DAVID L. PROWSE

Cert Guide

Learn, prepare, and practice for exam success

- Master every topic on CompTIA's new Security+ SY0-201 exam.
- Assess your knowledge and focus your learning.
- Get the practical workplace knowledge you need!

CompTIA® Security+ SY0-201

DVD FEATURES COMPLETE PRACTICE EXAM

PEARSON

CompTIA Security+ SY0-201 Cert Guide

David L. Prowse

Pearson
800 East 96th Street
Indianapolis, Indiana 46240 USA

CompTIA Security+ SY0-201 Cert Guide

ISBN-13: 978-0-7897-4713-6
ISBN-10: 0-7897-4713-8

Library of Congress Cataloging-in-Publication data is on file.
Printed in the United States of America
First Printing: November 2010

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.

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.

Bulk Sales

Pearson IT Certification offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
international@pearson.com

Associate Publisher
David Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Andrew Cupp

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Apostrophe Editing Services

Indexer
Cheryl Lenser

Proofreader
Sheri Cain

Technical Editor
Aubrey Adams

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Dan Scherf

Book Designer
Gary Adair

Composition
Mark Shirar

Contents at a Glance

Introduction xvii

Part I Systems and Application Security

Chapter 1 Introduction to Security 3

Chapter 2 Computer Systems Security 15

Chapter 3 OS Hardening and Virtualization 57

Chapter 4 Application Security 89

Part II Network Infrastructure

Chapter 5 Network Design Elements and Network Threats 117

Chapter 6 Network Perimeter Security 161

Chapter 7 Securing Network Media and Devices 185

Part III Access Control

Chapter 8 Physical Security and Authentication Models 213

Chapter 9 Access Control Methods and Models 249

Part IV Assessments and Audits

Chapter 10 Vulnerability and Risk Assessment 283

Chapter 11 Monitoring and Auditing 313

Part V Cryptography

Chapter 12 Encryption and Hashing Concepts 349

Chapter 13 PKI and Encryption Protocols 379

Part VI Organizational Security

Chapter 14 Redundancy and Disaster Recovery 403

Chapter 15 Policies, Procedures, and People 435

Part VII Preparing for the CompTIA Security+ Exam

Chapter 16 Taking the Real Exam 469

Practice Exam 1: CompTIA Security+ SY0-201 479

Practice Exam 2: CompTIA Security+ SY0-201 515

Glossary 553

Index 571

DVD

Practice Exam 3: CompTIA Security+ SY0-201

Appendix A Memory Tables 3

Appendix B Memory Tables Answer Key 25

Video Solutions to Hands-On Scenarios

Table of Contents

Introduction xvii

Part I Systems and Application Security

Chapter 1 Introduction to Security 3

Security 101 4

The CIA of Computer Security 4

The Basics of Data Security 6

Think Like a Hacker 7

Review Key Topics 9

Define Key Terms 10

Answer Review Questions 10

Answers and Explanations 11

Chapter 2 Computer Systems Security 15

Computer Systems Security Threats 16

Malicious Software 16

Viruses 16

Worms 17

Trojan Horses 17

Spyware 18

Rootkits 19

Spam 19

Summary of Malware Threats 20

Ways to Deliver Malicious Software 20

Via Software, Messaging, and Media 21

Active Interception 21

Privilege Escalation 21

Backdoors 21

Logic Bombs 22

Botnets and Zombies 23

Preventing and Troubleshooting Malware 23

Preventing and Troubleshooting Viruses 23

Preventing and Troubleshooting Worms and Trojans 27

Preventing and Troubleshooting Spyware 27

Preventing and Troubleshooting Rootkits 29

Preventing and Troubleshooting Spam 30
You Can't Save Every Computer from Malware! 31
Summary of Malware Prevention Techniques 32
Implementing Security Applications 33
Personal Software Firewalls 33
Host-Based Intrusion Detection Systems 34
Pop-Up Blockers 36
Securing Computer Hardware and Peripherals 37
Securing the BIOS 38
Securing Storage Devices 39
Removable Storage 39
Network Attached Storage 40
Whole Disk Encryption 40
Securing Cell Phones and PDAs 41
Review Key Topics 43
Complete Tables and Lists from Memory 43
Define Key Terms 43
Hands-On Labs 43
Equipment Needed 44
Lab 2-1: Using Free Malware Scanning Programs 44
Lab 2-2: How to Secure the BIOS 44
View Recommended Resources 46
Answer Review Questions 47
Answers and Explanations 51

Chapter 3 OS Hardening and Virtualization 57
Hardening Operating Systems 58
Removing Unnecessary Applications and Services 58
Service Packs 62
Windows Update, Patches, and Hotfixes 65
Patches and Hotfixes 67
Patch Management 68
Group Policies, Security Templates, and Configuration Baselines 69
Hardening File Systems and Hard Drives 71
Virtualization Technology 74
Types of Virtualization and Their Purposes 74
Working with Virtual Machines 76

Microsoft Virtual PC 76
Microsoft Windows XP Mode 78
Microsoft Virtual Server 78
VMware 78
Review Key Topics 79
Complete Tables and Lists from Memory 79
Define Key Terms 80
Hands-On Labs 80
Equipment Needed 80
Lab 3-1: Discerning and Updating the Service Pack Level 80
Lab 3-2: Creating a Virtual Machine in Virtual PC 2007 81
View Recommended Resources 82
Answer Review Questions 83
Answers and Explanations 86

Chapter 4 Application Security 89

Securing the Browser 90
General Browser Security Procedures 91
Implement Policies 91
Train Your Users 93
Use a Proxy and Content Filter 94
Secure Against Malicious Code 95
Securing Internet Explorer 96
Securing Firefox 100
Securing Other Applications 103
Review Key Topics 108
Complete Tables and Lists from Memory 108
Define Key Terms 108
Hands-On Labs 109
Equipment Needed 109
Lab 4-1: Securing the Browser 109
Lab 4-2: Disabling Applications with a Windows Server 2003 Policy 110
View Recommended Resources 112
Answer Review Questions 112
Answers and Explanations 114

Part II Network Infrastructure

Chapter 5 Network Design Elements and Network Threats 117

Network Design 118
Network Devices 118
Hub 118
Switch 119
Router 120
Network Address Translation, and Private Versus Public IP 121
Network Zones and Interconnections 123
LAN Versus WAN 123
Internet 123
Demilitarized Zone (DMZ) 124
Intranets and Extranets 124
Network Access Control (NAC) 125
Subnetting 126
Virtual Local Area Network (VLAN) 128
Telephony Devices 129
Modems 130
PBX Equipment 130
VoIP 131
Ports, Protocols, and Malicious Attacks 131
Ports and Protocols 131
Malicious Network Attacks 137
DoS 137
DDoS 140
Spoofing 140
Session Hijacking 141
Replay 142
Null Sessions 143
DNS Poisoning and Other DNS Attacks 143
ARP Poisoning 144
Summary of Network Attacks 145
Review Key Topics 149
Complete Tables and Lists from Memory 149
Define Key Terms 149
Hands-On Labs 150

Equipment Needed 150
Lab 5-1: Port Scanning Basics 150
View Recommended Resources 151
Answer Review Questions 152
Answers and Explanations 157

Chapter 6 Network Perimeter Security 161
Firewalls and Network Security 162
Firewalls 162
Proxy Servers 167
Honeypots and Honeynets 169
NIDS Versus NIPS 170
NIDS 170
NIPS 171
Summary of NIDS Versus NIPS 173
The Protocol Analyzer's Role in NIDS and NIPS 173
Review Key Topics 174
Complete Tables and Lists from Memory 174
Define Key Terms 174
Hands-On Labs 174
Equipment Needed 175
Lab 6-1: Packet Filtering and NAT Firewalls 175
Lab 6-2: Configuring an Inbound Filter on a SOHO Router/Firewall 176
Lab 6-3: Enabling MAC Filtering 177
View Recommended Resources 178
Answer Review Questions 178
Answers and Explanations 181

Chapter 7 Securing Network Media and Devices 185
Securing Wired Networks and Devices 186
Network Device Vulnerabilities 186
Default Accounts 186
Weak Passwords 187
Privilege Escalation 188
Back Doors 188
Network Attacks 189
Other Network Device Considerations 189

Cable Media Vulnerabilities 189
Interference 190
Crosstalk 191
Data Emanation 192
Tapping into Data and Conversations 192
Securing Wireless Networks 195
Wireless Access Point Vulnerabilities 195
Secure the Administration Interface 195
SSID Broadcast 196
Rogue Access Points 196
Weak Encryption 196
Other Wireless Access Point Security Strategies 198
Wireless Transmission Vulnerabilities 199
Bluetooth Vulnerabilities 199
Bluejacking 200
Bluesnarfing 200
Review Key Topics 202
Complete Tables and Lists from Memory 202
Define Key Terms 202
Hands-On Labs 203
Equipment Needed 203
Lab 7-1: Securing a Wireless Device: 8 Steps to a Secure Network 203
Lab 7-2: Wardriving...and The Cure 205
View Recommended Resources 206
Answer Review Questions 206
Answers and Explanations 209

Part III Access Control

Chapter 8 Physical Security and Authentication Models 213
Physical Security 215
General Building and Server Room Security 215
Door Access 216
Biometric Readers 217
Authentication Models and Components 219
Authentication Models 219
Localized Authentication Technologies 220
802.1X and EAP 221
LDAP 224

Kerberos and Mutual Authentication 225
Terminal Services 226
Remote Authentication Technologies 226
Remote Access Service 227
Virtual Private Networks 228
RADIUS Versus TACACS 230
Review Key Topics 233
Complete Tables and Lists from Memory 233
Define Key Terms 233
Hands-On Labs 234
Equipment Needed 234
Lab 8-1: Enabling 802.1X on a Network Adapter 234
Lab 8-2: Setting Up a VPN 235
Lab 8-3: Setting Up a RADIUS Server 236
View Recommended Resources 238
Answer Review Questions 240
Answers and Explanations 244

Chapter 9 Access Control Methods and Models 249
Access Control Models Defined 250
Discretionary Access Control 250
Mandatory Access Control 252
Role-Based Access Control (RBAC) 253
Access Control Wise Practices 254
Rights, Permissions, and Policies 256
Users, Groups, and Permissions 256
Permission Inheritance and Propagation 260
Moving and Copying Folders and Files 260
Usernames and Passwords 261
Policies 264
User Account Control (UAC) 267
Review Key Topics 269
Complete Tables and Lists from Memory 269
Define Key Terms 269
Hands-On Labs 270
Equipment Needed 270

Lab 9-1: Configuring Password Policies and User Account Restrictions 270
Lab 9-2: Configuring User and Group Permissions 272
View Recommended Resources 273
Answer Review Questions 273
Answers and Explanations 278

Part IV Assessments and Audits

Chapter 10 Vulnerability and Risk Assessment 283
Conducting Risk Assessments 284
Qualitative Risk Assessment 285
Quantitative Risk Assessment 286
Security Analysis Methodologies 287
Vulnerability Management 288
Penetration Testing 290
OVAL 290
Assessing Vulnerability with Security Tools 291
Network Mapping 292
Vulnerability Scanning 295
Network Sniffing 297
Password Analysis 298
Review Key Topics 302
Complete Tables and Lists from Memory 302
Define Key Terms 302
Hands-On Labs 303
Equipment Needed 303
Lab 10-1: Mapping and Scanning the Network 303
Lab 10-2: Password Cracking and Defense 304
View Recommended Resources 305
Answer Review Questions 306
Answers and Explanations 310

Chapter 11 Monitoring and Auditing 313
Monitoring Methodologies 314
Signature-Based Monitoring 314
Anomaly-Based Monitoring 315
Behavior-Based Monitoring 315
Using Tools to Monitor Systems and Networks 316

Performance Baselining 316
Protocol Analyzers 318
Wireshark 319
Network Monitor 320
SNMP 321
Conducting Audits 322
Auditing Files 322
Logging 324
Log File Maintenance and Security 327
Auditing System Security Settings 328
Review Key Topics 332
Complete Tables and Lists from Memory 332
Define Key Terms 332
Hands-On Labs 333
Equipment Needed 333
Lab 11-1: Using Protocol Analyzers 333
Lab 11-2: Auditing Files on a Windows Server 335
View Recommended Resources 337
Answer Review Questions 338
Answers and Explanations 343

Part V Cryptography

Chapter 12 Encryption and Hashing Concepts 349

Cryptography Concepts 350
Symmetric Versus Asymmetric Key Algorithms 353
Symmetric Key Algorithms 353
Asymmetric Key Algorithms 354
Public Key Cryptography 354
Key Management 355
Steganography 356
Encryption Algorithms 357
DES and 3DES 357
AES 357
RC 358
Summary of Symmetric Algorithms 359
RSA 359
Diffie-Hellman 360
Elliptic Curve 360

More Encryption Types 361
One-Time Pad 361
PGP 362
Hashing Basics 362
Cryptographic Hash Functions 364
MD5 364
SHA 364
Happy Birthday! 365
LANMAN, NTLM, and NTLM2 365
LANMAN 365
NTLM and NTLM2 367
Review Key Topics 368
Complete Tables and Lists from Memory 368
Define Key Terms 368
Hands-On Lab 369
Equipment Needed 369
Lab 12-1: Disabling the LM Hash in Windows Server 2003 369
View Recommended Resources 370
Answer Review Questions 370
Answers and Explanations 375

Chapter 13 PKI and Encryption Protocols 379
Public Key Infrastructure 380
Certificates 380
Certificate Authorities 381
Single-Sided and Dual-Sided Certificates 384
Web of Trust 384
Security Protocols 384
S/MIME 385
SSL/TLS 386
SSH 386
PPTP, L2TP, and IPsec 387
PPTP 387
L2TP 387
IPsec 388
Review Key Topics 389
Define Key Terms 389

Hands-On Labs 389
Equipment Needed 389
Lab 13-1: A Basic Example of PKI 390
Lab 13-2: Configuring an L2TP-Based VPN with Windows Server 2003 390
Lab 13-3: Making an SSH Connection 394
View Recommended Resources 395
Answer Review Questions 396
Answers and Explanations 399

Part VI Organizational Security

Chapter 14 Redundancy and Disaster Recovery 403
Redundancy Planning 404
Redundant Power 405
Redundant Power Supplies 406
Uninterruptible Power Supplies 407
Backup Generators 408
Redundant Data 410
Redundant Networking 413
Redundant Servers 415
Redundant Sites 415
Disaster Recovery Planning and Procedures 416
Data Backup 416
DR Planning 420
Review Key Topics 423
Complete Tables and Lists from Memory 423
Define Key Terms 423
Hands-On Labs 424
Equipment Needed 424
Lab 14-1: Backing Up Data on a Windows Server 424
Lab 14-2: Configuring RAID 1 and 5 425
View Recommended Resources 427
Answer Review Questions 427
Answers and Explanations 430

Chapter 15 Policies, Procedures, and People 435
Environmental Controls 436
Fire Suppression 436
Fire Extinguishers 436

Sprinkler Systems 438
Special Hazard Protection Systems 438
HVAC 439
Shielding 440
Social Engineering 441
Pretexting 441
Diversion Theft 441
Phishing 442
Hoaxes 442
Shoulder Surfing 443
Eavesdropping 443
Dumpster Diving 443
Baiting 444
Piggybacking 444
Summary of Social Engineering Types 444
User Education and Awareness 445
Legislative and Organizational Policies 445
Data Sensitivity and Classification of Information 447
Personnel Security Policies 448
Acceptable Use 449
Change Management 449
Separation of Duties/Job Rotation 450
Mandatory Vacations 450
Due Diligence 450
Due Care 450
Due Process 450
User Education and Awareness Training 451
Summary of Personnel Security Policies 451
How to Deal with Vendors 452
How to Dispose of Computers and Other IT Equipment Securely 452
Incident Response Procedures 454
Review Key Topics 458
Complete Tables and Lists from Memory 458
Define Key Terms 458
View Recommended Resources 458
Answer Review Questions 459
Answers and Explanations 464

Part VII Preparing for the CompTIA Security+ Exam

Chapter 16 Taking the Real Exam 469

Getting Ready and the Exam Preparation Checklist 469
Tips for Taking the Real Exam 472
Beyond the CompTIA Security+ Certification 475
Hands-On Lab 476

Practice Exam 1: CompTIA Security+ SY0-201 479

Practice Exam 2: CompTIA Security+ SY0-201 515

Glossary 553

Index 571

Elements Available on DVD

Practice Exam 3: CompTIA Security+ SY0-201

Appendix A Memory Tables 3

Appendix B Memory Tables Answer Key 25

Video Solutions to Hands-On Scenarios

Introduction

Welcome to the *CompTIA Security+ SY0-201 Cert Guide*. The CompTIA Security+ Certification is widely accepted as the first security certification you should attempt to attain in your information technology (IT) career. The CompTIA Security+ Certification is designed to be a vendor-neutral exam that measures your knowledge of industry-standard technologies and methodologies. It acts as a great stepping stone to other vendor-specific certifications and careers. I developed this book to be something you can study from for the exam and keep on your bookshelf for later use as a security resource.

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

Because this is a security book, it is a bit more serious than some of my other texts. This may come as a surprise to some, but levity should be used carefully when dealing with security concepts because too much humor can easily confuse the issue and be taken the wrong way. It is my belief that in this fast-paced world of ever-changing technology, an author needs to get right to the point. I understand that you don't have unlimited time for study, so you will notice me being blunt in the way I get to the core of concepts. Don't take offense! This is done by design to aid you in absorbing content quickly.

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. If you have any questions while reading through this book, please feel free to ask them at my website: www.davidlprowse.com.

A NOTE TO INSTRUCTORS I developed this book not only for the individual reader, but also to work well in the classroom setting. To complement this book, I also designed an instructor guide that can be accessed for free from the following link:

www.pearsonhighered.com/educator

The supplemental instructor guide includes a breakdown of each chapter, a sample lesson plan, and plenty of teaching tips and tricks. You can also find PowerPoint presentations and a test bank of questions available for download. And of course, if you have questions about the guide, please let me know at my website. Good luck in your teaching endeavors!

Goals and Methods

The number one goal of this book is to help you pass the 2008 version of the CompTIA Security+ Certification Exam (number SY0-201). To that effect, I have added three 100-question practice exams with explanations. Two are in the text at the end of the book. A third is located on the accompanying DVD (print version of this book only). These tests are geared to check your knowledge and ready you for the real exam. If you would like to purchase more electronic practice questions, go to www.pearsonitcertification.com/0132303381.

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 Topics 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.
- **Memory Tables and Lists**—These can be found on the DVD as Appendix A, "Memory Tables," and Appendix B, "Memory Tables Answer Key." Use them to help memorize important information.
- **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.
- **Hands-On Labs**—There are labs for each chapter (except Chapter 1, "Introduction to Security"). The step-by-step procedures appear at the end of the chapters and corresponding video solutions can be found on the DVD.
- **Review Questions**—At the end of each chapter is a quiz. The 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.

Another goal of this book is to offer support for you—the reader. I have posted additional practice questions, videos, and errata on my website at the following link: www.davidlprowse.com/secplus. And if you have any questions to ask, you can post them in the "Ask Dave" section. Anyone can view the content on the website, but you must register to post questions. Registration is free; all that is needed is a valid e-mail address that is kept strictly confidential. I try my best to answer questions as soon as possible. On the site you can find some free extras as well. Visit often!

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.

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 16 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 and Peripherals	Objectives 1.1, 1.2, and 1.5
3	Hardening Operating Systems Virtualization Technology	Objectives 1.3 and 1.6
4	Securing the Browser Securing Other Applications	Objective 1.4
5	Network Design Ports, Protocols, and Malicious Attacks	Objectives 2.1 and 2.2
6	Firewalls and Network Security NIDS Versus NIPS	Objectives 2.3 and 2.4
7	Securing Wired Networks and Devices Securing Wireless Networks	Objectives 2.5, 2.6, and 2.7
8	Physical Security Authentication Models and Components	Objectives 3.6, 3.7, 3.8, and 3.9
9	Access Control Models Defined Rights, Permissions, and Policies	Objectives 3.1, 3.2, 3.3, 3.4, and 3.5
10	Conducting Risk Assessments Assessing Vulnerability with Security Tools	Objectives 4.1, 4.2, and 4.3
11	Monitoring Methodologies Using Tools to Monitor Systems and Networks Conducting Audits	Objectives 4.4, 4.5, 4.6, and 4.7
12	Cryptography Concepts Encryption Algorithms Hashing Basics	Objectives 5.1, 5.2, and 5.3

Table I-1 CompTIA Security+ Exam Topics

Chapter	Exam Topic	CompTIA Security+ Exam Objectives Covered
13	Public Key Infrastructure Security Protocols	Objectives 5.4, 5.5, and 5.6
14	Redundancy Planning Disaster Recovery Planning and Procedures	Objective 6.1
15	Environmental Controls Social Engineering Legislative and Organizational Policies	Objectives 6.3, 6.4, 6.5, and 6.6
16	Getting Ready and the Exam Preparation Checklist Tips for Taking the Real Exam Beyond the CompTIA Security+ Certification	n/a

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 the CompTIA Security+ SY0-201 objectives 1.3 and 1.6.

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? Probably within a week—maybe sooner, depending on the size and popularity of the organization. And its not just servers! Workstations, routers, switches: You name it; they all need to be updated on a regular basis, 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 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 OSs *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 resources of the organization. Of course, these systems need to maintained and updated (hardened) as well.

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

Foundation Topics

Hardening Operating Systems

An 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 an OS where the controlling user account 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 a computer OS's 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 go about analyzing the system and deciding 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 go about removing 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 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 app are disabled as well. Basically, remove all instances of the application or, if necessary, reimage 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 Vista we can look at the list of installed programs by going to the **Control Panel** and accessing **Programs and Features**, as shown in Figure 3-1.

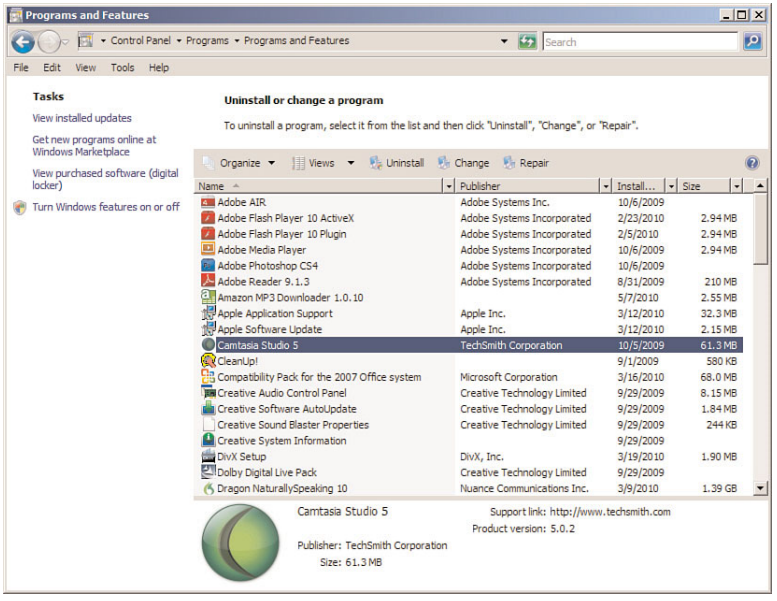

Figure 3-1 Windows Vista Programs and Features Window

Notice in the figure that Camtasia Studio 5 is installed. If in the future I decide to use another program, such as Adobe Captivate or something similar, and Camtasia is no longer necessary, 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 in to the Start menu that you can use. Camtasia takes up 61 MB, so it makes sense to remove apps like this to conserve hard drive space. This becomes more important when you deal with audio/video departments that would use an application (and many others like it) such as Camtasia. They are always battling for hard drive space, and it can get ugly! Not only that, but a lot of applications out there place a piece of themselves in the system tray. So a part of the program actually is running behind the scenes using processor and especially RAM resources. If the application is necessary, there are quite often ways to eliminate it from the

system tray, either by right-clicking the system tray icon and accessing its properties, or by turning it off with a configuration program such as 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 that is deemed necessary should be installed in the future.

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

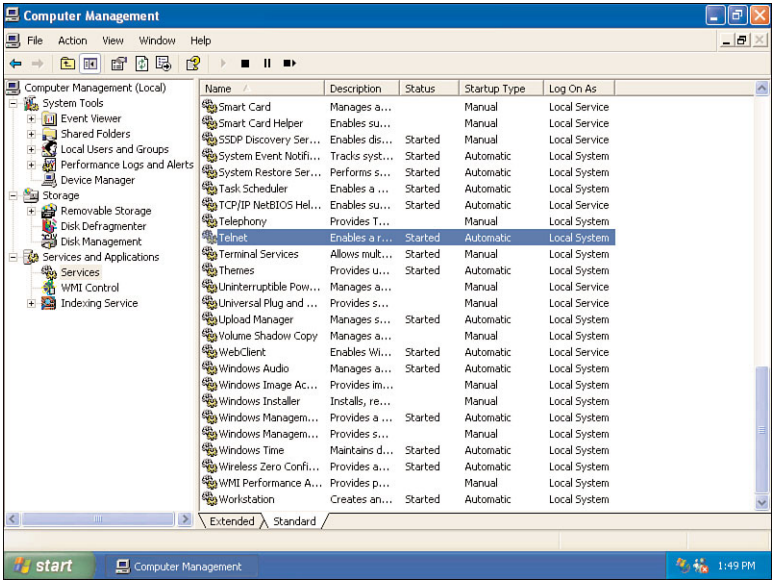

Figure 3-2 Services Window in Windows XP

The OS shown in the figure is Windows XP. 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-box security risk. But to make matter 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**, then click the **Stop** button, and change the Startup type drop-down menu to the **Disabled** option, as shown in Figure 3-3. 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 disabled in the Windows Command Prompt by using the **sc config** command, and can be started and stopped with the **net start** and **net stop** commands, respectively.

Key Topic

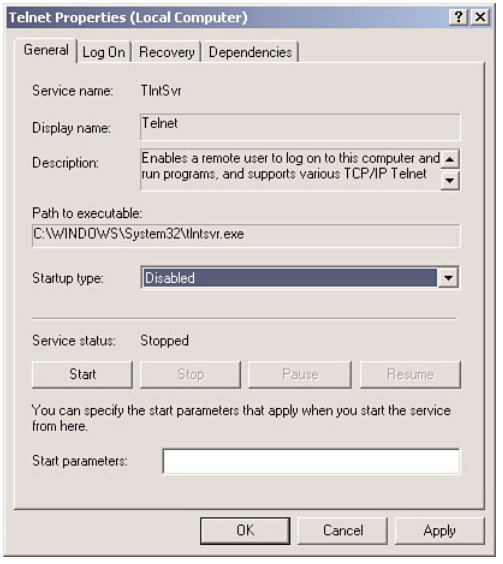

Figure 3-3 Telnet Properties Dialog Box

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

Key Topic

- By typing the following syntax:

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

  where <service> is the service name.

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

```
% sudo /sbin/service <service> stop
```

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 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 rewrites 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. For example, SP2 for Windows XP includes all the updates from SP1; a Windows XP installation with no SP installed can be updated directly to SP2 without having to install SP1 first. However, you will also see incremental SPs, for example, Windows XP SP3. A Windows XP installation with no SP *cannot* be updated directly to SP3; it needs to have SP1 or SP2 installed first before the SP3 update. Another example of an incremental SP is Windows Vista SP2; SP 1 must be installed before updating to SP2 in Windows Vista. This is becoming more common with Microsoft software. 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 Vista's System window is shown in Figure 3-4; it shows that SP2 is installed. An example of Windows XP's System Properties dialog box is shown in Figure 3-5; it has no SP installed (SP0). If an SP were installed, the SP number would be displayed under Version 2002; otherwise the area is left blank. Windows Server OSs work in the same fashion.

Key Topic

NOTE: 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!).

Key Topic

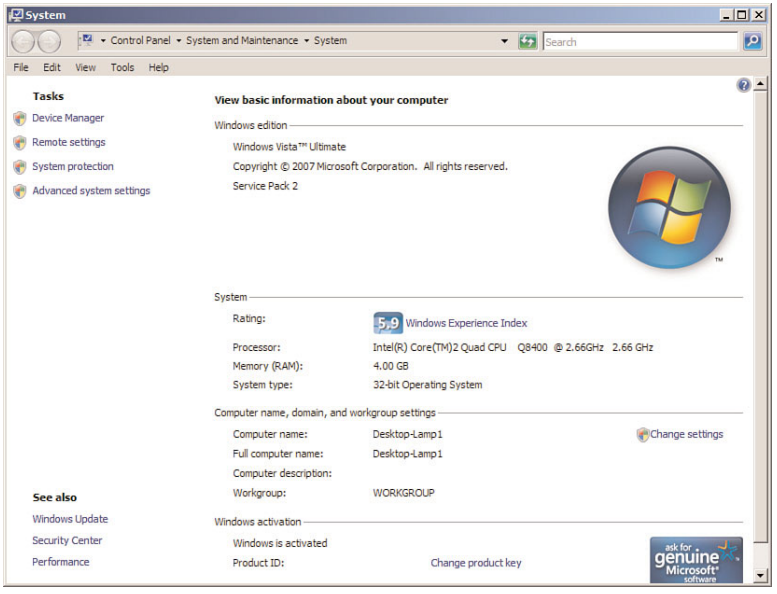

Figure 3-4 Windows Vista System Window

Key Topic

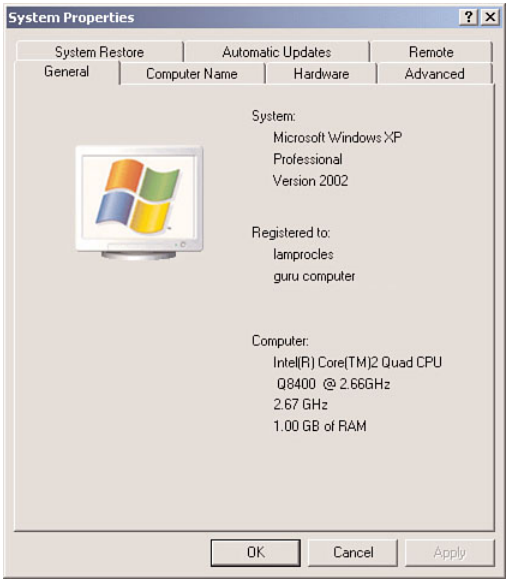

Figure 3-5 Windows XP System Properties Dialog Box

To find out what 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. An example of this in Outlook is shown in Figure 3-6. Office SPs affect all the applications within the Office suite.

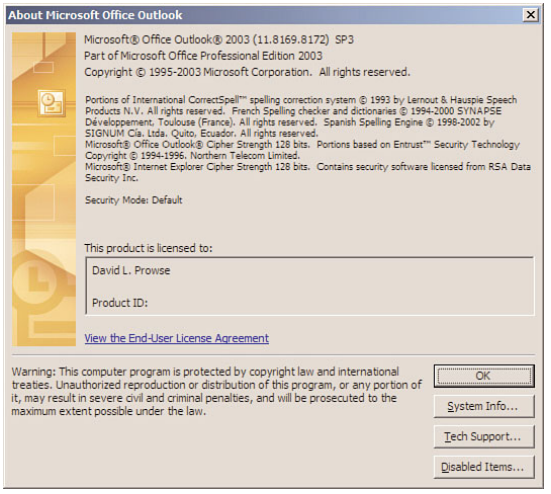

Figure 3-6 Office 2003 Outlook About Window

SPs can be acquired through Windows Update, at www.microsoft.com on CD/DVD and through a Microsoft Developer Network (MSDN) subscription. An SP might also have been incorporated into the original OS distribution DVD/CD. 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.

Table 3-1 defines the latest SPs as of August, 2010. You might see older OSs in the field. (If something works, why replace it, right?) For example, Windows NT and 2000 servers might be happily churning out the data necessary to users. That's okay; just make sure that they use the latest SP so that they can interact properly with other computers on the network. Keep in mind that this table is subject to change because new SPs can be released at any time. Note that other applications such as Microsoft Office, and server-based apps such as Microsoft Exchange Server, use SPs as well.

Key Topic

Table 3-1 Latest Windows SPs as of August 2010

Operating System	Service Pack
Windows 7	None as of the publishing of this book. (SP1 to be released the first half of 2011, according to Microsoft.)
Windows Vista	SP2
Windows XP	SP3
Windows Server 2008	None as of the publishing of this book. (SP1 to be released the first half of 2011, according to Microsoft.)

Table 3-1 Latest Windows SPs as of August 2010

Operating System	Service Pack
Windows Server 2003	SP2
Windows 2000 (Server and Professional)	SP4
Windows NT 4.0 (Server and Workstation)	SP6
Office 2007	SP2
Office 2003	SP3
Office 2000	SP3

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, service pack installations should be done offline. Disconnect the computer from the network by disabling the network adapter before initiating the SP upgrade. Again, because brand new OSs are inherently insecure to some extent (no matter what a manufacturer might say), organizations usually wait for the release of the first SP before implementing the OS on a live network. However, SPs are not the only type of updating you need to do to your computers. Microsoft OSs require further patching with the Windows Update program, and other applications require their own patches and hotfixes.

Windows Update, Patches, and Hotfixes

OSs 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 if any additional updates are available for download.

For example, if you want to install additional updates for Windows through Windows Update, you can do the following:

Step 1. Click **Start > All Programs > Windows Update**.

Step 2. Different OSs have different results at this point. For example, Windows Vista opens the Window Update window in which you can click the **Install Updates** button. Windows XP opens a web page in which you can select **Express** or **Custom** installation of updates. Follow the prompts to install the latest version of the Windows Update software if necessary.

NOTE: Do not select Express or let Microsoft automatically install all updates if you do not want to use newer applications, for example Internet Explorer 8 or XP SP3.

Step 3. The system (or web page) automatically scans for updates. Updates are divided into the following categories:

- **Critical updates and SPs—**These 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 system tray. 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, do the following in Windows Vista:

- Click **Start** > **All Programs** > **Windows Update**; then click the **Change Settings** link.

  It might require slightly different navigation in other OSs to access this.

From here, there will be four options (In other OSs, the options might be slightly different):

- **Install Updates Automatically—**This is the recommended option 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 download 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 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 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.

Another tool that can be used online is Microsoft Update, which is similar to Windows Update, but it can update for other Microsoft applications as well. It can be found at the following link: http://windowsupdate.microsoft.com/. For newer versions of Windows, this will simply open the Windows Update program on you local computer automatically.

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(s), 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

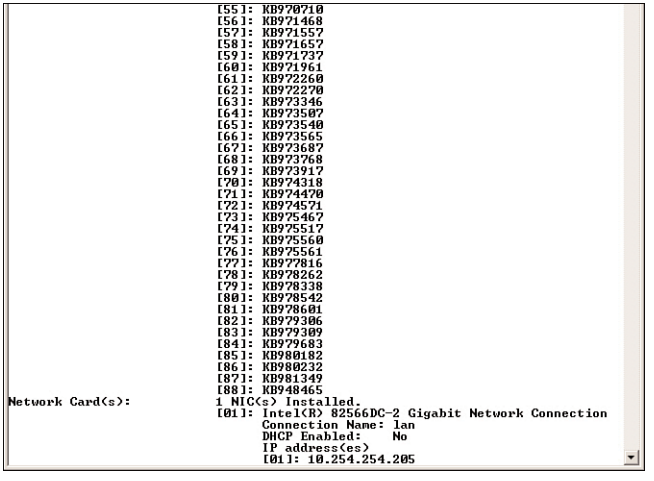

Figure 3-7 Systeminfo Command in Windows Vista

On the other side of the spectrum, World of Warcraft defines hotfixes 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 rewrites.) 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 we showed 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. If you look at my website (www.davidlprowse.com), note I am running a bulletin board system, also referred to as a forum or portal. If you scroll to the bottom, you will see that the bulletin board software is at least patch version 3.7.6. 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 if 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.

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:

Key Topic

- **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 if it will be 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 if 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 have to cover your tracks if a failure occurs!
- **Implementing—**If the test is successful, the patch should be deployed to all the necessary systems. In many cases this will be done in the evening or over the weekend for larger updates. Patches can be deployed automatically using software such as Microsoft's 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. SMS, and other third-party tools can be used in this endeavor.

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. 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; 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. *Group policies* are used in Microsoft 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. And 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 3-8 shows an example of this in Windows Vista.

Key Topic

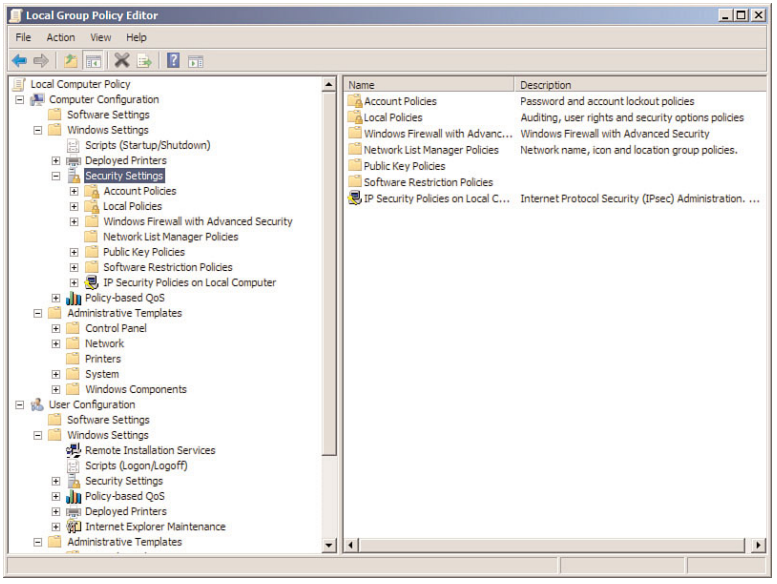

Figure 3-8 Local Group Policy Editor in Windows Vista

Although there are lots of 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 and only governs that particular machine and the local users of that machine. It is a basic version of the group policy used by Windows Server 2003 domain controllers that have Active Directory loaded.

It is also from here where 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. Figure 3-9 shows an example of this in Windows Server 2003. For example, securedc.inf file 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 hisecdc.inf is even more secure, perhaps too secure and limiting for some organizations. Generally, 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. Templates are generally stored in c:\Windows\Security\templates.

Key Topic

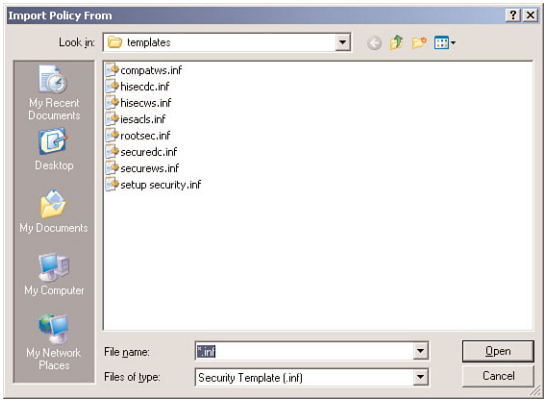

Figure 3-9 Import Policy From Window in Windows Server 2003

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 a lot of 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, 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. Baselining and benchmarking are extremely important when testing equipment and when monitoring already installed devices. We discuss this further in Chapter 11, "Monitoring and Auditing."

Hardening File Systems and Hard Drives

Last topic about hardening your system, I promise! Not! 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 for 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) that are a necessity in today's environment. Most systems today will 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.

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, 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 Windows Vista, 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 files such as ntldr, boot.ini, or bootmgr. You might also need to secure a system by turning off file sharing. For example, this can be done in Windows Vista 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:

- **Remove temporary files—**Temporary files and older files can clog up a hard disk and cause a decrease in performance and pose a security threat. It is rec-

ommended 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.

- **Defragment drives—**Drives also become defragmented over time. For a server, this could be 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 disks, to optical discs, or to tape. Microsoft domain controllers' Active Directory databases are particularly susceptible to attack; the System State for these OSs should be backed up, in the case that the server fails and the Active Directory needs to be recovered in the future.
- **Create restore points—**Restore points should also be created on a regular basis for servers and workstations. System Restore 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 or hardware is installed.
- **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. The hard drive that the OS inhabits can be completely wiped and re-installed 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.

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:

Key Topic

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—**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 Windows—**This includes the latest SPs and any Windows updates beyond that and setting Windows to alert if there are any new updates.

Step 4. **Update antimalware—**This includes making sure that there is a current license for the antimalware (antivirus and antispyware) 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 the 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 if 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 Complete PC Backups, or using third-party backup or drive imaging software.

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 virtualizations, their purposes, and define some of the various virtual applications.

Types of Virtualization and Their Purposes

Virtualization in the computing world is also referred to as v12n and may be referred to as other things depending on the virtual software vendor.

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)* that are created by this software run operating systems or individual applications. These virtual OSs are designed to run *inside* of a real OS. So the beauty behind this is that you can run multiple various OSs 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 OSs.

Virtual machines can be broken down into two categories:

- **System virtual machine—**A complete platform meant to take the place of an entire computer that enables you to run an entire OS virtually.
- **Process virtual machine—**Designed to run a single application, for example, if you ran 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. An example of a web-based emulator is D-Link's DIR-655 router emulator (we use this in Chapters 5–7), which you can find at the following link: http://support.dlink.com/emulators/dir655/133NA/login.html.

You might remember older emulators such as Basilisk, or the DOSBox, 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 8, "Physical Security and Authentication Models," and the virtual local area network (VLAN), which is covered in Chapter 5, "Network Design Elements and Threats."

Working with Virtual Machines

Several companies offer virtual software including Microsoft and VMware. Let's take a look at some of those programs now.

Microsoft Virtual PC

Microsoft's Virtual PC is commonly used to host workstation OSs, server OSs, and sometimes other OSs such as DOS or even Linux. There are 32-bit and 64-bit versions that can be downloaded for free and run on most Windows systems. The latest version is Virtual PC 2007 that can be downloaded from the following link: www.microsoft.com/downlOAds/details.aspx?familyid=04D26402-3199-48A3-AFA2-2DC0B40A73B6&displaylang=en.

After a quick installation, running the program displays the Virtual PC Console window, as shown in Figure 3-10.

Key Topic

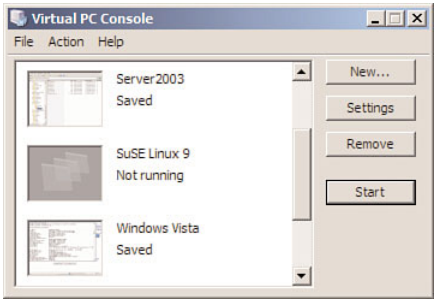

Figure 3-10 Virtual PC Console

After a fresh install of Virtual PC, there won't be any virtual machines listed. However, in Figure 3-10, you can note a Windows Server 2003 VM, a SuSE Linux 9 VM, and a Windows Vista VM. Personally, I run all kinds of platforms with Virtual PC, but it is not the only virtual software I use.

A virtual machine can be created by clicking the **New** button and following the directions. The virtual machine consists of two parts when you are done:

- Virtual machine configuration file or .vmc
- Virtual hard drive file or .vhd

In addition to this, you can save the state of the virtual machine. Let's say you needed to restart your main computer but don't want to restart the virtual machine. You could simply "save the state" of the VM that will save it, remember all the files that were open, and where you were last working, and close the VM. Even after rebooting the actual PC, you can immediately reload the last place you were working in a VM. When a VM's state is saved, an additional file called a .vsv file is stored adjacent to the .vhd. Figure 3-11 shows an example of a Windows Server 2003 virtual machine.

See Lab 2 in the Work Through Hands-On Scenarios at the end of this chapter for a quick tutorial/lab on using Virtual PC to create a virtual machine.

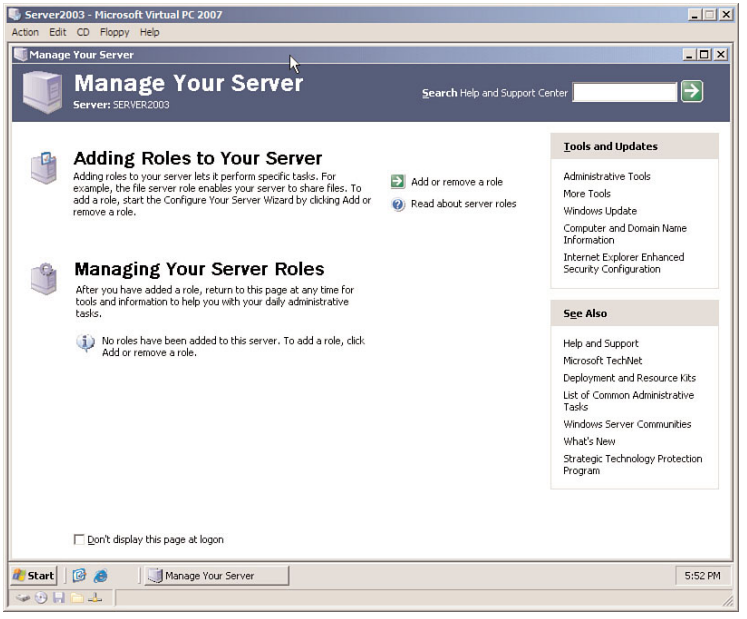

Figure 3-11 Windows Server 2003 Virtual Machine

NOTE: Also, if you are interested, I have demonstrations of several virtual machine OS installations on my website including the following:

Vista: www.davidlprowse.com/forums/showthread.php?t=1520

XP: www.davidlprowse.com/forums/showthread.php?t=1519

Server 2003: www.davidlprowse.com/forums/showthread.php?t=1515

Microsoft Windows XP Mode

Windows 7 can emulate the entire Windows XP OS if you so want. To do so, you must install Windows XP Mode, then Virtual PC, and then the Windows XP Mode update. This is done to help with program compatibility. These components can be downloaded for free (as long as you have a valid copy of Windows 7) from the following link: www.microsoft.com/windows/virtual-pc/download.aspx.

Microsoft Virtual Server

Virtual Server is similar to Virtual PC but is far more powerful and is meant for running server OSs in particular. It is not free like Virtual PC, and an install of Internet Information Services (IIS) is required prior to the install of Virtual Server to take full advantage of the program. When servers are created, they can be connected to by using the Virtual Machine Remote Control (VMRC) client, as shown in Figure 3-12.

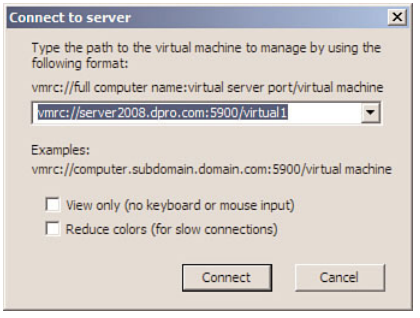

Figure 3-12 Virtual Machine Remote Client in Virtual Server 2005

VMware

VMware (part of EMC Corporation) runs on Windows, Linux, and Mac OSs. Some versions of VMware (for example VMware ESX Server) can run on server hardware without any underlying OS. These programs are extremely powerful, may require a lot of resources, and are generally web-based, meaning that you would control the virtual appliance through a browser.

Exam Preparation Tasks

Review Key Topics

Key Topic

Review the most important topics in the chapter, noted with the Key Topics icon in the outer margin of the page. Table 3-2 lists a reference of these key topics and the page numbers 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	60
Figure 3-3	Telnet Properties Dialog Box	61
Bullet list	Stopping services in Linux	61
Figures 3-4 and 3-5 and Note	Identifying the SP level	62–63
Table 3-1	Latest Windows Service Packs	64
Numbered list	Windows update	65
Figure 3-7	**systeminfo** Command in Windows Vista	67
Bulleted list	Patch management four steps	69
Figure 3-8	Local Group Policy Editor in Windows Vista	70
Figure 3-9	Import Policy from Window Windows Server 2003	71
Numbered list	Keeping a well-maintained computer	73
Figure 3-10	Virtual PC Console	76

Complete Tables and Lists from Memory

Print a copy of Appendix A, "Memory Tables," (found on the DVD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix B, "Memory Tables Answer Key," also on the DVD, includes completed tables and lists to check your work.

Define Key Terms

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

hardening, service pack (SP), hotfix, patch, patch management, group policy, security template, baselining, virtualization, virtual machine

Hands-On Labs

Complete the following written step-by-step scenarios. After you finish (or if you do not have adequate equipment to complete the scenario), watch the corresponding video solutions on the DVD.

If you have additional questions, feel free to post them at my website: www.davidlprowse.com in the Ask Dave forum. (Free registration is required to post on the website.)

Equipment Needed

- Computer with Internet access.
- Web browser: Internet Explorer version 6 and higher or Firefox are recommended.
- Virtual PC 2007: This can be downloaded at the following link: www.microsoft.com/downloads/details.aspx?FamilyID=04d26402-3199-48a3-afa2-2dc0b40a73b6&displaylang=en.

Lab 3-1: Discerning and Updating the Service Pack Level

In this lab, you observe the service pack currently used on a Windows Vista computer and show where to go to update the SP to the latest version. The steps are as follows:

Step 1. Access Windows Vista (other Windows OSs will be similar in appearance and in navigation).

Step 2. View the SP level:

A. Click **Start**.

B. Right-click **Computer** and select **Properties**. This brings up the System window. From here, you can see the SP level in the Windows edition section.

Step 3. Access Windows Update:

A. Click **Start**.

B. Click **All Programs**.

C. Click **Windows Update**.

Step 4. Modify Windows Update:

A. Click the **View Advanced Options** link.

B. Select the **Check for Updates but Let Me Choose Whether to Download Them or Install Them** radio button.

C. Click **OK**.

Step 5. Locate Windows Vista Service Pack 2 at support.microsoft.com.

You can find information about Windows Vista SP2 at the following link: http://support.microsoft.com/kb/948465.

Watch the solution video in the "Hands-On Scenarios" section of the DVD.

Lab 3-2: Creating a Virtual Machine in Virtual PC 2007

In this lab, you learn how to create a basic virtual machine (VM) in Virtual PC 2007. The steps are as follows:

Step 1. Download the Virtual PC 2007 application. It is a free download available at the following link: www.microsoft.com/downloads/details.aspx?FamilyID=04d26402-3199-48a3-afa2-2dc0b40a73b6&displaylang=en.

You can also search the phrase **virtual PC 2007 download**.

Step 2. Install Virtual PC 2007. Install the program with the default settings unless you want to modify them.

Step 3. Run Virtual PC 2007 by navigating to **Start > All Programs > Microsoft Virtual PC**. This displays the Virtual PC Console.

Step 4. Create a new virtual machine:

A. Click the **New** button.

B. Click **Next** for the wizard.

C. Select **Create a virtual machine** radio button and click **Next**.

D. Type a name for the virtual machine. Try to keep the name close to the name of the OS you plan to install. For example, if you install Windows Vista, type **Windows Vista**. Virtual PC can recognize these names. Keep in mind that you do not have to install an OS; this lab is simply to show how to create the virtual machine. This virtual machine will be available to you to use later on if you want, and you can load any OS into the VM that want.

E. Select where you want to save the virtual machine by clicking the **Browse** button, or simply leave the default. Then click **Next**.

F. Select the OS you want to install from the drop-down menu. If you are not planning on installing an OS, select **Other**. Then click **Next**.

G. Select the amount of RAM you would like the VM to use. You can increase the default by clicking the **Adjusting the RAM** radio button. As a rule of thumb it is recommended that you use no more than half of the physical RAM on your system for a single VM. Then click **Next**.

H. Select the **A New Virtual Hard Disk** radio button, and select where you want to save the virtual hard disk (.vhd file). Then click **Next**.

I. Review the summary and click **Finish**.
The new VM should now be listed in the Virtual PC Console.

Step 5. Run the VM:

A. Highlight the new VM.

B. Click **Start**.

Step 6. (Optional) Install an OS. Be sure to select **CD** from the menu bar and click **Use Physical Drive**. This way, the VM can use the physical CD-ROM drive.

Step 7. Save the VM:

A. Click **Action** on the menu bar.

B. Select **Close**.

C. From the drop-down menu in the Close dialog box, select **Save State** and click **OK**.

Step 8. Modify the VM settings:

A. Highlight the new VM.

B. Click the **Settings** button.

C. Click **OK** for the pop-up note.

D. Examine the various settings for each device within the VM. Note that you cannot make changes to some of the settings when the VM is in a saved state. To modify these, you need to turn off the VM either within Virtual PC or by shutting down the OS normally. Watch the solution video in the "Hands-On Scenarios" section of the DVD.

View Recommended Resources

For readers who want to brush up on their CompTIA A+ topics:

- Prowse, David L. *CompTIA A+ Exam Cram*, Fourth Edition. Que. 2010.

Virtualization software links:

- Microsoft Virtual PC: www.microsoft.com/downlOAds/details.aspx?familyid=04D26402-3199-48A3-AFA2-2DC0B40A73B6&displaylang=en
- Windows XP Mode: www.microsoft.com/windows/virtual-pc/download.aspx
- Virtual Server 2005: www.microsoft.com/windowsserversystem/virtualserver/
- VMware: www.vmware.com/

Answer Review Questions

Answer the following review questions. You can find the answers at the end of this chapter.

1. Virtualization technology is often implemented as operating systems and applications that run in software. Quite 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 Vista?
   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. In Windows XP and Windows Vista, what is the best file system to use?

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 Windows server 2003. 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 in order 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 pcAnywhere.

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

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 Vista.
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, and PHP scripts will generally not be used to harden an operating system.
6. **B.** NTFS is the most secure file system for use with Windows XP and Windows Vista. 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 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.
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.
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 to obtain averages of usage.
13. **C.** Quite 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 (NIDS) 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, pcAnywhere can actually make a computer less secure and should be installed only if the user requests it. PcAnywhere is just one of many examples of remote control software.
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.

Index

3-leg perimeter DMZ, 124
configuring, 165
3DES (triple DES), 357
10 tape rotation backup method, 419

A

AAA (authentication, authorization, accounting), 5–6
acceptable use policies, 449
access control
authentication. *See* authentication
best practices, 254–256
physical security, 215
biometric readers, 217–218
building security, 215
door access systems, 216–217
server room security, 215
policies, 264–267
UAC (User Account Control), 267–268
usernames/passwords, 261–264
users, groups, permissions, 256–261
access control lists (ACLs), 166, 258
for router security, 121
access control models, 250
DAC (discretionary access control), 250–252
MAC (mandatory access control), 252
RBAC (role-based access control), 253
Account lockout threshold, 266
accounting, 5
accounts
default accounts, 186–187
guest accounts, 187
restrictions, configuring, 270–272
user accounts
expiration, 256
time-of-day restrictions, 258
ACK, 318
ACLs (access control lists), 166, 258
for router security, 121
Active Directory Users and Computers (ADUC), 256
active fingerprinting, 288
active interception, 21
active security analysis, 288
ActiveX controls in Internet Explorer, 99
ad filtering, 37
add-ons
in Firefox, 103
in Internet Explorer, 99
addresses
IP addresses
public versus private, 121–122
subnetting, 126–127
network socket addresses, 134

administration interface for wireless access points, 195
administrative shares, 329
Administrator accounts, passwords for, 264
ADUC (Active Directory Users and Computers), 256
Advanced Encryption Standard (AES), 357–358
adware, 18
AES (Advanced Encryption Standard), 357–358
AH (authentication header), 388
air-conditioning systems, 439–440
ALE (annualized loss expectancy), 286
alerts, 318
ALG (application-level gateway), 164
algorithms
asymmetric key algorithms, 354
Diffie-Hellman key exchange, 360
ECC, 360–361
RSA, 359–360
defined, 352
hashes
LANMAN hash, 365–367
MD5, 364
NTLM 2 hash, 367
NTLM hash, 367
SHA, 364–365
one-time pads, 361
PGP, 362
public key cryptography, 354–355
symmetric key algorithms, 353-354, 359
AES, 357–358
DES and 3DES, 357
RC, 358–359
annualized loss expectancy (ALE), 286
annualized rate of occurrence (ARO), 286
anomaly-based monitoring, 315
anonymous access control, 254
anti-malware software, 6
antispyware software, 27–29
antivirus (AV) software, 23, 26–27
Application logs, 325
application security, 103–107. *See also* browser security
with group policies, 110–111
application-level gateway (ALG), 164
applications, removing, 58–62
archival methods, 420
armored viruses, 17
ARO (annualized rate of occurrence), 286
ARP poisoning, 144
ArpON, 144
assessing risk. *See* risk assessments
assessments. *See* audits
asymmetric key algorithms, 354
Diffie-Hellman key exchange, 360
ECC, 360–361
RSA, 359–360
attacks. *See also* vulnerabilities
ARP poisoning, 144
brute force attacks, 300
cryptanalysis attacks, 300
DDoS (Distributed Denial of Service), 140
dictionary attacks, 300
DNS poisoning, 143-144
DoS (Denial of Service), 137–140
network attacks, 145–148, 189
null sessions, 143

replay attacks, 142–143
session hijacking, 141–142
spoofing, 140–141
TCP reset attacks, 137
TCP/IP hijacking, 141
audit trails, 325
audits, 322
of files, 322–324, 335–337
log files for, 324–327
maintenance of, 327–328
in patch management, 69
steps in, 322
on system security settings, 328–331
authentication, 5–6, 213
localized technologies, 220
IEEE 802.1X standard, 221–224
Kerberos, 225–226
LDAP, 224
Terminal Services, 226
methods of, 214
models for, 219–220
remote technologies, 226
RADIUS versus TACACS, 230–232
RAS, 227–228
VPNs, 228–230
usernames/passwords, 261–264
authentication header (AH), 388
authentication servers (802.1X connections), 222
authenticators (802.1X connections), 222
authorization, 5, 213
automated monitoring, 314
AV (antivirus) software, 23, 26–27
availability, 5

B

Back Orifice, 17
back-to-back perimeter DMZ, 124
backdoors, 21, 106, 188
backup generators, 408–410
backup plans in disaster recovery, 416–420
backup sites, 416
backups of log files, 328. *See also* data backups
baiting, 444
Barracuda Networks Spam Firewall, 30
baselining, 71, 316–318
battery-inverter generators, 409
behavior-based monitoring, 315
Bell-La Padula access control, 252
best practices in access control, 254–256
Biba Integrity Model, 252
biometric readers, 217–218
BIOS, securing, 38–39, 44, 46
birthday attacks, 365
BitLocker, 40–41
black book analogy (cryptography), 350–352
black hats, 8
blacklists, 31
blackouts, 406
blind hijacking, 142
block ciphers, 354
blue hats, 8
Bluejacking, 42, 200
Bluesnarfing, 42, 200
Bluetooth vulnerabilities, 42, 199–200
boot sector viruses, 17, 27
botnets, 23, 140

bots, 18
Bro, 170
broadcast storms, 318
broadcasting, 118
brownouts, 406
browser security, 90–91
Firefox, 100–103
Internet Explorer, 96–100, 109–110
proxy servers and content filters, 94–95
security policies, implementing, 91–92
user education, 93–94
brute force attacks, 300
buffer overflows, 107
building loss (disaster recovery), 421
building security, 215
bulletin boards, policies for, 267
butt sets, 194

C

CA (certificate authorities), 381–384
cabling
STP (shielded twisted-pair) cables, 440
vulnerabilities, 189–195
crosstalk, 191–192
data emanation, 192
interference, 190–191
tapping into data, 192–195
caching proxy servers, 168
Cain & Abel password recovery tool, 299
CAM (Content Addressable Memory) table, 119
CAPTCHA, 267
carbon dioxide (CO2) extinguishers, 437
cardkey access systems, 216
castle analogy (network security), 161
CCI (co-channel interference), 191
cell phones, securing, 41–42
certificate authorities (CA), 381–384
certificate revocation list (CRL), 382–383
certificates, 355, 380–381
dual-sided certificates, 384
revoking, 383
single-sided certificates, 384
validation, 381
chain of custody, 456
challenge-handshake authentication protocol (CHAP), 227
change management policies, 449–450
CHAP (challenge-handshake authentication protocol), 227
cheat sheet for exam preparation, 472
Check Point Security Appliances, 172
checklist for exam preparation, 469–471
chromatic dispersion, 195
CIA triad, 4–5
cipher locks, 216
ciphers, defined, 352. *See also* algorithms
circuit-level gateway, 164
Clark-Wilson access control, 252
classification of data, policies concerning, 447–448
clean agent fire extinguishers, 437–438
clear-text passwords, 321
clearing data, 454
closing
pop-up windows, 94
ports, 136
clusters, 415
co-channel interference (CCI), 191

CO2 (carbon dioxide) extinguishers, 437
coaxial cables, 190
vampire taps on, 193
cold sites, 416
collisions in hashes, 364–365
combustible metal fires, extinguishing, 437
computer disposal policies, 452–454
computer forensics, 455
computer security audits. *See* audits
computer telephony integration (CTI), 129
confidence tricks, 443
confidentiality, 5
configuration baselines, 69–71
configuring
BIOS, 39
inbound filters, 176
L2TP-based VPNs with Windows Server 2003, 390–394
log files, 327
NAT firewalls, 175
password policies, 270–272
proxy server connections in Firefox, 102
RADIUS servers, 236–238
RAID, 425–426
security zones (Internet Explorer), 96
user and group permissions, 272
VPNs, 235–236
containment (incident response), 455
Content Addressable Memory table, 119
content filtering, 37, 169
browser security, 94–95
router security, 121
contracts with vendors, 452
converting NTFS to FAT32, 72
cookies
in Firefox, 101
in Internet Explorer, 97–98
stealing, 141
copying files/folders, permissions for, 260–261
cracking passwords, 304–305
CRL (certificate revocation list), 382–383
cross-site scripting (XSS), 98, 142
crosstalk, 191–192
cryptanalysis attacks, 300
cryptographic hash functions, 364–365
cryptography, 350–353. *See also* encryption
asymmetric key algorithms, 354
Diffie-Hellman key exchange, 360
ECC, 360–361
RSA, 359–360
black book analogy, 350–352
defined, 352
key management, 355
public key cryptography, 354–355
steganography, 356
symmetric key algorithms, 353–354, 359
AES, 357–358
DES and 3DES, 357
RC, 358–359
terminology, 352–353
CTI (computer telephony integration), 129
Ctrl+Alt+Del logon, 264

D

DAC (discretionary access control), 250–252
data, separating OS from, 25
data backups, 7, 73, 424–425
in disaster recovery, 416–420
data classification policies, 447–448
data emanation, 192
Data Encryption Standard (DES), 357
data failure, avoiding with RAID, 410–413
data removal, 7, 453–454
data security. *See* security
data sensitivity policies, 447–448
data validation, 107
DDoS (distributed denial of service) attacks, 23, 140
decryption, 351
default accounts, 186–187
default browser, setting, 100
Default Domain Policy, 265
defragmenting hard drives, 73
delivery methods for malware, 20–23
active interception, 21
backdoors, 21
botnets, 23
logic bombs, 22
privilege escalation, 21
removable media, 21
software, 21
zombies, 23
Demilitarized Zone (DMZ), 124
Denial of Service (DoS) attacks, 137–140
DES (Data Encryption Standard), 357
designing networks. *See* network design
destruction of computer equipment, 454
dial-up connections, RAS, 227–228
dictionary attacks, 300
differential backups, 417
Diffie-Hellman encryption, 355, 360
digital forensics, 455
Digital Signature Algorithm (DSA), 361
digital signatures, 355
Directory Service log, 326
dirty power, 407
disabling
file sharing, 72
Guest accounts, 264
LANMAN hash, 365, 369
services
in Linux, 61
in Mac OS X, 61
Telnet, 60
disaster recovery. *See also* environmental controls; redundancy planning
data backup, 416–420
incident response procedures, 454–457
planning, 420–422
types of disasters, 420–422
disaster-tolerant disk systems, 413
discretionary access control (DAC), 250–252
disposal of equipment, policies concerning, 452–454
distributed denial of service (DDoS) attacks, 23, 140
diversion theft, 441
DMZ (Demilitarized Zone), 124
DNS poisoning, 143–144
DNS Server log, 326

documentation
in incident response, 455
of network, 200, 292–295
domain name kiting, 144
door access systems, 216–217
DoS (Denial of Service) attacks, 137–140
double tagging, 129
Dragon IPS, 172
drills, fire, 439
drive lock technology, 38
dry pipe systems, 438
DSA (Digital Signature Algorithm), 361
dual-sided certificates, 384
due care, 450
due diligence, 450
due process, 450
dumpster diving, 443

E

e-mail addresses, removing from websites, 30
EAP (Extensible Authentication Protocol), 221–224
EAP-FAST authentication, 223
EAP-MD5 authentication, 223
EAP-TLS (Transport Layer Security) authentication, 223
EAP-TTLS (Tunneled Transport Layer Security) authentication, 223
Easter eggs, 22
eavesdropping, 192, 443
ECC (elliptic curve cryptography), 360–361
electrical fires, extinguishing, 436
electromagnetic interference (EMI), 190
shielding, 440–441
elite hackers, 8
elliptic curve cryptography (ECC), 360–361
email messages, S/MIME, 385–386
EMI (electromagnetic interference), 190
shielding, 440–441
employee security policies. *See* personnel security policies
emulators, 75
enabling
file auditing, 323
IEEE 802.1X standard, 234
MAC filtering, 177
packet filtering, 175
Encapsulating Security Payload (ESP), 388
encapsulation, 297
encryption, 7. *See also* cryptography; hashes
asymmetric key algorithms
Diffie-Hellman key exchange, 360
ECC, 360–361
RSA, 359–360
defined, 352
of log files, 328
one-time pads, 361
PGP, 362
PKI (public key infrastructure), 380, 390
certificate authorities (CA), 381–384
certificates, 380–381
dual-sided certificates, 384
single-sided certificates, 384
web of trust, 384

security protocols
IPsec, *388*
L2TP, *387–394*
PPTP, *387*
S/MIME, *385–386*
SSH, *386–387*
SSL/TLS, *386*
symmetric key algorithms, 359
AES, *357–358*
DES and 3DES, *357*
RC, *358–359*
website encryption notification, 94
whole disk encryption, 40–41, 73
on wireless access points, 196–197
Enterasys, 170
Enterasys Intrusion Prevention System, 172
environmental controls, 436
fire suppression, 436
fire extinguishers, *436–437*
hazard protection systems, *438–439*
sprinkler systems, *438*
HVAC, 439–440
shielding, 440–441
equipment disposal policies, 452–454
eradication (incident response), 455
ESP (Encapsulating Security Payload), 388
Ethereal. *See* Wireshark
events, incidents versus, 454
evidence gathering (incident response), 455
evidence preservation (incident response), 456
Evil Maid Attack, 19
exam preparation
cheat sheet, 472
checklist, 469–471
Security+ certification requirements, 469
tips for, 472–475
Excel, securing, 106
exhaust systems, 439
expiration of user accounts, 256
Extensible Authentication Protocol (EAP), 221–224
external security testing, 290
extranets, securing, 124–125

F

fail-over redundancy, 405
failopen mode, 119
failover clusters, 415
failure of power supplies, 406
failure-resistant disk systems, 413
failure-tolerant disk systems, 413
false negatives, 35, 172, 220
false positives, 35, 172, 220
far end crosstalk (FEXT), 191
Faraday cages, 192, 440
FAT32, converting to NTFS, 72
FEXT (far end crosstalk), 191
fiber-optic cables, 190
splitting, 194
File Replication Service log, 326
file sharing, disabling, 72
file systems, hardening, 71–73
files
auditing, 322–324, 335–337
moving/copying, permissions for, 260–261
FileZilla, 135
filters
ad filtering, 37
in browser security, 94–95
content filtering, 37

fingerprinting, 288
fire class A extinguishers, 436
fire class B extinguishers, 436
fire class C extinguishers, 436
fire class D extinguishers, 437
fire class K extinguishers, 437
fire drills, 439
fire extinguishers, 436–437
fire suppression, 436
fire extinguishers, 436–437
hazard protection systems, 438–439
sprinkler systems, 438
Firefox
Internet Explorer versus, 90–91
securing, 100–103
fires (disaster recovery), 420
firewall logs, 326–327
firewalls, 25, 162–167
configuring inbound filters, 176
enabling MAC filtering, 177
NAT firewalls, configuring, 175
personal firewalls, 33–34
for router security, 120
first responders, 455
flammable liquid/gas fires, extinguishing, 436
Flash scripts in Internet Explorer, 99
flashing the BIOS, 39
flood attacks, 137
floods (disaster recovery), 421
Fluke Networks, 298
folders, permissions for moving/copying, 260–261
fork bomb attacks, 139
Fraggle attacks, 138
FreeBSD, 252
FreeNAC, 126
FTP connections, ports and protocols for, 134
full backups, 417

G

gaseous fire suppression systems, 437–438
generators. *See* backup generators
Gnutella, 165
Gramm-Leach-Bliley Act, 447
grandfather-father-son backup rotation method, 419
gray hats, 8
grayware, 19
green hats, 8
group policies, 69–71
for application security, 110–111
groups
in access control, 256–261
permissions, configuring, 272
guessing passwords, 300
guest accounts, 187
disabling, 264

H

hackers, types of, 7–8
Halon extinguishers, 437
handheld devices, protocol analyzers, 298
handheld fire extinguishers, 436–437
hands-on labs
auditing files, 335–337
BIOS, securing, 44–46

configuring
inbound filters, *176*
L2TP-based VPNs with Windows Server 2003, *390–394*
NAT firewalls, *175*
password policies and user account restrictions, *270–272*
RADIUS servers, *236–238*
RAID, *425–426*
user and group permissions, *272*
VPNs, *235–236*
creating VMs (virtual machines) in Virtual PC 2007, 81–82
data backups, 424–425
disabling
applications with group policies, *110–111*
LANMAN hash, *369*
enabling
IEEE 802.1X, *234*
MAC filtering, *177*
packet filtering, *175*
network mapping, 303–304
password cracking, 304–305
PKI (public key infrastructure), 390
protocol analyzers, 333–335
scanning
for malware, *44*
ports, *150–151*
securing
Internet Explorer, *109–110*
wireless access points, *203–205*
SSH connections, 394–395
updating service packs, 80–81
wardriving, 205

hard drives
hardening, 71–73
sanitizing, 453–454

hardening operating systems, 58, 73–74
file systems and hard drives, 71–73
with group policies, security templates, configuration baselines, 69–71
installing
service packs, *62–65*
updates, *patches*, *hotfixes*, *65–69*
removing applications and services, 58–62

hashes, 362–364
cryptographic hash functions, 364–365
password hash functions, 365–367

hazard protection systems, 438–439

Health Insurance Portability and Accountability Act (HIPAA), 447

hidden files/folders, 72

hidden shares, 329

hiding protected system files, 72

HIDS (host-based intrusion detection systems), 33–36

high-availability clusters, 415

HIPAA (Health Insurance Portability and Accountability Act), 447

hoaxes, 442–443

honeyfarms, 170

honeynets, 169–170

honeypots, 169–170

horizontal privilege escalation, 188

host-based intrusion detection systems (HIDS), 33–36

hosts file attacks, 144

hot sites, 416

hotfixes, installing, 65–69

HTTP connections, ports and protocols for, 135

HTTP proxy servers, 168

HTTPS (Hypertext Transfer Protocol Secure), 386
hubs, securing, 118–119
humidity controls, 439
HVAC shielding, 440
HVAC systems, 439–440
Hypertext Transfer Protocol Secure (HTTPS), 386

I

ICMP flood attacks, 137
identification (incident response), 213, 455
identity proofing, 214
IDS (intrusion detection systems), 33–36
NIDS (network intrusion detection system), 170–171
IE. *See* Internet Explorer
IEEE 802.1Q standard, 128
IEEE 802.1X standard, 126, 198, 221–224
enabling, 234
impact assessment, 285
impersonation, 441
implementing in patch management, 69
implicit deny, 136, 254
inbound filters, configuring, 176
inbound ports, 133
incident response procedures, 454–457
incremental backups, 417
inheritance of permissions, 260
initialization in 802.1X authentication, 222
initiation in 802.1X authentication, 222
input validation, 107
installing
service packs, 24, 62–65
updates, patches, hotfixes, 24, 65–69
instant messaging programs, 58
integrity, 5
interconnections in network design, 123
DMZ (Demilitarized Zone), 124
Internet, 123
intranets/extranets, 124–125
LANs versus WANs, 123
interference, 190–191
shielding, 440–441
Internet
content filtering, 169
in network security, 123
Internet Explorer
Firefox versus, 90–91
securing, 96–100, 109–110
security policies, implementing, 91–92
security settings, 27
Internet Optimizer, 19
Internet Protocol Security (IPsec), 388
intranets, securing, 124–125
intrusion detection systems (IDS), 33–36
NIDS (network intrusion detection system), 170–171
intrusion prevention systems (IPS), 36
NIPS (network intrusion prevention system), 171–172
NIDS versus, 173
for router security, 121
investigation (incident response), 455
IP address spoofing, 141

IP addresses
public versus private, 121–122
subnetting, 126–127
IP masquerading, 121
IP proxy servers, 167
ipfirewall, 33
IPS (intrusion prevention systems), 36
NIPS (network intrusion prevention system), 171–172
NIDS versus, 173
for router security, 121
IPsec (Internet Protocol Security), 388
Ironkey, 40
ISO/IEC 27002 2005 standard, 447, 456
ISP (Internet service providers), redundancy planning, 414
IT security audits. *See* audits

J

job rotation, 256, 450

K

Kerberos, 225–226, 353
key algorithms. *See* algorithms
key escrow, 383
key management, 355
keys, defined, 352–353
kitchen fires, extinguishing, 437

L

L2TP (Layer 2 Tunneling Protocol), 229, 387–388
configuring VPN with Windows Server 2003, 390–394
label-based access control, 252
LAN Surveyor, 292
LANMAN hash, 365–367
disabling, 369
LANs (local area networks), WANs (wide area networks) versus, 123
lattice-based access control, 252
Layer 2 Tunneling Protocol (L2TP), 229, 387–388
configuring VPN with Windows Server 2003, 390–394
LDAP (Lightweight Directory Access Protocol), 224
LEAP (Lightweight EAP), 223
least privilege, 254, 260
legislative policies. *See* policies
Lightweight Directory Access Protocol (LDAP), 224
Lightweight EAP (LEAP), 223
line conditioners, 407
Linux, disabling services in, 61
load-balancing clusters, 415
local area networks (LANs), wide area networks (WANs) versus, 123
localized authentication technologies, 220
IEEE 802.1X standard, 221–224
Kerberos, 225–226
LDAP, 224
Terminal Services, 226
locking computers, 266
logic bombs, 22
logon process, locking computers, 266
logs
for audits, 324–327
maintenance of, 327–328
firewall logs, 165
security logs in file auditing, 323–324

long-term power loss (disaster recovery), 421
Love Bug virus, 16

M

MAC (mandatory access control), 252
MAC filtering, 167
enabling, 177
MAC flooding, 119
Mac OS X, disabling services in, 61
macro viruses, 17
maintenance release, 68
malicious attacks (disaster recovery), 421
malware, 6, 16, 20
delivery methods for, 20–23
active interception, 21
backdoors, 21
botnets, 23
logic bombs, 22
privilege escalation, 21
removable media, 21
software, 21
zombies, 23
preventing and troubleshooting, 23, 32
rootkits, 29–30
spam, 30–31
spyware, 27–29
viruses, 23–27
worms and Trojan horses, 27
rootkits, 19
scanning for, 44
spam, 19
spyware, 18
Trojan horses, 17
viruses, 16–17
worms, 17
man-in-the-middle attacks, 140–142
mandatory access control (MAC), 252
mandatory vacation policies, 450
mantraps, 217
manual monitoring, 314
many-to-one mapping, 382
mapping the network, 292–295, 303–304
McAfee IntruShield, 172
MD5 (Message-Digest algorithm 5), 364
message authentication code, 354
message digests, 363
Message-Digest algorithm 5 (MD5), 364
metal fires, extinguishing, 437
Microsoft Update, 67
Microsoft Virtual PC, 76–77
Microsoft Virtual Server, 78
Microsoft Windows XP Mode, 78
mining log files, 327
MITM attacks. *See* man-in-the-middle attacks
modems, securing, 130
monitoring
incident response, 455
in intrusion detection systems (IDS), 35
methodologies, 314
anomaly-based monitoring, 315
behavior-based monitoring, 315
signature-based monitoring, 314
tools
performance baselining, 316–318
protocol analyzers, 318-321

moving files/folders, permissions for, 260–261
MS-CHAP, 227
multifactor authentication, 219
multihomed connections, 167
multipartite viruses, 17
mutual authentication, 225–226

N

NAC (Network Access Control), 125–126
NAS (network attached storage), securing, 40
NAT (network address translation), 121–122
NAT filtering, 164
NAT firewalls, configuring, 175
near end crosstalk (NEXT), 191
negotiation in 802.1X authentication, 223
Nessus, 295
NetBus, 17
netmon. *See* Network Monitor
netstat command, 297
Network Access Control (NAC), 125–126
network address translation (NAT), 121–122
network attached storage (NAS), securing, 40
network connections, redundancy planning, 413–415
network design, 118
interconnections, 123
DMZ (Demilitarized Zone), 124
Internet, 123
intranets/extranets, 124–125
LANs versus WANs, 123
NAC (Network Access Control), 125–126
NAT (network address translation), 121–122
network devices, 118
hubs, 118–119
routers, 120–121
switches, 119–120
subnetting, 126–127
telephony devices, 129–131
modems, 130
PBX equipment, 130
VoIP, 131
VLAN (virtual local area network), 128–129
network devices, 118
hubs, 118–119
routers, 120–121
switches, 119–120
vulnerabilities, 186–189
backdoors, 188
default accounts, 186–187
network attacks, 189
privilege escalation, 188
weak passwords, 187
network intrusion detection system (NIDS), 35, 170–171
network intrusion prevention system (NIPS), 171–172
NIDS versus, 173
Network Magic, 292
network management system (NMS), 321
network mapping, 292–295, 303–304
network masquerading, 121
Network Monitor, 320–321

network monitoring methodologies, 314
anomaly-based monitoring, 315
behavior-based monitoring, 315
signature-based monitoring, 314
network monitoring tools
performance baselining, 316–318
protocol analyzers, 318
Network Monitor, 320–321
SNMP, 321
Wireshark, 319–320
network perimeter, 161
network security
ARP poisoning, 144
attacks, list of, 145–148
castle analogy, 161
DDoS (Distributed Denial of Service) attacks, 140
DNS poisoning, 143–144
DoS (Denial of Service) attacks, 137–140
firewalls, 162–167
honeypots and honeynets, 169–170
network design. *See* network design
network documentation, 200
NIDS (network intrusion detection system), 35, 170–171
NIPS (network intrusion prevention system), 171–172
NIDS versus, 173
null sessions, 143
ports and protocols, 131–136
protocol analyzers, 173
proxy servers, 167–169
replay attacks, 142–143
session hijacking, 141–142
spoofing attacks, 140–141
wired networks, 186
cable vulnerabilities, 189–195
device vulnerabilities, 186–189
wireless access points, securing, 203–205
wireless networks, 195
Bluetooth vulnerabilities, 199–200
wireless access point vulnerabilities, 195–199
wireless transmission vulnerabilities, 199
network sniffers. *See* protocol analyzers
network socket addresses, 134
network-based firewalls. *See* firewalls
NEXT (near end crosstalk), 191
NIDS (network intrusion detection system), 35, 170–171
Nimda worm, 17
NIPS (network intrusion prevention system), 171–172
NIDS versus, 173
NIST penetration testing, 290
Nmap, 136, 163, 295
NMS (network management system), 321
nonce, 142
nonpromiscuous mode, 318
nonrepudiation, 6, 323
NoScript, 103
NTFS
converting FAT32 to, 72
permissions, 259
NTLM 2 hash, 367
NTLM hash, 367
null sessions, 143

O

one-time pads, 361
one-to-one mapping, 121, 382
one-way functions, 363
open mail relays, 30
open ports on twisted-pair cables, 194
Open Source Security Testing Methodology Manual (OSSTMM), 290
Open Vulnerability and Assessment Language (OVAL), 290
operating systems
hardening, 58, 73–74
file systems and hard drives, 71–73
with group policies, security templates, configuration baselines, 69–71
installing service packs, 62–65
installing updates, patches, hotfixes, 65–69
removing applications and services, 58–62
separating from data, 25
optical splitters, 194
***The Orange Book*, 250**
organizational policies. *See* policies
OS. *See* operating systems
OSI Model, 120
Osiris, 36
OSSTMM (Open Source Security Testing Methodology Manual), 290
outbound ports, 133
Outlook, securing, 106
OVAL (Open Vulnerability and Assessment Language), 290

P

packet filtering, 164
enabling, 175
packet sniffers. *See* protocol analyzers
PacketFence, 126
padding schemes in RSA encryption, 360
PAP, 227
passive fingerprinting, 288
passive security analysis, 288
password analysis, 298–301, 304–305
password crackers, 299
password hash functions, 365–367
passwords
in access control, 261–264
BIOS passwords, 38
clear-text passwords, 321
frequency of changes, 263
guessing, 300
policies for, 264–266
configuring, 270–272
storing in web browsers, 102
strong passwords, 262–263
weak versus strong passwords, 187
PAT (port address translation), 121
patch management, 68–69
patch version, 68
patches, installing, 24, 65–69
PBX (private branch exchange) equipment, securing, 130
PDAs, securing, 41–42
PDoS (permanent DoS) attacks, 139
PEAP (protected extensible authentication protocol) authentication, 223

penetration testing, 290
performance baselining, 316–318
Performance Monitor, 316–317
permanent DoS (PDoS) attacks, 139
permanently installed generators, 409
permissions, 256–261
auditing, 329
inheritance and propagation, 260
moving/copying files and folders, 260–261
types of, 258
user and group permissions, configuring, 272
personal firewalls, 33–34
personally identifiable information (PII), 451
personnel security policies, 448–452
acceptable use, 449
change management, 449–450
due care, 450
due diligence, 450
due process, 450
mandatory vacation, 450
separation of duties, 450
training employees, 451
types of, 451
PGP (Pretty Good Privacy), 362
Phage virus, 25
phishing, 140, 442
Phlashing, 139
physical security, 215
biometric readers, 217–218
building security, 215
door access systems, 216–217
server room security, 215
of switches, 120
piggybacking, 444
PII (personally identifiable information), 451
ping flood attacks, 137
ping of death (POD) attacks, 139
PKI (Public Key Infrastructure), 355, 380, 390
certificate authorities (CA), 381–384
certificates, 380–381
dual-sided certificates, 384
single-sided certificates, 384
web of trust, 384
planning
for disaster recovery, 420–422
in patch management, 69
PNAC (port-based Network Access Control), 126
POD (ping of death) attacks, 139
point release, 68
Point-to-Point Tunneling Protocol (PPTP), 229, 387
policies. ***See also*** **procedures**
for access control, 264–267
for application security, 104-105, 110–111
auditing, 331
for browsers, implementing, 91–92
configuring, 270–272
data sensitivity and classification, 447–448
in disaster recovery plans, 422
equipment disposal, 452–454
example of, 446
group policies, 69–71
personnel security policies, 448–452
acceptable use, 449
change management, 449–450
due care, 450
due diligence, 450

due process, *450*
mandatory vacations, *450*
separation of duties, *450*
training employees, *451*
types of, *451*
vendor contracts, 452
polymorphic viruses, 17
pop-up blockers, 33, 36–37
in Firefox, 103
in Internet Explorer, 98
pop-up windows, closing, 94
POP3 connections, ports and protocols for, 135
port address translation (PAT), 121
port forwarding, 163
port scanning, 136, 295-297
port zero, securing, 136
port-based Network Access Control (PNAC), 126
portable gas-engine generators, 409
ports
closing, 136
inbound, 133
outbound, 133
protocol associations, list of, 133–134
ranges of, 131
scanning, 150–151
securing, 131–136
power supplies
failure of, 406
redundancy planning, 405–410
backup generators, *408–410*
redundant power supplies, *406–407*
UPS, *407–408*
PPTP (Point-to-Point Tunneling Protocol), 229, 387
pre-action sprinkler systems, 438
precomputation, 300
preparing for exam. *See* exam preparation
preservation of evidence (incident response), 456
pretexting, 441
Pretty Good Privacy (PGP), 362
preventing
BIOS attacks, 38–39
malware, 23, 32
rootkits, *29–30*
spam, *30–31*
spyware, *27–29*
viruses, *23–25*, *27*
worms and Trojan horses, *27*
previous logon notification, 266
Privacy Act of 1974, 447
private addresses, public addresses versus, 121–122
private branch exchange (PBX) equipment, securing, 130
private keys, 353. *See also* symmetric key algorithms
privilege de-escalation, 188
privilege escalation, 21, 188
procedures, incident response, 454–457. *See also* policies
process virtual machines, 75
program viruses, 17
programs. *See* applications
promiscuous mode, 171, 318
propagation of permissions, 260
protected system files, hiding, 72
protocol analyzers, 118, 173, 297–298, 318, 333–335
Network Monitor, 320–321
SNMP, 321
Wireshark, 319–320

protocols
port associations, list of, 133–134
securing, 131–136
proximity sensors, 217
proximity-based door access systems, 217
proxy servers, 167–169
in browser security, 94–95
configuring connections in Firefox, 102
public addresses, private addresses versus, 121–122
public key cryptography, 354–355
Public Key Infrastructure (PKI), 355, 380, 390
certificate authorities (CA), 381–384
certificates, 380–381
dual-sided certificates, 384
single-sided certificates, 384
web of trust, 384
public keys, 353
punch block connections, 194
Pure-FTPd, 135
purging data, 454

Q

qualitative risk assessments, 285–286
quantitative risk assessments, 286–287

R

RA (registration authority), 383
radio frequency interference (RFI), 191
RADIUS (Remote Authentication Dial-In User Service), 230–232
RADIUS servers, configuring, 236–238
RAID (redundant array of independent disks), 410–413
configuring, 425–426
Rainbow Tables, 300
RAS (Remote Access Service), 227–228
RATs (remote access Trojans), 17
raw socket programming, 137
RBAC (role-based access control), 253
RC (Rivest Cipher), 358–359
RC4, 358
RC5, 358
RC6, 358
recovery (incident response), 455. *See also* disaster recovery
recycling computers, policies concerning, 452–454
***The Red Book*, 250**
redundancy planning, 404–405. *See also* disaster recovery
network connections, 413–415
power supplies, 405–410
backup generators, 408–410
redundant power supplies, 406–407
UPS, 407–408
RAID, 410–413
servers, 415
single points of failure, 404
sites, 415–416
redundant array of independent disks (RAID), 410–413
configuring, 425–426
redundant ISP, 414
redundant power supplies, 406–407
registration authority (RA), 383
Remote Access Service (RAS), 227–228

remote access Trojans (RATs), 17
Remote Authentication Dial-In User Service (RADIUS), 230, 232
remote authentication technologies, 226
RADIUS versus TACACS, 230–232
RAS, 227–228
VPNs, 228–230
remote ports, 189
removable media
as malware delivery method, 21
securing, 39–40
removing. *See also* data removal
applications and services, 58–62
e-mail addresses from websites, 30
temporary files, 72, 99
web browsers, 99
replay attacks, 142–143
requirements for Security+ certification, 469
residual risk, 284
restoration from backup tapes, 418
restore points, 73
restrictions on user accounts, configuring, 270–272
revoking certificates, 383
RFI (radio frequency interference), 191
risk assessments, 284–285
qualitative risk assessments, 285–286
quantitative risk assessments, 286–287
security analysis methodologies, 287–288
vulnerability management, 288–291
risk management, 284
risk mitigation, 285
risks, residual, 284
Rivest Cipher (RC), 358–359
rogue wireless access points, 196
role-based access control (RBAC), 253
rootkits, 19
preventing and troubleshooting, 29–30
rotation schemes for backups, 418–419
routers, securing, 120–121
RSA (Rivest, Shamir, Adleman) encryption, 359–360
rule-based access control, 252

S

S/MIME (Security/Multipurpose Internet Mail Extensions), 385–386
SA (security association), 388
safety. *See* environmental controls
sags, 406
salting, 300
sandboxes, 107
sanitizing hard drives, 453–454
Sarbanes-Oxley Act (SOX), 447
saving log files, 327
SCA (side channel attacks), 361
scanning
for malware, 44
the network, 303–304
ports, 136, 150–151
for vulnerabilities, 295–297
secret key encryption, 352. *See also* symmetric key algorithms
Secure Hash Algorithm (SHA), 364–365
Secure HTTP (SHTTP), 386
Secure LDAP, 224
Secure Shell (SSH), 386–387
Secure Sockets Layer (SSL), 386
Secure/Multipurpose Internet Mail Extensions (S/MIME), 385–386

security
AAA, 5–6
access control. *See* access control models
application security, 103–107
with group policies, *110–111*
authentication models, 219–220
of BIOS, 38–39, 44, 46
browser security, 90–91
Firefox, *100–103*
Internet Explorer, *96–100*, *109–110*
proxy servers and content filters, *94–95*
security policies, *implementing*, *91–92*
user education, *93–94*
of cell phones and PDAs, 41–42
CIA triad, 4–5
of log files, 328
network design, 118
interconnections, *123–125*
NAC (Network Access Control), *125–126*
NAT (network address translation), *121–122*
network devices, *118–121*
subnetting, *126–127*
telephony devices, *129–131*
VLAN (virtual local area network), *128–129*
network security
ARP poisoning, *144*
attacks, *list of*, *145–148*
castle analogy, *161*
DDoS (Distributed Denial of Service) attacks, *140*
DNS poisoning, *143–144*
DoS (Denial of Service) attacks, *137–140*
firewalls, *162–167*
honeypots and honeynets, *169–170*
network documentation, *200*
NIDS (network intrusion detection system), *170–171*
NIPS (network intrusion prevention system), *171–173*
null sessions, *143*
ports and protocols, *131–136*
protocol analyzers, *173*
proxy servers, *167–169*
replay attacks, *142–143*
session hijacking, *141–142*
spoofing attacks, *140–141*
physical security, 215
biometric readers, *217–218*
building security, *215*
door access systems, *216–217*
server room security, *215*
risk assessments, 284–285
qualitative risk assessments, *285–286*
quantitative risk assessments, *286–287*
security analysis methodologies, *287–288*
vulnerability management, *288–291*
of storage devices
network attached storage (NAS), *40*
removable media, *39–40*
whole disk encryption, *40–41*
technologies
intrusion detection systems (IDS), *34–36*
personal firewalls, *33–34*
pop-up blockers, *36–37*
types of, *6–7*
threats
malware, *16–32*
types of, *6*

wired network security, 186
cable vulnerabilities, 189–195
device vulnerabilities, 186–189
wireless network security, 195
Bluetooth vulnerabilities, 199–200
wireless access point vulnerabilities, 195–199
wireless transmission vulnerabilities, 199
security analysis methodologies, 287–288
security association (SA), 388
security audits. *See* audits
security logs, 324–325
in file auditing, 323–324
security permissions, 259
security policies. *See* policies
security protocols
IPsec, 388
L2TP, 387–388
configuring VPN with Windows Server 2003, 390–394
PPTP, 387
S/MIME, 385–386
SSH, 386–387
SSL/TLS, 386
security settings (Internet Explorer), 27
security templates, 69–71
security tokens, 217
security tools. *See* technologies
security zones (Internet Explorer), configuring, 96
Security+ certification requirements, 469
sensitivity of data, policies concerning, 447–448
Separation of Duties (SoD), 255, 450
separation of OS and data, 25
server room security, 215
servers, redundancy planning, 415
service level agreement (SLA), 452
service packs
installing, 24, 62–65
services versus, 61
updating, 80–81
Service Set Identifier (SSID) broadcasting, 167, 196
services
removing, 58–62
service packs versus, 61
session cookies, 98
session hijacking, 141–142
Session Initiation Protocol (SIP), 131
session theft, 141
session-key. *See* symmetric key algorithms
SHA (Secure Hash Algorithm), 364–365
shared folders, auditing, 329
shared-key. *See* symmetric key algorithms
sharing permissions, 258
shielded twisted pair (STP) cables, 192, 440
shielding, 440–441
ShieldsUP!, 136, 163
shoulder surfing, 443
SHTTP (Secure HTTP), 386
side channel attacks (SCA), 361
signal emanation, 192
signature-based monitoring, 35, 314
Simple Network Management Protocol (SNMP), 321
single loss expectancy (SLE), 286
single points of failure, 404

Single Sign-on (SSO), 219
single-key. *See* symmetric key algorithms
single-sided certificates, 384
SIP (Session Initiation Protocol), 131
sites, redundancy planning, 415–416
SLA (service level agreement), 452
SLE (single loss expectancy), 286
slipstreaming, 64
smart cards, 217
SMTP open relays, 30
SMTP relay, 143
Smurf attacks, 137
SNMP (Simple Network Management Protocol), 321
SNMP agents, 321
Snort, 170, 172
social engineering, 6, 441
baiting, 444
diversion theft, 441
dumpster diving, 443
eavesdropping, 443
hoaxes, 442–443
phishing, 442
piggybacking, 444
pretexting, 441
shoulder surfing, 443
training employees against, 445
types of, 444–445
SoD (Separation of Duties), 255
software, as malware delivery method, 21
software versions, explained, 68
SOX (Sarbanes-Oxley) Act, 447
SP. *See* service packs
spam, 19
preventing and troubleshooting, 30–31
spam filters, 30
spam honeypots, 170
SPAP, 227
spectral analyzers, 194
SPI (stateful packet inspection), 164
spikes, 406
splitting
fiber-optic cables, 194
twisted-pair cable wires, 194
spoofing attacks, 140–141
sprinkler systems, 438
spyware, 18
preventing and troubleshooting, 27–29
symptoms of, 28
SSH (Secure Shell), 386–387
SSH connections, 394–395
SSID (Service Set Identifier) broadcasting, 167, 196
SSL (Secure Sockets Layer), 386
certificates, 382
settings in Internet Explorer, 99
SSO (Single Sign-on), 219
standard load, 316
standby generators, 409
stateful packet inspection (SPI), 164
stateless packet inspection, 164
static NAT (network address translation), 121
statistical anomaly monitoring, 35, 315
stealth viruses, 17
steganography, 356
storage devices
network attached storage (NAS), securing, 40
removable media, securing, 39–40
whole disk encryption, 40–41
STP (shielded twisted pair) cables, 192, 440

stream ciphers, 354
strong passwords, 187, 262–263
subnetting, 126–127
SubSeven, 18
subversion errors, 172
supplicants (802.1X connections), 222
surges, 406
switch spoofing, 129
switches, securing, 119–120
symmetric key algorithms, 353–354, 359
AES, 357–358
DES and 3DES, 357
RC, 358–359
symptoms
of spyware, 28
of viruses, 26
SYN, 318
SYN flood attacks, 138
system failure, 6
System logs, 325
System Monitor, 318
System Restore, 73
system security settings, audits on, 328–331
system virtual machines, 75

T

TACACS (Terminal Access Controller Access-Control System), 231
TACACS+, 231
tape backups, types of, 417
tapping into data, 192–195
TCP reset attacks, 137
TCP/IP hijacking, 141
TDEA (Triple Data Encryption Algorithm), 357
teardrop attacks, 139
technologies
intrusion detection systems (IDS), 34–36
localized authentication technologies, 220
IEEE 802.1X standard, 221–224
Kerberos, 225–226
LDAP, 224
Terminal Services, 226
monitoring tools
performance baselining, 316–318
protocol analyzers, 318–321
personal firewalls, 33–34
pop-up blockers, 36–37
remote authentication technologies, 226
RADIUS versus TACACS, 230–232
RAS, 227–228
VPNs, 228–230
types of, 6–7
for vulnerability assessments, 291
network mapping, 292–295
password analysis, 298–301
protocol analyzers, 297–298
vulnerability scanning, 295–297
telephony devices, securing, 129–131
modems, 130
PBX equipment, 130
VoIP, 131
Telnet, 130, 189
disabling, 60
TEMPEST standards, 192, 440
templates, 69–71
temporary files, removing, 72, 99

Terminal Access Controller Access-Control System (TACACS), 231
Terminal Services, 226
test systems, importance of, 18
testing in patch management, 69
theft (disaster recovery), 421
threats
malware, 16, 20
delivery methods for, 20–23
preventing and troubleshooting, 23–32
rootkits, 19
spam, 19
spyware, 18
Trojan horses, 17
viruses, 16–17
worms, 17
types of, 6
tickets (Kerberos), 225
time bombs, 22
time-of-day restrictions on user accounts, 258
TLS (Transport Layer Security), 386
tools. *See* technologies
Towers of Hanoi backup rotation method, 419
training employees
against social engineering, 445
on policies, 451
Transport Layer Security (TLS), 386
Trend Micro OSSEC, 36
Triple Data Encryption Algorithm (TDEA), 357
Trojan horses, 17
preventing and troubleshooting, 27
troubleshooting malware, 23, 32
rootkits, 29–30
spam, 30–31
spyware, 27–29
viruses, 23–27
worms and Trojan horses, 27
true negatives, 220
true positives, 220
TrueCrypt, 40
tunneling protocols (VPNs), 228
twisted-pair cables, 190–191
open ports on, 194
splitting wires of, 194
Type I errors, 220
Type II errors, 220

U

UAC (User Account Control), 104, 267–268
UDP flood attacks, 138
unauthorized access, 6
unicast, 119
uninterruptible power supplies (UPS), 407–408
unshielded twisted pair (UTP) cables, 192
updates, installing, 24, 65–69
updating
BIOS, 39
service packs, 80–81
UPS (uninterruptible power supplies), 407–408
URL spoofing attacks, 140
USB devices, securing, 39
User Account Control (UAC), 104, 267–268
user accounts
expiration, 256
time-of-day restrictions, 258
user awareness, 6

user education
in browser security, 93–94
to prevent viruses, 25
spam prevention, 31
spyware prevention, 28
usernames in access control, 261–264
users
in access control, 256–261
account restrictions, configuring, 270–272
permissions, configuring, 272
UTP (unshielded twisted pair) cables, 192

V

v12n. *See* virtualization
validation
of certificates, 381
of input, 107
vampire taps, 193
vendor contracts, 452
Verisys, 36
versions of patches, explained, 68
vertical privilege escalation, 188
virtual appliances, 75
virtual local area network (VLAN), 128–129
virtual machines (VMs), 74–75
creating in Virtual PC 2007, 81–82
Microsoft Virtual PC, 76–77
Microsoft Virtual Server, 78
Microsoft Windows XP Mode, 78
VMware, 78
Virtual PC, 76–77
Virtual PC 2007, creating VMs (virtual machines) in, 81–82
virtual private networks (VPNs), 228–230
configuring, 235–236
IPsec, 388
L2TP, 387–388
configuring with Windows Server 2003, 390–394
PPTP, 387
for router security, 121
Virtual Server, 78
virtual servers, 163
virtualization, 74
Microsoft Virtual PC, 76–77
Microsoft Virtual Server, 78
Microsoft Windows XP Mode, 78
types of, 74–76
VMware, 78
viruses, 16–17
preventing and troubleshooting, 23–27
symptoms of, 26
VLAN (virtual local area network), 128–129
VLAN hopping, 129
VMs (virtual machines), 74–75
creating in Virtual PC 2007, 81–82
Microsoft Virtual PC, 76–77
Microsoft Virtual Server, 78
Microsoft Windows XP Mode, 78
VMware, 78
VMware, 78
VoIP (voice over Internet Protocol), securing, 131
VPNs (virtual private networks), 228–230
configuring, 235–236
IPsec, 388

L2TP, 387–388
configuring with Windows Server 2003, *390–394*
PPTP, 387
for router security, 121
vulnerabilities, 283. *See also* attacks
of Bluetooth, 199–200
of cabling, 189–195
crosstalk, *191–192*
data emanation, *192*
interference, *190–191*
tapping into data, *192–195*
of network devices, 186–189
backdoors, *188*
default accounts, *186–187*
network attacks, *189*
privilege escalation, *188*
weak passwords, *187*
of wireless access points, 195–199
of wireless transmission, 199
vulnerability assessments, tools for, 291
network mapping, 292–295
password analysis, 298–301
protocol analyzers, 297–298
vulnerability scanning, 295–297
vulnerability management, 288–291
vulnerability scanning, 295–297

W

WANs (wide area networks), LANs (local area networks) versus, 123
wardialing, 130
wardriving, 199, 205
warm sites, 416
weak encryption on wireless access points, 196–197
weak passwords, 187
guessing, 300
web browser security. *See* browser security
web of trust, 384
web proxy servers, 168
websites
encryption notification, 94
pop-up blocking, 36–37
pop-up windows, closing, 94
removing e-mail addresses from, 30
well-known ports, list of, 133–134
wet pipe systems, 438
white hats, 7
whitelists, 31, 101
whole disk encryption, 40–41, 73
wide area networks (WANs), location area networks (LANs) versus, 123
Windows Firewall, 33
Windows Update, installing updates, patches, hotfixes, 65–69
Windows XP Mode, 78
wire tapping, 192–195
wired network security, 186
cable vulnerabilities, 189–195
crosstalk, *191–192*
data emanation, *192*
interference, *190–191*
tapping into data, *192–195*
device vulnerabilities, 186–189
backdoors, *188*
default accounts, *186–187*
network attacks, *189*
privilege escalation, *188*
weak passwords, *187*

wireless access points
securing, 203–205
vulnerabilities, 195–199
wireless network security, 195
wireless access point vulnerabilities, 195–199
wireless transmission vulnerabilities, 199
wireless networks, vulnerability assessments, 292
wireless transmission vulnerabilities, 199
Wireshark, 297, 319–320
wood fires, extinguishing, 436
Word, securing, 106
worms, 17
preventing and troubleshooting, 27

X

X.509 standard, 380
XSS (cross-site scripting), 98, 142

Z

zombies, 23, 140
zone transfers, 143
ZoneAlarm, 33