization of network servers?
- A.** To centralize patch management
  - B.** To isolate network services and roles
  - C.** To add network services
  - D.** To analyze network traffic
- 55.** Removable media such as USB flash drives can be a threat to security. In what two ways can you mitigate this threat? (Select the two best answers.)
- A.** Run an antivirus scan daily.
  - B.** Disable the USB root hub.
  - C.** Design a written policy stating that USB flash drives are not allowed.
  - D.** Turn off USB in the BIOS.
- 56.** You are the network administrator for your organization. You decide to implement whitelisting, blacklisting, and the closing of open relays. Which of the following threats are you attempting to mitigate?
- A.** Spyware
  - B.** Spam
  - C.** Viruses
  - D.** Worms
- 57.** Your organization implements a policy in which accounting staff needs to be cross-trained in various banking software to detect possible fraud. What is this an example of?
- A.** Separation of duties
  - B.** Least privilege

- C.** Job rotation
  - D.** Due care
- 58.** Your company's T1 has failed. Which of the following enables your users to continue accessing the Internet?
- A.** Redundant ISP
  - B.** RAID 5
  - C.** Redundant servers
  - D.** UPS
- 59.** In an attempt to gain access to discarded company documents, which of the following social engineering attacks might a person implement?
- A.** Phishing
  - B.** Dumpster diving
  - C.** Shoulder surfing
  - D.** Identity theft
- 60.** Which of the following environmental controls is part of the TEMPEST standards?
- A.** Shielding
  - B.** Fire suppression
  - C.** HVAC
  - D.** Biometrics
- 61.** You have completed the deployment of PKI within your organization's network. Legally you are required to implement a way to provide decryption keys to a governmental third party on an as-needed basis. Which of the following should you implement?
- A.** Additional certificate authority
  - B.** Key escrow
  - C.** Recovery agent
  - D.** Certificate registration

- 62.** Which of the following are symmetric encryption algorithms? (Select the four best answers.)
- A.** ECC
  - B.** AES
  - C.** RSA
  - D.** DES
  - E.** RC4
  - F.** Diffie-Hellman
  - G.** 3DES
- 63.** You are in charge of auditing resources and the changes made to those files. Which of the following log files will show any unauthorized changes to those resources?
- A.** System log file
  - B.** Application log file
  - C.** Directory Services log file
  - D.** Security log file
- 64.** Which of the following is used when performing a quantitative risk analysis?
- A.** Asset value
  - B.** Surveys
  - C.** Focus group
  - D.** Best practice
- 65.** You are determining environmental control requirements for a data center that will contain several computers. What is the role of an HVAC system in this environment? (Select the two best answers.)
- A.** Shield equipment from EMI
  - B.** Provide isolation in case of a fire
  - C.** Maintain appropriate humidity levels
  - D.** Provide an appropriate ambient temperature
  - E.** Vent fumes from the data center

- 66.** Which of the following should be performed on a computer to protect the OS from malicious software? (Select the two best answers.)
- A.** Install a perimeter firewall.
  - B.** Update HIPS signatures.
  - C.** Update NIDS signatures.
  - D.** Disable unused services.
  - E.** Disable DEP settings.
- 67.** Which of the following cloud computing services offers easy-to-configure operating systems?
- A.** SaaS
  - B.** IaaS
  - C.** PaaS
  - D.** VM
- 68.** A virus is designed to format a hard drive on a specific day. What kind of threat is this?
- A.** Botnet
  - B.** Logic bomb
  - C.** Spyware
  - D.** Adware
- 69.** Which of the following defines the difference, if any, between a Trojan horse and a worm?
- A.** Worms self-replicate but Trojan horses do not.
  - B.** There is no difference; the two are the same.
  - C.** Worms are sent via e-mail; Trojan horses are not.
  - D.** Trojan horses are malicious attacks; worms are not.
- 70.** You notice that a computer is communicating with an unknown IRC server, and is also scanning older systems on your network. Which of the following threats have you discovered?
- A.** Rootkit
  - B.** Botnet

- C. Spyware
  - D. Worm
71. Which of the following is a common symptom of spyware?
- A. Applications freeze
  - B. Pop-up windows
  - C. Infected files
  - D. Computer shuts down
72. Which of the following should you implement to fix a single security issue on the computer?
- A. Service pack
  - B. Support website
  - C. Patch
  - D. Baseline
73. Which of the following algorithms adhere to the requirement of 128 bits?
- A. AES
  - B. DES
  - C. 3DES
  - D. SHA
74. What kinds of attacks involve intercepting packets on the network and modifying them? (Select the two best answers.)
- A. MITM
  - B. Spoofing
  - C. TCP/IP hijacking
  - D. Null session
  - E. DNS poisoning
75. You check the application log of your web server and see that someone attempted unsuccessfully to enter the text **test; etc/passwd** into an HTML form field. Which attack was attempted?
- A. SQL injection
  - B. Code injection

- C.** Command injection
  - D.** Buffer overflow
- 76.** What are the minimum requirements for a cold site?
  - A.** Location near the data center that meets power requirements
  - B.** Location that meets power and connectivity requirements
  - C.** Location with all required equipment loaded with all updates
  - D.** Location with duplicate systems
- 77.** Which type of social engineering attack relies on impersonation?
  - A.** Dumpster diving
  - B.** Hoaxes
  - C.** Phishing
  - D.** Shoulder surfing
- 78.** You want to prevent any intrusions to a single computer. What is the best solution?
  - A.** VPN concentrator
  - B.** Host-based firewall
  - C.** Host-based intrusion detection
  - D.** Network firewall
- 79.** You find out that confidential information is being encoded into graphic files in a form of security through obscurity. What have you encountered?
  - A.** Digital signature
  - B.** Non-repudiation
  - C.** Confidentiality
  - D.** Steganography
- 80.** 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

- 81.** Your organization does business with in a TEMPEST-certified building. What attack does this help to prevent?
- A.** Weak encryption
  - B.** War-driving
  - C.** Bluejacking
  - D.** Bluesnarfing
- 82.** You perform several war-driving routes in your company's campus and take note of a large number of unauthorized devices. What are these devices?
- A.** Rogue access points
  - B.** EMI
  - C.** Network switches
  - D.** Cell phones
- 83.** What two security precautions can best help to protect against wireless network attacks?
- A.** Authentication and the WEP
  - B.** Access control lists and WEP
  - C.** Identification and WPA2
  - D.** Authentication and WPA
- 84.** You need to gather information about a network attacker but you want to prevent the attacker from knowing that their attempt has been detected. What is the best solution?
- A.** Deploy a proxy server on the perimeter of the network.
  - B.** Deploy a honeypot on the perimeter of the network.
  - C.** Deploy a NIPS outside the perimeter of the network.
  - D.** Deploy a protocol analyzer.
- 85.** What needs to be configured to allow remote access to your network?
- A.** Kerberos
  - B.** Biometrics
  - C.** ACLs
  - D.** Tokens

- 86.** Which of the following protocols does the 802.11i standard support? (Select the two best answers.)
- A.** AES
  - B.** RSA
  - C.** TKIP
  - D.** ECC
  - E.** DES
- 87.** Which of the following is a network addressing scheme that uses numbers and letters?
- A.** IPv4
  - B.** ICMP
  - C.** IGMP
  - D.** IPv6
- 88.** What is a definition of implicit deny?
- A.** Everything is denied by default.
  - B.** All traffic from one network to another is denied.
  - C.** ACLs are used to secure the firewall.
  - D.** Resources that are not given access are denied by default.
- 89.** You are designing security for an application. You need to ensure that all tasks relating to the transfer of money require actions by more than one user through a series of checks and balances.
- What access control *method* should you use?
- A.** Separation of duties
  - B.** Implicit deny
  - C.** Job rotation
  - D.** Least privilege
- 90.** Why do hackers often target nonessential services? (Select the two best answers.)
- A.** Quite often, they are not configured correctly.
  - B.** They are not monitored as often.

- C. They are not used.
  - D. They are not monitored by an IDS.
91. Which of the following is the best example of a strong password?
- A. A 14-character sequence of numbers, letters, and symbols
  - B. The name of your pet
  - C. The last four digits of your Social Security number
  - D. A 15-character sequence of letters only
92. What tool should you use to identify network spike activity?
- A. Network mapper
  - B. Protocol analyzer
  - C. Performance Monitor
  - D. Multimeter
93. Which port number is used by RPC?
- A. 25
  - B. 119
  - C. 135
  - D. 161
94. Which port is used by Microsoft SQL?
- A. 443
  - B. 445
  - C. 1433
  - D. 1723
95. Which of the following is the weakest encryption type?
- A. DES
  - B. RSA
  - C. AES
  - D. SHA

- 96.** Which device is used to encrypt the authentication process?
- A.** WPA
  - B.** HSM
  - C.** Enigma machine
  - D.** Smart card
- 97.** You are configuring security for a network that is isolated from the Internet by a perimeter network. You need to test the network's ability to detect and respond to a DoS attack. What should you implement?
- A.** Port scanning
  - B.** Network packet analysis
  - C.** Penetration testing
  - D.** Vulnerability scanning
- 98.** Which of the following fire extinguishers should be used to put out magnesium- or titanium-based metal fires?
- A.** Class A
  - B.** Class B
  - C.** Class C
  - D.** Class D
- 99.** What is it known as when an unauthorized person follows an authorized person into a restricted area?
- A.** Tailgating
  - B.** Baiting
  - C.** Dumpster diving
  - D.** Phishing
- 100.** Which of the following is software designed to gain administrator-level control over a computer system?
- A.** Spam
  - B.** Rootkit
  - C.** Spyware
  - D.** Worm

## Answers to Practice Exam 2

- |               |               |                        |               |
|---------------|---------------|------------------------|---------------|
| 1. A.         | 26. D.        | 51. C.                 | 76. B.        |
| 2. C.         | 27. A.        | 52. A.                 | 77. C.        |
| 3. D.         | 28. D.        | 53. B.                 | 78. B.        |
| 4. B.         | 29. B.        | 54. B.                 | 79. D.        |
| 5. C.         | 30. B. and C. | 55. B. and D.          | 80. B.        |
| 6. A. and C.  | 31. D.        | 56. B.                 | 81. B.        |
| 7. A.         | 32. B.        | 57. C.                 | 82. A.        |
| 8. D.         | 33. C.        | 58. A.                 | 83. D.        |
| 9. A.         | 34. A.        | 59. B.                 | 84. B.        |
| 10. B.        | 35. C. and D. | 60. A.                 | 85. C.        |
| 11. C.        | 36. A.        | 61. B.                 | 86. A. and C. |
| 12. A.        | 37. C.        | 62. B., D., E., and G. | 87. D.        |
| 13. D.        | 38. B.        | 63. D.                 | 88. D.        |
| 14. A.        | 39. B.        | 64. A.                 | 89. A.        |
| 15. B. and C. | 40. A. and C. | 65. C. and D.          | 90. A. and B. |
| 16. D.        | 41. D.        | 66. B. and D.          | 91. A.        |
| 17. B.        | 42. A.        | 67. C.                 | 92. B.        |
| 18. C.        | 43. C.        | 68. B.                 | 93. C.        |
| 19. D.        | 44. B.        | 69. A.                 | 94. C.        |
| 20. A.        | 45. B.        | 70. B.                 | 95. A.        |
| 21. B.        | 46. B.        | 71. B.                 | 96. B.        |
| 22. C.        | 47. D.        | 72. C.                 | 97. C.        |
| 23. D.        | 48. D.        | 73. A.                 | 98. D.        |
| 24. A.        | 49. D.        | 74. A. and C.          | 99. A.        |
| 25. B.        | 50. B.        | 75. C.                 | 100. B.       |

## Answers with Explanations

**1.** Answer: A. Biometrics.

Explanation: Biometrics is the science of recognizing humans by their physical characteristic traits. It is the only answer listed that is not logical in nature. By logical, we are referring to software-based access control methods. Software tokens, access control lists (ACLs), and group policies are all software-based; therefore they are logical in nature.

See the section titled “Physical Security” in Chapter 9, “Physical Security and Authentication Models,” for more information.

**2.** Answer: C. When the device is first powered on.

Explanation: Most hardware devices use blank passwords as the default. This is an obvious no-no and should be changed when the device is first powered on; it should be the first order of business. It is a common policy for operating system passwords to be changed once per month. In the future, if threats become known, passwords should be modified as well.

See the section titled “Rights, Permissions, and Policies” in Chapter 10, “Access Control Methods and Models,” for more information.

**3.** Answer: D. Authentication verifies a set of credentials, whereas identification verifies the identity of a user requesting credentials.

Explanation: Identification is when a person is in a state of being identified. It can also be described as something that identifies a person, such as an ID card. Authentication is when a person’s identity is confirmed or verified through the use of a specific system based on credentials.

See the section titled “Physical Security” in Chapter 9, “Physical Security and Authentication Models,” for more information.

**4.** Answer: B. Three-factor authentication.

Explanation: Three-factor authentication includes three separate ways that users must identify themselves. For example, a username/password combination, a key card, plus biometric thumbprint. The other single-factor authentication methods are all more common than a three-factor authentication method, with the username/password combination the most common by far.

See the section titled “Rights, Permissions, and Policies” in Chapter 10, “Access Control Methods and Models,” for more information.

5. Answer: C. Remove the read permission from the Finance group for the Reports folder.

Explanation: The best answer is to remove the read permission from the Finance group for the Reports folder. This will ensure that members of the Finance group solely cannot access the folder. However, members with dual membership, such as users who are part of the Accounting group and the Finance group, will still be able to access the folder. Denying the read permission to the Finance group for the Reports folder is incorrect because if the Finance group is denied access, that will override any other permissions, including anyone who is a member of the Finance department and a member of another department (such as Accounting) that is normally allowed access. Bottom line: deny access overrides any other permissions. Denying the read permission individually for each member of the Finance group for the Reports folder is incorrect because of the same reason, but this time each individual user of the Finance group is being denied, which again would include users with dual membership. It is never wise to delete a group because that would have serious implications for all the users involved.

See the section titled “Rights, Permissions, and Policies” in Chapter 10, “Access Control Methods and Models,” for more information.

6. Answers: A. and C. Create security groups and assign access permissions based on organizational roles, and create an OU for each organizational role and link GPOs to each OU.

Explanation: The first thing you should do as a network administrator is create organizational units (OUs) for each of the departments in your organization; this helps to categorize and classify where users will ultimately end up. Each OU will be considered a different role. Next on the list is creating Group Policy objects (GPOs), modifying the security policies, and applying those to each individual OU. Then, you should create the users and place them in their correct OUs according to the department that they will be working in and the role that they will play. Finally, you should create security groups, add users to the appropriate security group or groups, and apply access permissions to the groups, instead of the users, to save time and keep administrative overhead to a minimum. Placing the user’s computer in an OU could cause issues when it comes time to move a user account to another OU; the computer account would need to be moved with it. Access permissions should not be assigned solely by the individual user account; this would increase administrative overhead by a great deal.

See the section titled “Rights, Permissions, and Policies” in Chapter 10, “Access Control Methods and Models,” for more information.

**7.** Answer: A. Configure expiration dates for the temp user accounts.

Explanation: One easy solution is to configure expiration dates for the temp user accounts. This can be done within the Account tab of each user's Properties window. This way, the users cannot log on to the domain after their work period has ended. You cannot configure password expiration dates for the user accounts within the user's Properties window; however, you can configure a policy with a password expiration date, but you have to make additional configurations for this to work properly. By default, the users would simply be asked to change their password when the password expiration date arrives. Password policies can be configured in the same manner (password expiration dates and so on), but they have the same problems as well. Deleting user accounts is usually not a good idea; organizations will generally disable accounts so that they can audit any actions the user accounts have taken in the past. Deleting a user account will make auditing difficult.

See the section titled "Rights, Permissions, and Policies" in Chapter 10, "Access Control Methods and Models," for more information.

**NOTE** You will notice that the previous string of questions all dealt with very similar concepts from the same chapter. Sometimes you will get a string of questions on the real exam that are all similar. Be ready to answer several questions on the same topic in a row!

**8.** Answer: D. Lattice.

Explanation: Mandatory access control has two common implementations: rule-based access control and lattice-based access control. Lattice-based access control is used for more complex determinations of object access by subjects; this is done with advanced mathematics that creates sets of objects and subjects and defines how the two interact. Bell-La Padula is a state machine model used for enforcing access control in government applications. It is a less-common, multilevel security derivative of mandatory access control. This model focuses on data confidentiality and controlled access to classified information. The Biba Integrity Model describes rules for the protection of data integrity. Clark-Wilson is another integrity model that provides a foundation for specifying and analyzing an integrity policy for a computing system.

See the section titled "Access Control Models Defined" in Chapter 10, "Access Control Methods and Models," for more information.

9. Answer: A. MS-CHAPv1 is capable of mutual authentication.

Explanation: MS-CHAPv1 is not capable of mutual authentication. Kerberos is an example of an authentication protocol capable of mutual authentication. This is when the client and the server both verify each other's identity. The rest of the statements are true. CHAP is more secure than PAP because CHAP sends usernames and passwords in an encrypted format, and PAP does not. RADIUS provides authentication and authorization for dial-up access and other types of remote connections; it also provides accountability.

See the section titled “Authentication Models and Components” in Chapter 9, “Physical Security and Authentication Models,” for more information.

10. Answer: B. 802.1X.

Explanation: 802.1X makes use of three components: a supplicant, which is software running on a workstation; an authenticator, which is a wireless access point or switch; and an authentication server, which is an authentication database, most likely a RADIUS server. Kerberos makes use of a key distribution center that works with tickets to prove the identity of users. RADIUS provides centralized administration of dial-up, VPN, and wireless authentication and can be used with 802.1X and EAP (Extensible Authentication Protocol). LDAP (Lightweight Directory Access Protocol) can access and modify directory services data.

See the section “Authentication Models and Components” in Chapter 9, “Physical Security and Authentication Models,” for more information.

11. Answer: C. A self-service password reset management system.

Explanation: When a network has a large number of users, it is difficult to control the passwords that the users use. By using a self-service password reset management system, you rely on the users to reconfigure their passwords after set intervals, which should be set by security policy. Large networks should store the passwords at a controlling server; for example, in a Windows domain, this would be a domain controller.

See the section “Rights, Permissions, and Policies” in Chapter 10, “Access Control Methods and Models,” for more information.

12. Answer: A. System.

Explanation: The System log file shows when a computer was started or shut down. The Security log file shows audit entries. The Application log file shows changes, warnings, or errors to applications built into Windows and third-party applications. The Directory Services log file shows events, warnings, and errors that occur on a domain controller.

See the section “Conducting Audits” in Chapter 12, “Monitoring and Auditing,” for more information.

- 13.** Answer: D. The target computer’s audit logs.

Explanation: The target computers’ audit logs should show the IP address and MAC address of the attacking computer if it were within the same network. It would be difficult to find out who the attacking computer is, which is why you look to the target computer (the computer that was affected by the attack) for clues. Directory Services logs give information about Active Directory on a domain controller. The firewall logs show information concerning attackers from outside the network but will probably not give information about attackers inside the network.

See the section “Conducting Audits” in Chapter 12, “Monitoring and Auditing,” for more information.

- 14.** Answer: A. Penetration testing.

Explanation: Penetration testing is the method most closely associated with DLL injection, which is a technique used to run code within the address space of another process by forcing it to load a dynamic link library. It is used to influence the behavior of a program in a way that the creator of the program did not intend. This type of injection can be incorporated into the Registry in Windows. Penetration testing is a type of active security analysis used to find out if DLL injection attempts will work. The other three answers are not active security and analyses; they are passive. Vulnerability assessment can find open ports and define the threats associated with those ports. Performance monitoring can analyze a server’s resources such as CPU and RAM. Auditing is making a technical assessment of applications, systems, and networks. Auditing often includes reviewing security logs, vulnerability scans, performance logs, and policies.

See the section “Conducting Risk Assessments” in Chapter 11, “Vulnerability and Risk Assessment,” for more information.

- 15.** Answers: B. and C. Perform hashing of the log files, and apply retention policies on the log files.

Explanation: You need to retain log files for future analysis. Log files are normally not deleted, and sometimes operating systems will overwrite events in log files after they reach their maximum size. Careful consideration should be taken when configuring log files. Hashing the log files enables people in the future to verify the integrity of those log files and verify that the files have not been tampered with. A cyclic redundancy check (CRC) is an error-detecting code that runs automatically, and isn’t really something that would

be performed per se. CRCs and collecting temporary files are not necessary when it comes to log files.

See the section “Conducting Audits” in Chapter 12, “Monitoring and Auditing,” for more information.

- 16.** Answer: D. Malformed or fragmented packets.

Explanation: A protocol analyzer usually detects malformed, fragmented, or oversized packets. You can then use a protocol analyzer to delve into those packets and find out why they were defective. You can find out whether network adapters have been disabled by using a variety of command-line tests or by checking the local computer’s Device Manager. A HIDS, NIDS, or NIPS should be able to find out whether encrypted network traffic is being decrypted anywhere other than its intended destination. Identifying passive sniffing of network traffic can be difficult; however, tools are available to locate other computers that are running protocol analyzers in a passive mode. Some vulnerability scanners can accomplish this.

See the section “Using Tools to Monitor Systems and Networks” in Chapter 12, “Monitoring and Auditing,” for more information.

- 17.** Answer: B. When testing to identify known potential security risks inherent to your design.

Explanation: When it is time to identify known potential security risks that might be inherent to the design of your network, it is appropriate to use vulnerability scanners. At other times you may want a more active analysis approach, such as penetration testing, to find out your network’s response to specific attacks, or when testing the automatic detection of those attacks.

See the section “Assessing Vulnerability with Security Tools” in Chapter 11, “Vulnerability and Risk Assessment,” for more information.

- 18.** Answer: C. Signature-based.

Explanation: Antivirus programs normally use signature-based monitoring. IDS solutions also use this. Signature-based monitoring analyzes frames and packets of network traffic for predetermined attack patterns. Anomaly-based monitoring establishes a performance baseline based on a set of normal network traffic and valuations. Behavior-based monitoring looks at the previous behavior of applications and compares that to the current activity on the system. Statistical-based monitoring is another name for anomaly-based monitoring.

See the section “Monitoring Methodologies” in Chapter 12, “Monitoring and Auditing,” for more information.

**19.** Answer: D. Signatures.

Explanation: Signatures are the patterns that an IDS looks for when detecting attacks. This is known as signature-based monitoring and is common to IDS solutions and antivirus programs. Anomalies are detected through the use of anomaly-based monitoring. Viruses and most other types of malware have a specific signature. As long as the signature-based monitoring system has the signature within its database, the virus or other malware should be detected. If the virus is brand new and the signature-based monitoring system has not been updated and does not have the signature of the new virus within its database, the virus just might wreak havoc.

See the section “Monitoring Methodologies” in Chapter 12, “Monitoring and Auditing,” for more information.

**20.** Answer: A. Audit trail.

Explanation: An audit trail is a collection of security log files, unauthorized security violations, and other logged information such as successful or failed logins. And it is a technical assessment made of applications and networks; quite often this includes an audit trail.

See the section “Conducting Audits” in Chapter 12, “Monitoring and Auditing,” for more information.

**21.** Answer: B. Vulnerability assessment.

Explanation: Vulnerability assessments can include password analysis, port scanning, network mapping, and network sniffing. Antivirus scanning might also be included in a vulnerability assessment of an individual computer. Fingerprinting (of an OS) usually means finding all the open ports, entrances, and back doors into a computer. Baselingining is a type of vulnerability assessment but does not deal with password cracking.

See the section “Conducting Risk Assessments” in Chapter 11, “Vulnerability and Risk Assessment,” for more information.

**22.** Answer: C. SNMP.

Explanation: SNMP (Simple Network Management Protocol) can pass passwords over the network. This can be a security risk and should be avoided if possible. DNS and ICMP do not supply passwords over the network. Kerberos can possibly supply passwords over the network, but they will be in an encrypted format and difficult to crack.

See the section “Using Tools to Monitor Systems and Networks” in Chapter 12, “Monitoring and Auditing,” for more information.

**23.** Answer: D. Performance baseline.

Explanation: A performance baseline gives you the normal traffic that a network adapter sees at a specific time. By comparing this to current network utilization (as analyzed by a protocol analyzer or performance monitoring program), you can determine if the current amount of network traffic is abnormal. Security logs show auditing information such as object access and login information. Vulnerability assessments tell you whether there are open ports, weak passwords, and so on. Penetration testing is performed to see how a security system reacts to an attack.

See the section “Conducting Risk Assessments” in Chapter 11, “Vulnerability and Risk Assessment,” for more information.

**24.** Answer: A. Recipient’s private key.

Explanation: The recipient’s private key is necessary to decrypt the message. The recipient’s private key is part of a key pair that also includes the public key that was used to encrypt the message.

See the section “Cryptography Concepts” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**25.** Answer: B. Store the keys in escrow.

Explanation: By storing the keys in escrow, the organization can continue to have access to them, even after the employee has been terminated. A CRL is a certificate revocation list, which stores certificates that have been revoked; for many different reasons, these certificates are no longer in circulation. Usually organizations will have a policy stating that employees’ user accounts should not be deleted. By not deleting the user account, it will continue to be linked to the user’s private keys and to any logged auditing information associated with the employee. Generally, when employees are terminated, the hardware token and users’ accounts will be disabled. A hardware token deals with a different technology than private keys being stored in escrow. The proper place to access the employee’s private keys is within escrow within a PKI.

See the section “Public Key Infrastructure” in Chapter 14, “PKI and Encryption Protocols,” for more information.

**26.** Answer: D. You can encrypt and digitally sign e-mail messages.

Explanation: S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard that provides cryptographic security for electronic messaging such as e-mail. It is used for authentication, message integrity, and non-repudiation. It encrypts and digitally signs e-mail messages. Generally, S/MIME relies on PKI. E-mails can be sent with a return receipt in most of today’s e-mail applications,

such as Microsoft Outlook. By default, e-mails are not sent anonymously. A person would need to maliciously adapt the e-mail to send it in an anonymous fashion. S/MIME does not expedite the delivery of e-mails but most likely slows down the transmission of e-mails because it is encrypting them.

See the section “Security Protocols” in Chapter 14, “PKI and Encryption Protocols,” for more information.

**27.** Answer: A. Collision.

Explanation: A collision occurs when a hashing algorithm creates the same hash from two different messages. The birthday attack is based off of this and uses the birthday paradox probability theory. However, collisions don’t necessarily mean that an attack has occurred. Rainbow tables are lookup tables used in recovering passwords from a hash generated by a hash function. MD5 is the Message-Digest algorithm 5, a widely used hashing algorithm that provides integrity.

See the section “Hashing Basics” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**28.** Answer: D. SHA-1 has greater collision resistance.

Explanation: SHA-1 has greater collision resistance than MD5. SHA-1 employs a 160-bit hash, whereas MD5 employs a 128-bit hash. As of the writing of this book, both MD5 and SHA-1 have vulnerabilities, although SHA-1 is less vulnerable than MD5.

See the section “Hashing Basics” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**29.** Answer: B. A recipient must trust a public key that is received.

Explanation: In PGP (Pretty Good Privacy), a user must trust any public keys that are received to access data from the sender. There is no centralized key distribution in PGP. It uses a web of trust. PGP is based on RSA encryption; as long as the RSA encryption is implemented properly, it should be uncrackable. Private keys are just that, private. They should not be compromised. Man-in-the-middle attacks are not common with PGP; however, PGP has been known to be vulnerable to cryptanalysis attacks through use of Trojan horses.

See the section “Encryption Algorithms” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**30.** Answers: B. and C. A secure hash cannot be reversed, and secure encryption can be reversed.

Explanation: A secure hash cannot be reversed. This is an example of a one-way function. However, secure encryption can be reversed through decryption.

See the section “Cryptography Concepts” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**31.** Answer: D. L2TP.

Explanation: L2TP (Layer Two Tunneling Protocol) implements an unencrypted tunnel between two devices or networks. The protocol that handles encryption in this type of VPN is IPsec. Hypertext Transfer Protocol Secure (HTTPS) secures websites. Point-to-Point Tunneling Protocol (PPTP), which is used in VPNs, has built-in encryption and automatically creates an encrypted tunnel but is less secure than a VPN using L2TP with IPsec. The Advanced Encryption Standard (AES) is common in wireless networks.

See the section “Security Protocols” in Chapter 14, “PKI and Encryption Protocols,” for more information.

**32.** Answer: B. RSA.

Explanation: RSA (Rivest, Shamir, and Adleman) is a public-key cryptography algorithm based on the inability to factor large prime numbers. It is used in many e-commerce scenarios. AES is based on the substitution-permutation network. Elliptic curve is based on the difficulty of certain mathematical problems that generate keys by graphing specific points on a curve. Diffie-Hellman relies on the secure exchange of keys before data can be transferred.

See the section “Encryption Algorithms” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**33.** Answer: C. PGP.

Explanation: PGP (Pretty Good Privacy) uses a preshared key (PSK), which was previously shared between two parties using a secure channel before it is used to decrypt data. TPM stands for trusted platform module. CRL stands for certificate revocation list. DES stands for Data Encryption Standard.

See the section “Encryption Algorithms” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**34.** Answer: A. RC5.

Explanation: RC5 is the only encryption algorithm listed. The other three answers have to do with hashing. RC5 is a symmetric encryption block cipher that has been succeeded by RC6.

See the section “Encryption Algorithms” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**35.** Answers: C. and D. Public key and session key.

Explanation: SSL sessions use a public key, private key, and session key. Remote entry keys are used on cars; they are a physical key. Key loggers can be installed on keyboards as a physical device or as software on an operating system to log all keystrokes a user types.

See the section “Security Protocols” in Chapter 14, “PKI and Encryption Protocols,” for more information.

**36.** Answer: A. Run a test of the recovery plan.

Explanation: By running a test of the recovery plan, you can find out if the plan can be implemented quickly and correctly. Most likely, the first time you run through the tests, you will find several issues that need to be resolved to make the DRP run more efficiently. When your plan is complete, you should send it to management for approval, but that will not ensure that the actual implementation of the plan during a disaster will be quick and efficient. You need to distribute copies of the plan to key personnel, but unless the key personnel are trained properly and a test has been run, you will not know for sure if the DRP can be implemented quickly and efficiently. Storing your copy of the recovery plan in a secure area is an excellent method to ensure that it is not lost, but it doesn’t let people know what the DRP is or ensure that the DRP will be implemented quickly.

See the section “Disaster Recovery Planning and Procedures” in Chapter 15, “Redundancy and Disaster Recovery,” for more information.

**37.** Answer: C. Back up data to removable media and store a copy offsite.

Explanation: Backing up data to removable media and storing it offsite is the least expensive solution. Hot sites and cold sites can cost the organization a lot of money, especially hot sites. Implementing a remote backup solution usually requires some sort of service with a monthly fee. You, as the network administrator, can back up data to removable media and store it offsite without incurring any other fees except for the cost of the removable media.

See the section “Disaster Recovery Planning and Procedures” in Chapter 15, “Redundancy and Disaster Recovery,” for more information.

**38.** Answer: B. Use file servers with removable hard disks. Secure the hard disks in a separate area after hours.

Explanation: Using file servers with removable hard disks is the best answer. All the other answers do not offer easy backup of user data. The time it would take to use separate USB hard disks makes it anything but easy. The idea of locking entire servers in a secure area doesn’t sound easy either. However,

securing removable hard disks in a separate area seems like an easy way to implement the solution. It should also minimize the risk of physical data theft because the hard disks are stored in a secure area. Using multiple file servers should minimize the impact of failure on any one file server.

See the section “Redundancy Planning” in Chapter 15, “Redundancy and Disaster Recovery,” for more information.

**39.** Answer: B. Generator.

Explanation: A backup power generator should be implemented, which is used in the case that power is lost for more than a few hours. Most uninterruptible power supply (UPS) systems provide only electricity for up to an hour. A warm site is not necessary in this scenario. Redundant power supplies are necessary if one power supply within a server fails; however, they do not help in the case of a power outage.

See the section “Redundancy Planning” in Chapter 15, “Redundancy and Disaster Recovery,” for more information.

**40.** Answers: A. and C. A two-factor authentication scheme and security awareness training.

Explanation: Of the listed answers, the two best ways to decrease social engineering are to incorporate security awareness training and implement a multifactor authentication scheme. For example, users might be required to identify themselves with an ID card and by presenting a thumbprint for biometric scanning. Risk assessments and vulnerability assessments are performed to find out what kind of threats an organization faces. A viable threat might include social engineering; however, risk and vulnerability assessments will not decrease the chance of social engineering occurring.

See the section “Social Engineering” in Chapter 16 “Policies, Procedures, and People,” for more information.

**41.** Answer: D. Phishing.

Explanation: Phishing is an attempt at fraudulently obtaining private information. The phisher usually masquerades as another entity and uses e-mail to accomplish its goal. A hoax is an attempt at deceiving people into believing something that is false. The difference between phishing and a hoax can be kind of a gray area. But generally, hoaxes are carried out in person, whereas phishing is done by e-mail or by phone. Spam is the abuse of electronic messaging systems such as e-mail or instant messaging; it is usually used to market illegitimate products. A denial of service is a type of attack associated with servers.

See the section “Social Engineering” in Chapter 16 “Policies, Procedures, and People,” for more information.

**42.** Answer: A. The hard drive should be sanitized.

Explanation: Before a hard drive is recycled, it should be sanitized. Also known as purging, sanitizing is the removal of data in such a way that it cannot be reconstructed by any known technique. At this point the drive can be recycled within the organization or recycled with the rest of the computer. Reformatting the drive is not enough because reformatting leaves data remanence, or data residue. Destroying the drive can render it useless and therefore cannot be recycled. Storing the drive in a safe area is not recycling the drive.

See the section “Legislative and Organizational Policies” in Chapter 16, “Policies, Procedures, and People,” for more information.

**43.** Answer: C. Disaster recovery plan.

Explanation: The single most important thing that you should have in the case of a disaster is a disaster recovery plan (DRP). This needs to detail exactly who you should contact, what you should do, where you should go, and where your data should be located in the case of a disaster.

See the section “Disaster Recovery Planning and Procedures” in Chapter 15, “Redundancy and Disaster Recovery,” for more information.

**44.** Answer: B. Confidentiality.

Explanation: Confidentiality means preventing the access and disclosure of information to unauthorized persons. Integrity means that authorization is necessary before data can be modified by a user. Availability means that data is obtainable regardless of how information is stored, accessed, or protected. Non-repudiation is a concept of ensuring that people cannot refute claims against them; it is accomplished with computer evidence such as log files.

See the section “Security 101” in Chapter 1, “Introduction to Security,” for more information.

**45.** Answer: B. Input validation.

Explanation: Input validation is the best programming technique to stop buffer overflow attacks and is also used to prevent SQL injection attacks. A sandbox is used to run the web scripts in their own testing environment. Backdoors are used in computer programs to bypass normal authentication. Backdoor analysis includes checking the operating system, applications, and firmware on devices and making sure they are updated.

See the section “Securing Other Applications” in Chapter 4, “Application Security,” for more information.

46. Answer: B. Disable unauthorized ActiveX controls.

Explanation: ActiveX controls can be built directly into websites and can contain malicious code that can be easily downloaded by users without their knowledge. ActiveX controls can be disabled in whole or in part within the browser and can also be controlled as add-ons. A NIDS can possibly defend against malicious ActiveX controls to a certain extent, but you should not solely depend on it. Implementing policies is always a good idea, but you don't want to minimize the problem; you want to fix it. The use of virtual machines works well to isolate problems that might occur from ActiveX controls, but it does not fix the problem as far as downloading the malicious code.

See the section “Securing the Browser” in Chapter 4, “Application Security,” for more information.

47. Answer: D. Spoofing.

Explanation: Spoofing is an attack where an attacker masquerades as another person by falsifying information. Types of spoofing attacks include the man-in-the-middle attack and phishing. Aliasing is when a secondary name is given to a computer or other device, usually for legitimate purposes. Flooding is a category of attack that can use different types of packets to flood a device or server to deny service. Redirecting is when a particular connection is redirected to another resource, for example, when mapping a network drive.

See the section “Malicious Attacks” in Chapter 6, “Networking Protocols and Threats,” for more information.

48. Answer: D. Deploy a honeypot in the perimeter network.

Explanation: A honeypot can be used to lure attackers in and trap them while you analyze their methods. The honeypot is usually placed within the perimeter network, which is the DMZ. Proxy servers are usually not placed in the perimeter network; they act as go-betweens, or mediators, for users on the LAN and servers on the Internet. A NIPS can be placed in or out of a perimeter network, but it does not lure in attackers; instead, a NIPS attempts to prevent attacks from happening.

See the section “Firewalls and Network Security” in Chapter 7, “Network Perimeter Security,” for more information.

49. Answer: D. Previous logon notification.

Explanation: Previous logon notification notifies the user and possibly the administrator of when the last-known good logon occurred. If a user knows that they did not log on at that time, it is a good indicator that unauthorized access occurred. Session lock mechanisms can be implemented on several different

types of operating systems. For example, in Windows a policy can be created to lock the computer after a specific timeout. Sessions can also be terminated automatically via systems such as an FTP server after a specific timeout. Two-factor authentication is a type of multifactor authentication in which two types of identification are necessary to gain access to a network.

See the section “Rights, Permissions, and Policies” in Chapter 10, “Access Control Methods and Models,” for more information.

**50.** Answer: B. Protocol analyzer.

Explanation: A protocol analyzer will capture packets and timestamp each one. This tells you exactly what type of packets were captured and when. If the timestamps correspond to the network activity spikes, you know you have a match for the time. By digging into the packets with a protocol analyzer, you can find out exactly what type of traffic is causing the activity. Network mappers such as SolarWinds’ Network Topology Mapper (previously LANSurveyor) locate all the hosts on a network. System Monitor is a program used by Linux, and Performance Monitor is a program used by Windows; both of these monitor a server’s resources such as CPU, RAM, and hard drive.

See the section “Using Tools to Monitor Systems and Networks” in Chapter 12, “Monitoring and Auditing,” for more information.

**51.** Answer: C. Integrity.

Explanation: Message authentication code (MAC) is a short piece of information that authenticates the message in an attempt to guarantee the messages data integrity. The MAC algorithm is sometimes referred to as a cryptographic hash function. To maintain confidentiality, something needs to prevent the disclosure of information to unauthorized persons; it is often done with encryption, but not hashing. Fault tolerance is the capability for a server, network device, or entire network to continue functioning even if an error or attack occurs. Data recovery is necessary if a failure occurs that the network cannot recover from automatically. It is usually part of a disaster recovery plan.

See the section “Hashing Basics” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**52.** Answer: A. AES.

Explanation: AES (Advanced Encryption Standard) is the best solution for this scenario. It uses the least amount of CPU resources yet is the most secure symmetric algorithm listed. SHA-1 is not a symmetric encryption algorithm; it is a hashing algorithm. 3DES is the predecessor to AES; it is not as secure or fast. RSA is an asymmetric encryption algorithm; it is secure but can use a lot of CPU resources.

See the section “Encryption Algorithms” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

- 53.** Answer: B. Gaseous fire suppression.

Explanation: A gaseous fire suppression system is the best way to go in this scenario. Server room equipment can be easily damaged by other types of systems. An example of a gaseous fire suppression system would be FM-200. A less powerful example would be a CO<sub>2</sub> fire extinguisher. Some municipalities require that a sprinkler system be installed, even if a gaseous fire suppression system has already been installed to the server room. If this is the case, a dry pipe sprinkler system will be installed in addition to the gaseous fire suppression system. Multipurpose dry chemical fire extinguishers can be extremely messy and can damage server room equipment easily and therefore should not be used. Wet chemical suppression is even worse. These and water-based fire extinguishers should not be used in server rooms.

See the section “Environmental Controls” in Chapter 16, “Policies, Procedures, and People,” for more information.

- 54.** Answer: B. To isolate network services and roles.

Explanation: Virtualization is the creation of a virtual entity as opposed to an actual server or operating system. The most common type is the virtual machine that runs an entire operating system virtually within the original operating system of the computer. The best security reason for implementing virtualization is to isolate different services and roles. Patch management centralization is done to secure all the client operating systems on the network and make sure that they are up to date. Although network services can be added through the use of virtualization, it is the specific concept of isolating those additional network services that makes virtualization secure. The analysis of network traffic can be done with a protocol analyzer, otherwise known as a network sniffer.

See the section “Virtualization Technology” in Chapter 3, “OS Hardening and Virtualization,” for more information.

- 55.** Answers: B. and D. Disable the USB root hub, and turn off USB in the BIOS.

Explanation: The best way to disable USB flash drives is to turn off USB altogether in the BIOS; however, it can also be turned off by disabling one or more of the USB root hubs within Device Manager in Windows. Disabling the USB flash drive is the best solution when it comes to mitigating this threat. An antivirus scan might find viruses or other malware contained within the USB flash drive; if USB flash drives must be used, it would be wise to set up automatic scanning of removable media before usage is allowed. Written

policies are difficult to enforce; a better option would be to create a software-based policy on the network controlling server.

See the section “Securing Computer Hardware, Peripherals, and Mobile Devices” in Chapter 2, “Computer Systems Security,” for more information.

**56.** Answer: B. Spam.

Explanation: Spam can be prevented by using known good and bad lists of e-mail addresses, known as whitelists and blacklists. It can also be prevented by closing open SMTP relays and by forcing users to authenticate themselves before they are allowed to use the SMTP e-mail server. Viruses, worms, and spyware are all types of malware. They should be prevented with various anti-malware programs and by implementing user education and awareness.

See the section “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

**57.** Answer: C. Job rotation.

Explanation: Job rotation is one of the checks and balances that might be employed to enforce proper separation of duties. Job rotation can increase user insight and skill level and prevent fraud, thereby increasing the security of an organization’s data and applications. It is quite often implemented through the use of cross-training. Separation of duties is when more than one person is required to complete a particular task. The principle of least privilege states that a user will be given only the permissions necessary to complete a task. Due care is the mitigation action an organization takes to defend against the risks that have been uncovered during due diligence.

See the section “Legislative and Organizational Policies” in Chapter 16, “Policies, Procedures, and People,” for more information.

**58.** Answer: A. Redundant ISP.

Explanation: A redundant ISP means that your organization has multiple connections to the Internet. This could be multiple T1s or perhaps lesser secondary Internet connections such as ISDN or dial-up. **RAID 5** is a type of data fault tolerance involving three or more hard drives. Redundant servers cannot help if an Internet connection fails. Examples of redundant servers include failover and clustering. A UPS is used in the case of power failure.

See the section “Redundancy Planning” in Chapter 15, “Redundancy and Disaster Recovery,” for more information.

**59.** Answer: B. Dumpster diving.

Explanation: Dumpster diving is when a person scavenges for private information in an organization’s garbage or recyclable containers. To protect against

this, sensitive documents should be shredded. Phishing is when a masquerader tries to fraudulently obtain private information. Shoulder surfing is when a person uses direct observation to find out information about a target, such as the target's password. A simple resolution for this is for users to shield their screen. Identity theft is when an attacker successfully steals personally identifiable information about a target; this can include Social Security numbers, credit card numbers, and so on. Phishing, dumpster diving, and shoulder surfing are all social engineering attacks used to steal a person's identity.

See the section "Social Engineering" in Chapter 16, "Policies, Procedures, and People," for more information.

**60. Answer: A. Shielding.**

Explanation: Shielding is part of the TEMPEST standards. TEMPEST is a group of standards that refers to the investigations of conducted admissions from electrical and mechanical devices that may or may not compromise an organization. It is important to shield devices such as air conditioners to prevent electromagnetic interference to network devices and cabling. Suppression deals with the prevention of fires. HVAC deals with heating, ventilation, and air-conditioning. Biometrics is the measurement of human characteristics, such as thumbprint scans and voice recognition.

See the section "Environmental Controls" in Chapter 16, "Policies, Procedures, and People," for more information.

**61. Answer: B. Key escrow.**

Explanation: Key escrow should be implemented so that the governmental third party can be provided decryption keys as necessary. Key escrow is when certificate keys are held in the case that third parties such as government or other organizations need access to encrypted communications. Additional certificate authorities are normally implemented as a form of fault tolerance. To avoid single points of failure such as a single CA, certificate authorities can be organized in a hierarchical manner. Key recovery agents are configured if the lost or corrupted keys need to be restored. Certificate registration occurs when a user tries to access secure information and needs to apply for a certificate. The registration might be completed by the certificate authority or by a registration authority.

See the section "Public-Key Infrastructure" in Chapter 14, "PKI and Encryption Protocols," for more information.

**62. Answers: B., D., E., and G. AES, DES, RC4, and 3DES.**

Explanation: AES, DES, RC4, and 3DES are all symmetric encryption algorithms. ECC, RSA, and Diffie-Hellman are asymmetric encryption algorithms.

See the section “Encryption Algorithms” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**63.** Answer: D. Security log file.

Explanation: The Security log file shows any unauthorized changes to the resources that you decide to audit. These resources can include files, folders, printers, and so on. This can work only if object access auditing has been enabled, and if auditing has been turned on for the resource in question. The System log file logs information pertaining to drivers, operating system files, the kernel, and so on. The Application log file logs information pertaining to applications such as Windows Explorer, File Explorer, the Command Prompt, and third-party applications. The Directory Services log file logs information pertaining to the active directory.

See the section “Conducting Audits” in Chapter 12, “Monitoring and Auditing,” for more information.

**64.** Answer: A. Asset value.

Explanation: Asset value is an actual concrete piece of information that you can make risk-based decisions with in a quantitative manner. The other answers are vague at best and don’t give solid details for your risk analysis; they might be better suited for *qualitative* risk analysis.

See the section “Conducting Risk Assessments” in Chapter 11, “Vulnerability and Risk Assessment,” for more information.

**65.** Answers: C. and D. Maintain appropriate humidity levels, and provide an appropriate ambient temperature.

Explanation: An HVAC system should maintain appropriate humidity levels to avoid ESD, and provide an appropriate ambient temperature to avoid overheating of equipment. In many cases, HVAC systems need to be shielded themselves in order to prevent EMI. In the case of a fire, isolation should be provided by actual firewalls—walls around the server room that are insulated properly. There should not be any fumes in the data center; no equipment in a data center or server room should give off any fumes that need to be vented out.

See the section “Environmental Controls” in Chapter 16, “Policies, Procedures, and People,” for more information.

**66.** Answers: B. and D. Update HIPS signatures and disable unused services.

Explanation: An individual operating system should be protected by disabling unused services, and by updating any host-based intrusion detection systems or intrusion prevention systems. Since we’re talking about a single computer,

network intrusion detection systems and perimeter firewalls are not required. DEP stands for data execution prevention and does not apply to this scenario.

See the section “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

- 67.** Answer: C. PaaS.

Explanation: PaaS (platform as a service) is a cloud computing service that offers many software solutions including easy-to-configure operating systems and on-demand computing. SaaS is software as a service, used to offer solutions such as webmail. IaaS is infrastructure as a service, used for networking and storage. VM stands for virtual machine, which is something that PaaS also offers.

See the section “Cloud Security and Server Defense” in Chapter 5, “Network Design Elements,” for more information.

- 68.** Answer: B. Logic bomb.

Explanation: A logic bomb is a type of malware that is designed to be set off at a specific time. It could contain a virus or worm. A botnet is a group of compromised computers known as zombies. Spyware and adware are unwanted programs that are unknowingly downloaded from the Internet, usually through a browser.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

- 69.** Answer: A. Worms self-replicate but Trojan horses do not.

Explanation: The primary difference between a Trojan horse and a worm is that worms will self-replicate without any user intervention; Trojan horses do not self-replicate.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

- 70.** Answer: B. Botnet.

Explanation: A botnet is a group of compromised computers. If a single computer is communicating with unknown servers and scanning other hosts on the network, it could be part of a botnet. A rootkit is designed to gain administrative access to a computer. Spyware is installed through browsers to spy on the activity of an Internet user. A worm is an executable designed to damage a computer system and infect files.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

**71.** Answer: B. Pop-up windows.

Explanation: Pop-up windows are common to spyware. The rest of the answers are more common symptoms of viruses.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

**72.** Answer: C. Patch.

Explanation: A patch can fix a single security issue on a computer. A service pack addresses many issues and rewrites many files on a computer; it may be overkill to use a service pack when only a patch is necessary. You might obtain the patch from a support website. A baseline can measure a server or a network and can be used to obtain averages of usage.

See the section “Hardening Operating Systems” in Chapter 3, “OS Hardening and Virtualization,” for more information.

**73.** Answer: A. AES.

Explanation: AES (Advanced Encryption Standard) can be 128-, 192-, or 256-bit. DES is an older, deprecated algorithm that runs at 64-bit. 3DES runs at 168-bit. SHA runs at either 160-bit, 256-bit, or 512-bit.

See the section “Cryptography Concepts” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**74.** Answers: A. and C. MITM and TCP/IP hijacking.

Explanation: MITM (man-in-the-middle) and TCP/IP hijacking are methods used to intercept network transmissions and modify packets that are captured.

See the section “Malicious Attacks” in Chapter 6, “Networking Protocols and Threats,” for more information.

**75.** Answer: C. Command injection.

Explanation: In this case a command was entered, and the attacker was attempting to gain access to the password file within the /etc directory. If the attacker tried to inject code, they would not use commands, but rather PHP, ASP, or another language. SQL injections are usually run on databases, not web servers’ HTML forms. Buffer overflows have to do with memory and how applications utilize it.

See the section “Secure Programming” in Chapter 4, “Application Security,” for more information.

76. Answer: B. Location that meets power and connectivity requirements.

Explanation: A cold site only requires power and connectivity. All systems and data are configured afterward. Any other requirements would be needed by warm and hot sites—for example, duplicate systems, additional equipment, and a location near the data center.

See the section “Disaster Recovery Planning and Procedures” in Chapter 15, “Redundancy and Disaster Recovery,” for more information.

77. Answer: C. Phishing.

Explanation: Phishing is when an attacker impersonates a legitimate institution; it is implemented via e-mail or phone. Dumpster diving is when a person attempts to gather information by sifting through a company’s garbage. A hoax is when an attacker attempts to make a victim believe something that is not true. Shoulder surfing is when an attacker attempts to gain information or passwords by looking over a user’s shoulder while the user works at a computer, or by examining the user’s desk.

See the section “Social Engineering” in Chapter 16, “Policies, Procedures, and People,” for more information.

78. Answer: B. Host-based firewall.

Explanation: A host-based firewall is the best solution to prevent intrusions to a single computer. Firewalls can block various types of traffic that might include attacks or other intrusions. A VPN concentrator allows remote access for multiple users. Host-based intrusion detection (via an HIDS) will locate an intrusion but not prevent it; to prevent it you would want a host-based intrusion prevention system (HIPS). A network firewall can help to protect an entire network but will not be the best solution if you were only trying to prevent intrusions to a single computer. The host-based firewall will have definitions that are more specific to the types of attacks that might be perpetuated on a single local computer.

See the section titled “Implementing Security Applications” in Chapter 2, “Computer Systems Security,” for more information.

79. Answer: D. Steganography.

Explanation: Steganography is the art and science of hiding messages within other messages. For example, hiding messages within the bits of a graphic file. It is a form of security through obscurity. Digital signatures, non-repudiation, and confidentiality are less ambiguous terms as opposed to steganography.

See the section titled “Cryptography Concepts” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

**80.** Answer: B. Firewall.

Explanation: Install a firewall to protect the network. Protocol analyzers will 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.

See the section titled “Network Design” in Chapter 5, “Network Design Elements,” for more information.

**81.** Answer: B. War-driving.

Explanation: War-driving can be prevented by using TEMPEST-certified techniques. War-driving is when a person attempts to access a company’s wireless network from a laptop within their vehicle. Weak encryption is not an attack, but is definitely something you want to remedy as soon as possible—for example, if a company is using WEP. Bluejacking and bluesnarfing are attacks that are perpetuated on mobile phones and smartphones.

See the section titled “Securing Wireless Networks” in Chapter 8, “Securing Network Media and Devices,” for more information.

**82.** Answer: A. Rogue access points.

Explanation: Rogue access points are unauthorized devices in a wireless network. They should be joined to the network properly and disabled as soon as possible. EMI stands for electromagnetic interference. It is not a device but rather an issue that can plague electronic devices. Shielding is required to reduce EMI. Network switches do not connect to the wireless network, and do not broadcast, so they should not be discovered when you do a war-driving route. Cell phones are common, but your war-driving process should not uncover these devices, and if it does you should filter your program to look specifically for wireless access points and other similar devices.

See the section titled “Securing Wireless Networks” in Chapter 8, “Securing Network Media and Devices,” for more information.

**83.** Answer: D. Authentication and WPA.

Explanation: The best two security precautions are authentication and WPA. Although WPA2 is more secure than WPA, the term identification is not correct. WEP is a deprecated wireless encryption protocol and should be avoided.

See the section titled “Securing Wireless Networks” in Chapter 8, “Securing Network Media and Devices,” for more information.

- 84.** Answer: B. Deploy a honeypot on the perimeter of the network.

Explanation: The best solution is to deploy a honeypot on the perimeter of the network. This will, hopefully, attract and trap the attacker in a simulated environment that they cannot escape from. An added benefit of a properly designed honeypot is that the attacker does not know that their attempt has been detected, and the attacker does not know that they are within a honeypot. Proxy servers act as go-betweens for clients on the network and websites. A NIPS (network intrusion prevention system) prevents attackers from accessing the network. Protocol analyzers are used to capture and analyze packets.

See the section titled “Firewalls and Network Security” in Chapter 7, “Network Perimeter Security,” for more information.

- 85.** Answer: C. ACLs.

Explanation: ACLs (access control lists) need to be configured properly on a firewall to allow users remote access to your network. Kerberos, biometrics, and tokens are all used to grant the local access to a network.

See the section titled “Authentication Models and Components” in Chapter 9, “Physical Security and Authentication Models,” for more information.

- 86.** Answers: A. and C. AES and TKIP.

Explanation: AES and TKIP are supported by the 802.11i standard. This standard deals with wireless transmissions. RSA deals with the encrypting of data through the use of tokens. ECC (elliptic curve cryptography) and DES are also used to encrypt data.

See the section titled “Encryption Algorithms” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

- 87.** Answer: D. IPv6.

Explanation: IPv6 is a network addressing scheme that utilizes IP numbers that are 128-bit and are composed of numbers and letters, due to the fact that they are based on the hexadecimal numbering system. IPv4 uses numbers only. ICMP and IGMP are TCP/IP protocols.

See the section titled “Network Design” in Chapter 5, “Network Design Elements,” for more information.

- 88.** Answer: D. Resources that are not given access are denied by default.

Explanation: If a resource is not given specific access, it will be implicitly denied by default. Access control lists are used to permit or deny access from one network to another and are often implemented on a firewall.

See the section titled “Access Control Models Defined” in Chapter 10, “Access Control Methods and Models,” for more information.

**89.** Answer: A. Separation of duties.

Explanation: Separation of duties is when more than one person is required to complete a task. Contrast this with job rotation, which is when multiple people are required to *know* the same task, but don’t complete it together. Implicit deny is usually the last rule in a firewall rule set. Least privilege means that a program or a person only has the permissions needed to accomplish their task.

See the section titled “Access Control Models Defined” in Chapter 10, “Access Control Methods and Models,” for more information.

**90.** Answers: A. and B. Quite often, they are not configured correctly, and they are not monitored as often.

Explanation: Nonessential services are often not configured and secured by the network administrator; this goes hand in hand with the fact that they are not monitored as often as essential services. It is imperative that network administrators scan for nonessential services and close any corresponding ports. Even though services may be nonessential, that doesn’t necessarily mean that they are not used. An IDS, if installed properly, should monitor everything on a given system.

See the section titled “Assessing Vulnerability with Security Tools” in Chapter 11, “Vulnerability and Risk Assessment,” for more information.

**91.** Answer: A. A 14-character sequence of numbers letters and symbols.

Explanation: the strongest passwords incorporate numbers, letters, and symbols. Easily identifiable information such as the name of your pet or the last four digits of an ID such as a Social Security number or a driver’s license number should not be used as passwords or for account numbers. It is wise to use 14 characters or more in a highly secure environment, but it is important to also use uppercase letters, numbers, and symbols.

See the section titled “Rights, Permissions, and Policies” in Chapter 10, “Access Control Methods and Models,” for more information.

**92.** Answer: B. Protocol analyzer.

Explanation: A protocol analyzer is used to capture network packets and analyze them. It can identify network spikes and a host of other issues that can adversely affect your network. A network mapper is used to create a diagram of your network and discover all the computers on the network. Performance Monitor is a Microsoft program that is used to watch the performance of a computer’s CPU, RAM, and so on. A multimeter is used to test voltage and other electrical properties.

See the section titled “Assessing Vulnerability with Security Tools” in Chapter 11, “Vulnerability and Risk Assessment,” for more information.

- 93.** Answer: C. 135.

Explanation: Port 135 is the RPC (Remote Procedure Call) port. 25 is SMTP. 119 is NNTP. 161 is SNMP.

See the section titled “Ports and Protocols” in Chapter 6, “Networking Protocols and Threats,” for more information.

- 94.** Answer: C. 1433.

Explanation: Microsoft SQL (and the MS-SQL-S service) uses port 1433. Port 443 is used by HTTPS. 445 is used by SMB. 1723 is used by PPTP.

See the section titled “Ports and Protocols” in Chapter 6, “Networking Protocols and Threats,” for more information.

- 95.** Answer: A. DES.

Explanation: Of the listed answers, DES (Data Encryption Standard), developed in the 1970s, is the weakest encryption type; its 56-bit key has been superseded by 3DES (max 168-bit key) and AES (max 256-bit key). DES is now considered to be insecure for many applications. RSA is definitely stronger than DES even when you compare its asymmetric strength to a relative symmetric strength. SHA is a hashing algorithm.

See the section titled “Cryptography Concepts” in Chapter 13, “Encryption and Hashing Concepts,” for more information.

- 96.** Answer: B. HSM.

Explanation: An HSM (hardware security module) is a physical device that acts as a secure cryptoprocessor. It is used for the digital signing of data and login/authentication processes. WPA is a wireless protocol. An Enigma machine is a machine that was used in World War II for the encryption/decryption of secret messages. Smart cards are used to authenticate individuals, but an HSM offers faster software encryption.

See the section titled “Securing Computer Hardware, Peripherals, and Mobile Devices” in Chapter 2, “Computer Systems Security,” for more information.

- 97.** Answer: C. Penetration testing.

Explanation: Penetration testing is required in this scenario. The only way to simulate a DoS attack is to actively test the network with a penetration test of your own design. The other methods are passive attempts at testing the network.

See the section titled “Conducting Risk Assessments” in Chapter 11, “Vulnerability and Risk Assessment,” for more information.

**98.** Answer: D. Class D.

Explanation: Class D fire extinguishers are the type used for combustible metal fires such as ones that can burn magnesium, titanium, and lithium. They are designated with a yellowed decagon. Class A extinguishers are used for ordinary fires that consume wood. Class B extinguishers are used for liquid and gas fires. Class C extinguishers are used for electrical fires.

See the section titled “Environmental Controls” in Chapter 16, “Policies, Procedures, and People,” for more information.

**99.** Answer: A. Tailgating.

Explanation: Tailgating is when an unauthorized person follows an authorized person into a restricted area, without that person’s permission. If the other person was aware, and allowed this behavior, it would be known as piggybacking. Baiting is when an attacker leaves some type of media, such as a USB flash drive, that contains malware, in the hopes that an unknowing user will pick it up and connect it to a computer. Dumpster diving is when an attacker sifts through a company’s garbage to obtain confidential information. Phishing is when an attacker attempts to gain information by posing as an accredited institution.

See the section titled “Social Engineering” in Chapter 16, “Policies, Procedures, and People,” for more information.

**100.** Answer: B. Rootkit.

Explanation: A rootkit is malware that is designed to gain administrator-level control over a computer system without being detected. Spam is the abuse of e-mail. Spyware is malicious software either downloaded unwittingly from a website or installed with third-party software. A worm infects files on a computer and self-replicates.

See the section titled “Computer Systems Security Threats” in Chapter 2, “Computer Systems Security,” for more information.

*This page intentionally left blank*

# Where are the Companion Content Files?

Thank you for purchasing this Premium Edition version of:

**CompTIA® Security+ SY0-401 Authorized Cert Guide, Deluxe Edition, Third Edition**



The print version of this title comes with a disc of companion content. As an eBook reader, you have access to these files—as well as the additional premium edition practice test file—by following the steps below:

1. Go to [www.pearsonITcertification.com/account](http://www.pearsonITcertification.com/account) and log in.
2. Click on the “Access Bonus Content” link in the Registered Products section of your account page for this product, to be taken 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 steps at left, please visit [www.pearsonITcertification.com/contact](http://www.pearsonITcertification.com/contact) and select the “Site Problems/Comments” option. Our customer service representatives will assist you.

---

The Professional and Personal Technology Brands of Pearson



Cisco Press



informIT

PEARSON IT Certification



que

SAMS

VMWARE PRESS