DAVID L. PROWSE

CompTIA APPROVED QUALITY CONTENT AUTHORIZED

Authorized Cert Guide

Learn, prepare, and practice for exam success

- Master every topic on CompTIA's new Security+ SY0-301 exam.
- Assess your knowledge and focus your learning.
- Get the practical workplace knowledge you need!
- Practice with realistic exam questions on the DVD

CompTIA Security+™ SY0-301

Second Edition

DVD FEATURES COMPLETE SAMPLE EXAM

PEARSON

CompTIA Security+ SY0-301 Authorized Cert Guide

David L. Prowse

PEARSON

Pearson IT Certification
800 East 96th Street,
Indianapolis,
Indiana
46240
USA

CompTIA Security+ SY0-301 Authorized Cert Guide

CompTIA Security+ SY0-301 Authorized Cert Guide, Deluxe Edition

ISBN-13: 978-0-7897-4827-0
ISBN-10: 0-7897-4827-4

CompTIA Security+ SY0-301 Authorized Cert Guide, Standard Edition:

ISBN-13: 978-0-7897-4921-5
ISBN-10: 0-7897-4921-1

Library of Congress Cataloging-in-Publication Data:
Prowse, David L.
CompTIA security+ SY0-301 authorized cert guide / David L. Prowse.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-7897-4827-0 (hardcover : alk. paper)
1. Computer security—Examinations—Study guides. 2. Computer technicians—Certification—Study guides. 3. Computer networks—Security measures—Examinations—Study guides. 4. Computing Technology Industry Association—Examinations—Study guides. I. Title.
QA76.9.A25P788 2012
005.8—dc23
2011042332

Printed in the United States of America
First Printing: December 2011

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.

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 the United States, please contact

International Sales
international@pearson.com

Editor-in-Chief
David Dushimer

Acquisitions Editor
Betsy Brown

Development Editor
Andrew Cupp

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Geneil Breeze

Indexer
Cheryl Lenser

Proofreader
Leslie Joseph

Technical Editor
Aubrey Adams

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Tony Palleschi

Book Designer
Gary Adair

Compositor
Bronkella Publishing LLC

Contents at a Glance

Introduction xxv

CHAPTER 1 Introduction to Security 3

CHAPTER 2 Computer Systems Security 17

CHAPTER 3 OS Hardening and Virtualization 67

CHAPTER 4 Application Security 109

CHAPTER 5 Network Design Elements and Network Threats 149

CHAPTER 6 Network Perimeter Security 205

CHAPTER 7 Securing Network Media and Devices 233

CHAPTER 8 Physical Security and Authentication Models 265

CHAPTER 9 Access Control Methods and Models 305

CHAPTER 10 Vulnerability and Risk Assessment 341

CHAPTER 11 Monitoring and Auditing 379

CHAPTER 12 Encryption and Hashing Concepts 415

CHAPTER 13 PKI and Encryption Protocols 451

CHAPTER 14 Redundancy and Disaster Recovery 475

CHAPTER 15 Policies, Procedures, and People 509

CHAPTER 16 Taking the Real Exam 551

Practice Exam 1: CompTIA Security+ SY0-301 561

Practice Exam 2: CompTIA Security+ SY0-301 611

Glossary 663

Master List of Key Topics 684

Index 692

On the DVD:

Appendix A: Memory Tables

Appendix B: Memory Tables Answer Key

Table of Contents

Introduction xxv

Chapter 1 Introduction to Security 3

Foundation Topics 4

Security 101 4

The CIA of Computer Security 4

The Basics of Information Security 6

Think Like a Hacker 9

Exam Preparation Tasks 11

Review Key Topics 11

Define Key Terms 11

Answer Review Questions 11

Answers and Explanations 13

Chapter 2 Computer Systems Security 17

Foundation Topics 18

Computer Systems Security Threats 18

Malicious Software 18

Viruses 18

Worms 19

Trojan Horses 20

Spyware 21

Rootkits 21

Spam 21

Summary of Malware Threats 22

Ways to Deliver Malicious Software 23

Via Software, Messaging, and Media 23

Active Interception 23

Privilege Escalation 24

Backdoors 24

Logic Bombs 24

Botnets and Zombies 25

Preventing and Troubleshooting Malware 26

Preventing and Troubleshooting Viruses 26

Preventing and Troubleshooting Worms and Trojans 30

Preventing and Troubleshooting Spyware 30

Preventing and Troubleshooting Rootkits 32

Preventing and Troubleshooting Spam 33

You Can't Save Every Computer from Malware! 35

Summary of Malware Prevention Techniques 35

Implementing Security Applications 36

Personal Software Firewalls 36

Host-Based Intrusion Detection Systems 38

Pop-Up Blockers 40

Data Loss Prevention Systems 42

Securing Computer Hardware and Peripherals 42

Securing the BIOS 43

Securing Storage Devices 44

Removable Storage 44

Network Attached Storage 45

Whole Disk Encryption 45

Hardware Security Modules 47

Securing Cell Phones and Smartphones 47

Exam Preparation Tasks 49

Review Key Topics 49

Complete Tables and Lists from Memory 49

Define Key Terms 50

Hands-On Labs 50

Equipment Needed 50

Lab 2-1: Using Free Malware Scanning Programs 50

Lab 2-2: How to Secure the BIOS 51

View Recommended Resources 53

Answer Review Questions 54

Answers and Explanations 60

Chapter 3 OS Hardening and Virtualization 67

Foundation Topics 68

Hardening Operating Systems 68

Removing Unnecessary Applications and Services 68

Service Packs 72

Windows Update, Patches, and Hotfixes 75

Patches and Hotfixes 77

Patch Management 79

Group Policies, Security Templates, and Configuration Baselines 80

Hardening File Systems and Hard Drives 82

Virtualization Technology 86

Types of Virtualization and Their Purposes 86

Working with Virtual Machines 88

Microsoft Virtual PC 88

Microsoft Windows XP Mode 90

Microsoft Virtual Server 90

VMware 91

Hypervisor 92

Securing Virtual Machines 92

Exam Preparation Tasks 94

Review Key Topics 94

Complete Tables and Lists from Memory 95

Define Key Terms 95

Hands-On Labs 95

Equipment Needed 95

Lab 3-1: Discerning and Updating the Service Pack Level 96

Lab 3-2: Creating a Virtual Machine in Virtual PC 2007 96

Lab 3-3: Securing a Virtual Machine 98

View Recommended Resources 101

Answer Review Questions 102

Answers and Explanations 105

Chapter 4 Application Security 109

Foundation Topics 110

Securing the Browser 110

General Browser Security Procedures 111

Implement Policies 111

Train Your Users 114

Use a Proxy and Content Filter 114

Secure Against Malicious Code 116

Securing Internet Explorer 116

Securing Firefox 121

Securing Other Applications 124

Secure Programming 127

Systems Development Life Cycle 128

Programming Testing Methods 130

Programming Vulnerabilities and Attacks 132

Backdoors 132

Buffer Overflows 132

XSS and XSRF 133

More Code Injection Examples 133

Directory Traversal 134

Zero Day Attack 135

Exam Preparation Tasks 136

Review Key Topics 136

Complete Tables and Lists from Memory 136

Define Key Terms 137

Hands-On Labs 137

Equipment Needed 137

Lab 4-1: Securing the Browser 137

Lab 4-2: Disabling Applications with a Windows Server 2008 Policy 138

View Recommended Resources 141

Answer Review Questions 141

Answers and Explanations 145

Chapter 5 Network Design Elements and Network Threats 149

Foundation Topics 150

Network Design 150

Network Devices 150

Hub 150

Switch 151

Router 152

Network Address Translation, and Private Versus Public IP 154

Network Zones and Interconnections 156

LAN Versus WAN 157

Internet 157

Demilitarized Zone (DMZ) 157

Intranets and Extranets 159

Cloud Computing 159

Network Access Control (NAC) 162

Subnetting 162

Virtual Local Area Network (VLAN) 164

Telephony Devices 165

Modems 166

PBX Equipment 166

VoIP 167

Ports and Protocols 167

Ports Ranges, Inbound Versus Outbound, and Common Ports 167

Protocols That Can Cause Anxiety on the Exam 174

Malicious Network Attacks 175

DoS 175

DDoS 178

Spoofing 178

Session Hijacking 179

Replay 181

Null Sessions 181

Transitive Access and Client-Side Attacks 182

DNS Poisoning and Other DNS Attacks 183

ARP Poisoning 184

Summary of Network Attacks 185

Exam Preparation Tasks 188
Review Key Topics 188
Complete Tables and Lists from Memory 189
Define Key Terms 189
Hands-On Labs 189
Equipment Needed 190
Lab 5-1: Port Scanning Basics 190
View Recommended Resources 191
Answer Review Questions 192
Answers and Explanations 199
Chapter 6 Network Perimeter Security 205
Foundation Topics 206
Firewalls and Network Security 206
Firewalls 207
Proxy Servers 212
Honeypots and Honeynets 215
Data Loss Prevention (DLP) 216
NIDS Versus NIPS 217
NIDS 217
NIPS 218
Summary of NIDS Versus NIPS 219
The Protocol Analyzer's Role in NIDS and NIPS 220
Exam Preparation Tasks 220
Review Key Topics 220
Complete Tables and Lists from Memory 221
Define Key Terms 221
Hands-On Labs 221
Equipment Needed 222
Lab 6-1: Packet Filtering and NAT Firewalls 222
Lab 6-2: Configuring an Inbound Filter on a SOHO Router/Firewall 223
Lab 6-3: Enabling MAC Filtering 224
View Recommended Resources 225
Answer Review Questions 225
Answers and Explanations 229

Chapter 7 Securing Network Media and Devices 233

Foundation Topics 234

Securing Wired Networks and Devices 234

Network Device Vulnerabilities 234

Default Accounts 234

Weak Passwords 235

Privilege Escalation 236

Back Doors 237

Network Attacks 237

Other Network Device Considerations 238

Cable Media Vulnerabilities 238

Interference 239

Crosstalk 240

Data Emanation 241

Tapping into Data and Conversations 241

Securing Wireless Networks 244

Wireless Access Point Vulnerabilities 244

Secure the Administration Interface 244

SSID Broadcast 245

Rogue Access Points 245

Evil Twin 246

Weak Encryption 246

Other Wireless Access Point Security Strategies 248

Wireless Transmission Vulnerabilities 250

Bluetooth Vulnerabilities 250

Bluejacking 251

Bluesnarfing 251

Exam Preparation Tasks 252

Review Key Topics 252

Complete Tables and Lists from Memory 253

Define Key Terms 253

Hands-On Labs 253

Equipment Needed 254

Lab 7-1: Securing a Wireless Device: 8 Steps to a Secure Network 254

Lab 7-2: Wardriving...and The Cure 256

View Recommended Resources 257

Answer Review Questions 257

Answers and Explanations 261

Chapter 8 Physical Security and Authentication Models 265

Foundation Topics 267

Physical Security 267

General Building and Server Room Security 267

Door Access 268

Biometric Readers 270

Authentication Models and Components 271

Authentication Models 271

Localized Authentication Technologies 273

802.1X and EAP 273

LDAP 276

Kerberos and Mutual Authentication 277

Terminal Services 279

Remote Authentication Technologies 279

Remote Access Service 280

Virtual Private Networks 281

RADIUS Versus TACACS 284

Exam Preparation Tasks 286

Review Key Topics 286

Complete Tables and Lists from Memory 287

Define Key Terms 287

Hands-On Labs 287

Equipment Needed 288

Lab 8-1: Enabling 802.1X on a Network Adapter 288

Lab 8-2: Setting Up a VPN 289

View Recommended Resources 291

Answer Review Questions 292

Answers and Explanations 299

Chapter 9 Access Control Methods and Models 305

Foundation Topics 306

Access Control Models Defined 306

Discretionary Access Control 306

Mandatory Access Control 308

Role-Based Access Control (RBAC) 309

Access Control Wise Practices 310

Rights, Permissions, and Policies 313

Users, Groups, and Permissions 313

Permission Inheritance and Propagation 317

Moving and Copying Folders and Files 318

Usernames and Passwords 318

Policies 322

User Account Control (UAC) 325

Exam Preparation Tasks 326

Review Key Topics 326

Complete Tables and Lists from Memory 327

Define Key Terms 327

Hands-On Labs 327

Equipment Needed 327

Lab 9-1: Configuring Password Policies and User Account Restrictions 328

Lab 9-2: Configuring User and Group Permissions 330

View Recommended Resources 331

Answer Review Questions 332

Answers and Explanations 337

Chapter 10 Vulnerability and Risk Assessment 341

Foundation Topics 342

Conducting Risk Assessments 342

Qualitative Risk Assessment 344

Quantitative Risk Assessment 344

Security Analysis Methodologies 346

Security Controls 347

Vulnerability Management 349

Penetration Testing 350

OVAL 351

Assessing Vulnerability with Security Tools 352

Network Mapping 352

Vulnerability Scanning 355

Network Sniffing 358

Password Analysis 359

Exam Preparation Tasks 363

Review Key Topics 363

Complete Tables and Lists from Memory 363

Define Key Terms 364

Hands-On Labs 364

Equipment Needed 364

Lab 10-1: Mapping and Scanning the Network 365

Lab 10-2: Password Cracking and Defense 366

View Recommended Resources 367

Answer Review Questions 368

Answers and Explanations 374

Chapter 11 Monitoring and Auditing 379

Foundation Topics 380

Monitoring Methodologies 380

Signature-Based Monitoring 380

Anomaly-Based Monitoring 381

Behavior-Based Monitoring 381

Using Tools to Monitor Systems and Networks 382

Performance Baselining 382

Protocol Analyzers 384

Wireshark 385

Network Monitor 386

SNMP 388

Conducting Audits 389

Auditing Files 389

Logging 392

Log File Maintenance and Security 394

Auditing System Security Settings 396

Exam Preparation Tasks 399
Review Key Topics 399
Complete Tables and Lists from Memory 400
Define Key Terms 400
Hands-On Labs 400
Equipment Needed 400
Lab 11-1: Using Protocol Analyzers 401
View Recommended Resources 403
Answer Review Questions 404
Answers and Explanations 409
Chapter 12 Encryption and Hashing Concepts 415
Foundation Topics 416
Cryptography Concepts 416
Symmetric Versus Asymmetric Key Algorithms 419
Symmetric Key Algorithms 420
Asymmetric Key Algorithms 421
Public Key Cryptography 421
Key Management 422
Steganography 423
Encryption Algorithms 423
DES and 3DES 424
AES 424
RC 425
Summary of Symmetric Algorithms 426
RSA 426
Diffie-Hellman 427
Elliptic Curve 428
More Encryption Types 428
One-Time Pad 428
PGP 429
Hashing Basics 430
Cryptographic Hash Functions 431
MD5 432
SHA 432

Happy Birthday! *432*

LANMAN, NTLM, and NTLM2 433

LANMAN *433*

NTLM and NTLM2 *435*

Exam Preparation Tasks 436

Review Key Topics 436

Complete Tables and Lists from Memory 436

Define Key Terms 436

Hands-On Lab 437

Equipment Needed 437

Lab 12-1: Disabling the LM Hash in Windows Server 2003 437

View Recommended Resources 438

Answer Review Questions 439

Answers and Explanations 445

Chapter 13 PKI and Encryption Protocols 451

Foundation Topics 452

Public Key Infrastructure 452

Certificates 452

Certificate Authorities 453

Single-Sided and Dual-Sided Certificates 456

Web of Trust 456

Security Protocols 457

S/MIME 457

SSL/TLS 458

SSH 459

PPTP, L2TP, and IPsec 459

PPTP *460*

L2TP *460*

IPsec *460*

Exam Preparation Tasks 461

Review Key Topics 461

Define Key Terms 462

Hands-On Labs 462

Equipment Needed 462

Lab 13-1: A Basic Example of PKI 462

Lab 13-2: Making an SSH Connection 463

View Recommended Resources 465

Answer Review Questions 465

Answers and Explanations 470

Chapter 14 Redundancy and Disaster Recovery 475

Foundation Topics 476

Redundancy Planning 476

Redundant Power 478

Redundant Power Supplies 479

Uninterruptible Power Supplies 480

Backup Generators 481

Redundant Data 483

Redundant Networking 486

Redundant Servers 488

Redundant Sites 489

Disaster Recovery Planning and Procedures 490

Data Backup 490

DR Planning 494

Exam Preparation Tasks 497

Review Key Topics 497

Complete Tables and Lists from Memory 497

Define Key Terms 498

Hands-On Labs 498

Equipment Needed 498

Lab 14-1: Configuring RAID 1 and 5 498

View Recommended Resources 500

Answer Review Questions 500

Answers and Explanations 504

Chapter 15 Policies, Procedures, and People 509

Foundation Topics 510

Environmental Controls 510

Fire Suppression 510

Fire Extinguishers 510

Sprinkler Systems 512

Special Hazard Protection Systems 512

HVAC 513

Shielding 514

Social Engineering 515

Pretexting 516

Diversion Theft 516

Phishing 516

Hoaxes 518

Shoulder Surfing 518

Eavesdropping 518

Dumpster Diving 519

Baiting 519

Piggybacking/Tailgating 519

Summary of Social Engineering Types 519

User Education and Awareness 520

Legislative and Organizational Policies 521

Data Sensitivity and Classification of Information 522

Personnel Security Policies 524

Privacy Policies 525

Acceptable Use 525

Change Management 525

Separation of Duties/Job Rotation 526

Mandatory Vacations 526

Due Diligence 527

Due Care 527

Due Process 527

User Education and Awareness Training 527

Summary of Personnel Security Policies 528

How to Deal with Vendors 529

How to Dispose of Computers and Other IT Equipment Securely 529

Incident Response Procedures 531

Exam Preparation Tasks 534

Review Key Topics 534

Complete Tables and Lists from Memory 535

Define Key Terms 535

View Recommended Resources 535

Answer Review Questions 536

Answers and Explanations 543

Chapter 16 Taking the Real Exam 551

Foundation Topics 552

Getting Ready and the Exam Preparation Checklist 552

Tips for Taking the Real Exam 555

Beyond the CompTIA Security+ Certification 558

Hands-On Lab 559

Practice Exam 1 561

Practice Exam 2 611

Glossary 663

Master List of Key Topics 685

Index 692

On the DVD:

Appendix A: Memory Tables

Appendix B: Memory Tables Answer Key

About the Author

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

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

About the Reviewer

Aubrey Adams (CCNA, Security+) is an electronic and computer system engineering lecturer and Cisco Networking Academy instructor at Central Institute of Technology in Perth, Western Australia. Coming from a background in telecommunications design, with qualifications in electronic engineering and management and graduate diplomas in computing and education, he teaches across a range of computer systems and networking vocational education and training areas. Aubrey also authors Networking Academy curriculum and assessments and is a Cisco Press author and Pearson Education technical editor.

Acknowledgments

This book and accompanying DVD wouldn't have been possible without my publisher, Pearson. I've been involved in many projects with Pearson over the past several years and give my thanks for the ongoing opportunities and support I have received.

One person in particular I'd like to acknowledge is Andrew Cupp. Drew, once again, your guidance during this project has been nothing short of greatness. You definitely helped develop what I think is an exceptional product.

I'd also like to thank Aubrey Adams for his excellent feedback during the creation of this book. Good technical editors are difficult to find; I'm grateful to Aubrey for his dedication and hard work during this project. My thanks also go out to the various people involved in developing and publishing this book: David Dusthimer, Betsy Brown, Sandra Schroeder, Tony Palleschi, Tonya Simpson, Tim Warner, and Vanessa Evans. It takes a lot of talented people to get a final product on the shelves—I appreciate everything you did to make this book a reality.

Special thanks to Dr. Rick Blazek, Tony Ardito, and Brian Campbell. Your contributions and suggestions helped me to incorporate a "real-world" feel and were key ingredients in keeping the book current.

And then there are the usual suspects—my wife, family, friends; thank you for bearing with me on yet another crazy book-writing crusade!

Finally, I thank my website readers. Your input over the years has helped me tailor my book projects, making them more complete and helping them to be successful.

We Want to Hear from You!

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

As an associate publisher for Pearson IT Certification, I welcome your comments. You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

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

Email: feedback@pearsonitcertification.com

Mail: David Dusthimer
Associate Publisher
Pearson IT Certification
800 East 96th Street
Indianapolis, IN 46240 USA

CompTIA Security+

- Designed for IT professionals focused on system security.
- Covers network infrastructure, cryptography, assessments, and audits.
- Security+ is mandated by the U.S. Department of Defense and is recommended by top companies such as Microsoft, HP, and Cisco.

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill. Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation, and promotion.

Security is one of the highest demand job categories. Growing in importance as the frequency and severity of security threats continues to be a major concern for organizations around the world.

- **Jobs for security administrators are expected to increase by 18%** -the skill set required for these types of jobs map to CompTIA Security+ certification.
- **Network Security Administrators -** can earn as much as $106,000 per year.
- **CompTIA Security+ is the first step -** in starting your career as a Network Security Administrator or Systems Security Administrator.
- **CompTIA Security+ is regularly used in organizations -** such as Hitachi Information Systems, Trendmicro, the McAfee Elite Partner program, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

How Certification Helps Your Career

IT is Everywhere

IT is ubiquitous, needed by most organizations. Globally, there are over 600,000 IT job openings.

IT Knowledge and Skills Gets Jobs

Certifications are essential credentials that qualify you for jobs, increased compensation, and promotion.

Retain your Job and Salary

Make your expertise stand above the rest. Competence is usually retained during times of change.

Want to Change Jobs

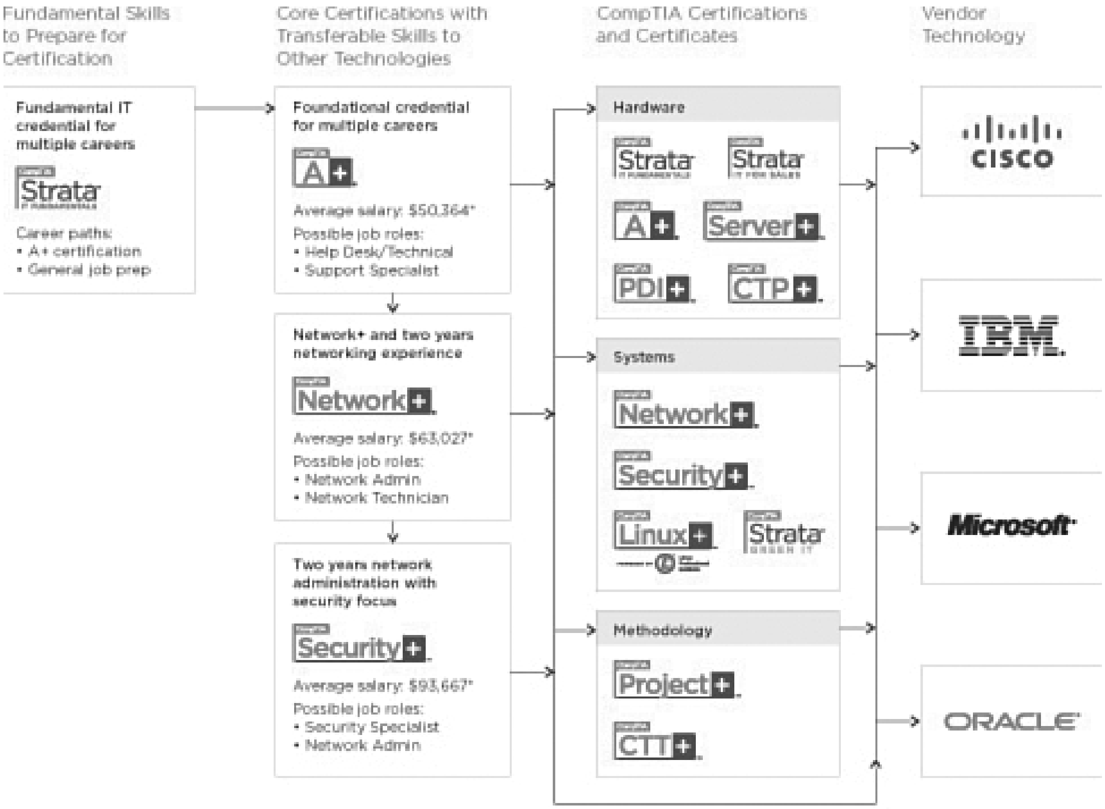
Certifications qualify you for new opportunities, whether locked into a current job, see limited advancement, or need to change careers.

Stick Out from the Resume Pile

Hiring managers can demand the strongest skill set.

CompTIA Career Pathway

CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.



*Source: *Computerworld* Salary Survey 2010—U.S. salaries only

Steps to Getting Certified and Staying Certified	
Review Exam Objectives	Review the certification objectives to make sure you know what is covered in the exam. http://www.comptia.org/certifications/testprep/examobjectives.aspx
Practice for the Exam	After you have studied for the certification, take a free assessment and sample test to get an idea what type of questions might be on the exam. http://www.comptia.org/certifications/testprep/practicetests.aspx
Purchase an Exam Voucher	Purchase your exam voucher on the CompTIA Marketplace, which is located at: www.comptiastore.com
Take the Test!	Select a certification exam provider and schedule a time to take your exam. You can find exam providers at the following link: http://www.comptia.org/certifications/testprep/testingcenters.aspx
Stay Certified! **Continuing Education**	Effective January 1, 2011, new CompTIA Security+ certifications are valid for three years from the date of your certification. There are a number of ways the certification can be renewed. For more information go to: http://certification.comptia.org/getCertified/steps_to_certification/stayCertified.aspx

Join the Professional Community

Join IT Pro Community http://itpro.comptia.org	The free IT Pro online community provides valuable content to students and professionals. • Career IT Job Resources ▪Where to start in IT ▪Career Assessments ▪Salary Trends ▪US Job Board • Forums on Networking, Security, Computing and Cutting Edge Technologies • Access to blogs written by Industry Experts • Current information on Cutting Edge Technologies • Access to various industry resource links and articles related to IT and IT careers

Content Seal of Quality

This courseware bears the seal of **CompTIA Approved Quality Content.** This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.

Why CompTIA?

- **Global Recognition** – CompTIA is recognized globally as the leading IT non-profit trade association and has enormous credibility. Plus, CompTIA's certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.
- **Valued by Hiring Managers -** Hiring managers value CompTIA certification because it is vendor and technology independent validation of your technical skills.
- **Recommended or Required by Government and Businesses** - Many government organizations and corporations either recommend or require technical staff to be CompTIA certified. (e.g. Dell, Sharp, Ricoh, the U.S. Department of Defense and many more)
- **Three CompTIA Certifications ranked in the top 10**. In a study by DICE of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

How to obtain more information

- **Visit CompTIA online** - www.comptia.org to learn more about getting CompTIA certified.
- **Contact CompTIA** - call 866-835-8020 ext. 5 or email questions@comptia.org
- **Join the IT Pro Community** – http://itpro.comptia.org to join the IT community to get relevant career information.
- **Connect with us :** in f t •• You Tube

Introduction

Welcome to the *CompTIA Security+ SY0-301 Authorized 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.

IMPORTANT NOTE!!

The first thing you should do before you start reading Chapter 1 is check my website for errata and updated information, and mark those new items in the book. On my site you will also find videos, articles, and additional test questions. And of course, feel free to ask me questions about the book. You can reach the Security+ page of my website directly at the following link:

www.SY0-301.com

Or, go to my home page at the following link:

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.davidlprowse.com/instructor-sy0-301.php

(You may afterward be redirected to a separate Pearson web page to download the materials.)

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 2011 version of the CompTIA Security+ Certification Exam (number SY0-301). To that effect, I have filled this book with more than 500 questions/answers and explanations in total, including two 100-question practice exams. The exams are in text at the end of the book and located on the disc in a simulated test environment. These tests are geared to check your knowledge and ready you for the real exam.

Deluxe Edition

The Deluxe Edition has one additional practice exam as well as a suite of Security+ learning activities on the DVD.

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

- **Opening topics list**—This defines the topics to be covered in the chapter; it also lists the corresponding CompTIA Security+ objective numbers.
- **Topical coverage**—The heart of the chapter. Explains the topics from a theory-based standpoint, as well as from a hands-on perspective. This includes in-depth descriptions, tables, and figures that are geared to build your knowledge so that you can pass the exam. The chapters are broken down into two to three topics each.

- **Key Topics**—The Key Topic icons indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in table format at the end of the chapter.
- **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 most chapters. The step-by-step procedures appear at the end of the chapters (as well as on the disc) and the corresponding video solutions can be found on the disc as well.
- **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. Again, if you have questions or suggestions, please contact me through my website:

www.davidlprowse.com

I try my best to answer your queries as soon as possible.

Who Should Read This Book?

This book is for anyone who wants to start or advance a career in IT security. Readers of this book can range from persons taking a Security+ course to individuals already in the field who want to keep their skills sharp, or perhaps retain their job due to a company policy mandating they take the Security+ exam. Some information assurance professionals who work for the Department of Defense or have privileged access to DoD systems are required to become Security+ certified as per DoD directive 8570.1.

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

Although not a prerequisite, it is recommended that CompTIA Security+ candidates have at least two years of technical networking experience with an emphasis on security. The CompTIA Network+ certification is also recommended as a prerequisite. It is expected that you understand computer topics such as how to install operating systems and applications, and networking topics such as how to configure IP, what a

VLAN is, and so on. The focus of this book is to show how to secure these technologies and protect against possible exploits and attacks. Generally, for people looking to enter the IT field, the CompTIA Security+ certification is attained after the A+ and Network+ certifications.

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

CompTIA Security+ Exam Topics

Table I-1 lists the exam topics for the CompTIA Security+ exam. This table lists the chapter in which each exam topic is covered. Chapter 1 is an introductory chapter and as such does not map to any specific exam objectives. Chapter 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 3.1, 3.2, 4.2, 4.3
3	Hardening Operating Systems Virtualization Technology	Objectives 3.6, 4.1, 4.2
4	Securing the Browser Securing Other Applications Secure Programming	Objective 3.5, 4.1, 4.2
5	Network Design Ports and Protocols Malicious Attacks	Objectives 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 3.2, 3.5, 4.3
6	Firewalls and Network Security NIDS Versus NIPS	Objectives 1.1, 1.2, 3.6

Table I-1 CompTIA Security+ Exam Topics

Chapter	Exam Topic	CompTIA Security+ Exam Objectives Covered
7	Securing Wired Networks and Devices Securing Wireless Networks	Objectives 1.6, 3.4, 6.2
8	Physical Security Authentication Models and Components	Objectives 3.6, 4.2, 5.1, 5.2
9	Access Control Models Defined Rights, Permissions, and Policies	Objectives 2.2, 5.2, 5.3
10	Conducting Risk Assessments Assessing Vulnerability with Security Tools	Objectives 1.1, 2.1, 2.2, 3.7, 3.8
11	Monitoring Methodologies Using Tools to Monitor Systems and Networks Conducting Audits	Objectives 2.2, 2.3, 3.6, 4.1
12	Cryptography Concepts Encryption Algorithms Hashing Basics	Objectives 4.3, 6.1, 6.2
13	Public Key Infrastructure Security Protocols	Objectives 1.4, 6.2, 6.3, 6.4
14	Redundancy Planning Disaster Recovery Planning and Procedures	Objective 1.1, 2.5, 2.7
15	Environmental Controls Social Engineering Legislative and Organizational Policies	Objectives 2.1, 2.3, 2.4, 2.6, 3.3, 5.2
16	Getting Ready and the Exam Preparation Checklist Tips for Taking the Real Exam Beyond the CompTIA Security+ Certification	n/a

Pearson IT Certification Practice Test Engine and Questions on the DVD

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

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

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

Install the Software from the DVD

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

- Windows XP (SP3), Windows Vista (SP2), or Windows 7
- Microsoft .NET Framework 4.0 Client
- Pentium class 1GHz processor (or equivalent)
- 512 MB RAM
- 650 MB disc space plus 50 MB for each downloaded practice exam

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

The following steps outline the installation process:

Step 1. Insert the DVD into your PC.

Step 2. The software that automatically runs is the Pearson software to access and use all DVD-based features, including the exam engine and the DVD-only appendices. From the Practice Exam tab, click the option **Install Practice Exam**.

Step 3. Respond to windows prompts as with any typical software installation process.

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

Activate and Download the Practice Exam

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

Step 1. Start the Pearson IT Certification Practice Test software from the Windows **Start** menu or from your desktop shortcut icon.

Step 2. To activate and download the exam associated with this book, from the **My Products** or **Tools** tab, select the **Activate** button.

Step 3. At the next screen, enter the Activation Key from the paper inside the cardboard DVD holder in the back of the book. Once entered, click the **Activate** button.

Step 4. The activation process will download the practice exam. Click **Next**; then click **Finish.**

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

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

If you want to check for updates to the Pearson IT Certification Practice Test software, simply select the **Tools** tab and select the **Update Engine** button. This ensures you are running the latest version of the software engine.

Activating Other Exams

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

Premium Edition

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

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

To view the premium edition product page, go to

www.informit.com/title/9780132939607

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+ SY0-301 objectives 3.6, 4.1, and 4.2.

CHAPTER 3

OS Hardening and Virtualization

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

Another way to create a secure environment is to run 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 be 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 was easily accessible and had no password? Although these types of oversights are constantly being improved upon, making an out-of-the-box experience more pleasant, new applications and new technologies offer new security implications as well. So regardless of the product, we must try to protect it after the installation is complete.

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

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

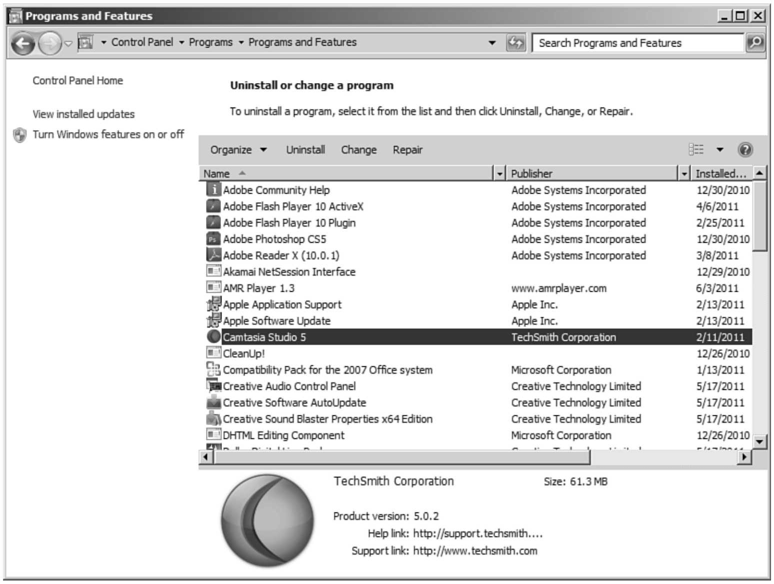
Removing Unnecessary Applications and Services

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 application are disabled as well. Basically, remove all instances of the application or, if necessary, re-image the computer! That is just one example of many, but it can be applied to most superfluous programs. Another type of program you should watch out for are remote control programs. Applications that enable remote control of a computer should be avoided if possible.

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



Programs and Features
Control Panel ▸ Programs ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾
Uninstall
Change
Repair

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed...
Adobe Community Help	Adobe Systems Incorporated	12/30/2010
Adobe Flash Player 10 ActiveX	Adobe Systems Incorporated	4/6/2011
Adobe Flash Player 10 Plugin	Adobe Systems Incorporated	2/25/2011
Adobe Photoshop CS5	Adobe Systems Incorporated	12/30/2010
Adobe Reader X (10.0.1)	Adobe Systems Incorporated	3/8/2011
Akamai NetSession Interface		12/29/2010
AMR Player 1.3	www.amrplayer.com	6/3/2011
Apple Application Support	Apple Inc.	2/13/2011
Apple Software Update	Apple Inc.	2/13/2011
Camtasia Studio 5	TechSmith Corporation	2/11/2011
CleanUp!		12/26/2010
Compatibility Pack for the 2007 Office system	Microsoft Corporation	1/13/2011
Creative Audio Control Panel	Creative Technology Limited	5/17/2011
Creative Software AutoUpdate	Creative Technology Limited	5/17/2011
Creative Sound Blaster Properties x64 Edition	Creative Technology Limited	5/17/2011
DHTML Editing Component	Microsoft Corporation	12/26/2010

TechSmith Corporation Size: 61.3 MB

Product version: 5.0.2
Help link: http://support.techsmith....
Support link: http://www.techsmith.com

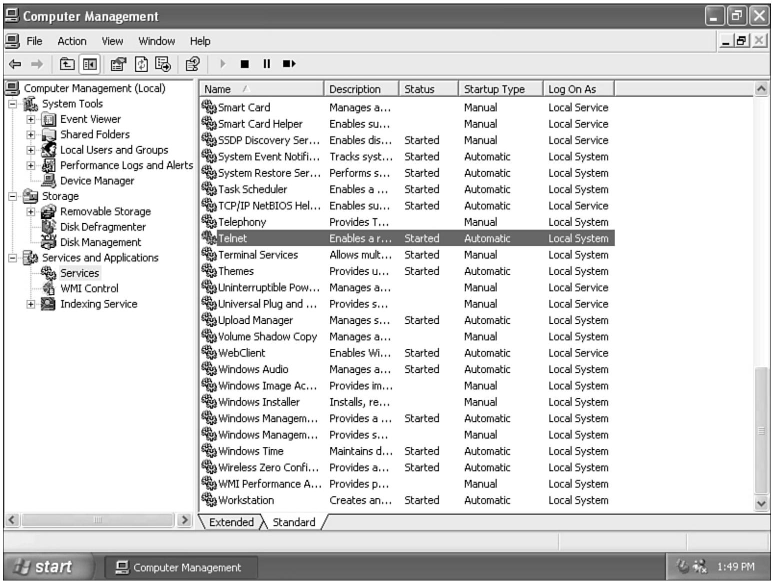
Figure 3-1 Windows 7 Programs and Features Window

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 many applications place a piece of themselves in the system tray. So, a part of the program is actually running behind the scenes using processor/RAM resources. If the application is necessary, there are often ways to eliminate it from the 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 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

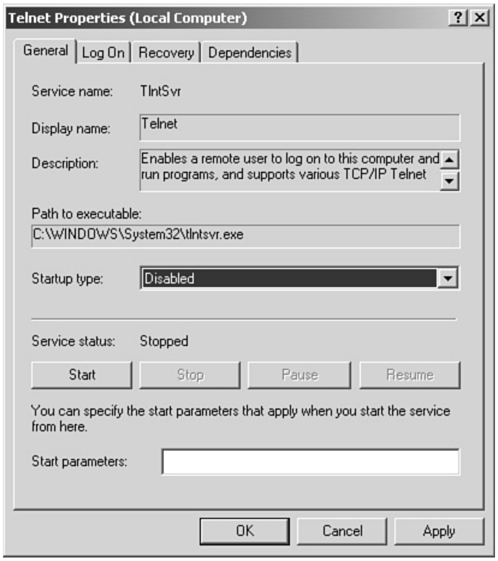


Name	Description	Status	Startup Type	Log On As
Smart Card	Manages a...		Manual	Local Service
Smart Card Helper	Enables su...		Manual	Local Service
SSDP Discovery Ser...	Enables dis...	Started	Manual	Local Service
System Event Notifi...	Tracks syst...	Started	Automatic	Local System
System Restore Ser...	Performs s...	Started	Automatic	Local System
Task Scheduler	Enables a ...	Started	Automatic	Local System
TCP/IP NetBIOS Hel...	Enables su...	Started	Automatic	Local Service
Telephony	Provides T...		Manual	Local System
Telnet	Enables a r...	Started	Automatic	Local System
Terminal Services	Allows mult...	Started	Manual	Local System
Themes	Provides u...	Started	Automatic	Local System
Uninterruptible Pow...	Manages a...		Manual	Local Service
Universal Plug and ...	Provides s...		Manual	Local Service
Upload Manager	Manages s...	Started	Automatic	Local System
Volume Shadow Copy	Manages a...		Manual	Local System
WebClient	Enables Wi...	Started	Automatic	Local Service
Windows Audio	Manages a...	Started	Automatic	Local System
Windows Image Ac...	Provides im...		Manual	Local System
Windows Installer	Installs, re...		Manual	Local System
Windows Managem...	Provides a ...	Started	Automatic	Local System
Windows Managem...	Provides s...		Manual	Local System
Windows Time	Maintains d...	Started	Automatic	Local System
Wireless Zero Confi...	Provides a...	Started	Automatic	Local System
WMI Performance A...	Provides p...		Manual	Local System
Workstation	Creates an...	Started	Automatic	Local System

Figure 3-2 Services Window in Windows XP

The OS shown in Figure 3-2 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 matters worse, the Telnet service in the figure is started! Instead of using Telnet, a more secure application/protocol should be utilized such as SSH. Then Telnet should be stopped and disabled. To do so, just right-click the service, select **Properties**, 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



Telnet Properties (Local Computer)

Service name: TlntSvr

Display name: Telnet

Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet

Path to executable:
C:\WINDOWS\System32\tlntsvr.exe

Startup type: Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 3-3 Telnet Properties Dialog Box

Key Topic

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

- By typing the following syntax:

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

  where <service> is the service name.

- 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.

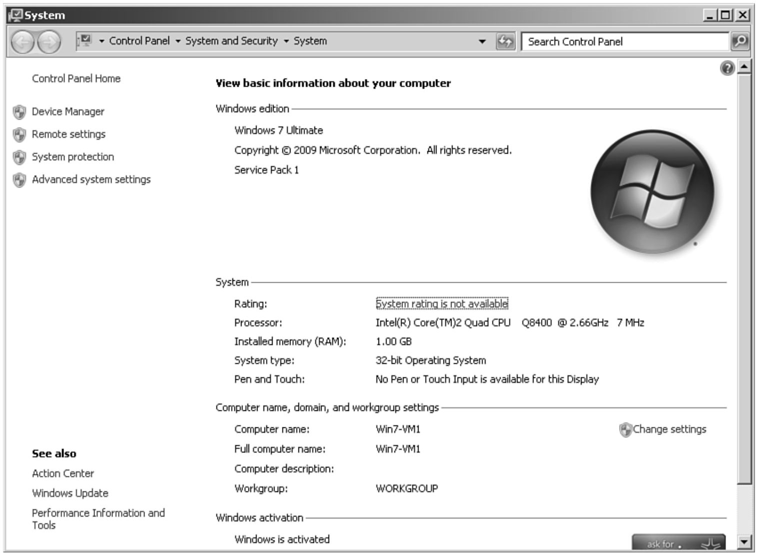
Historically, many SPs have been cumulative, meaning that they also contain previous SPs. For example, SP2 for Windows XP includes all the updates from SP1; a Windows XP installation with no SP installed can be updated directly to SP2 without having to install SP1 first. However, you also see incremental 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; SP1 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 7's System window is shown in Figure 3-4; it shows that SP1 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



View basic information about your computer

Windows edition

Windows 7 Ultimate

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

System

Rating: System rating is not available

Processor: Intel(R) Core(TM)2 Quad CPU Q8400 @ 2.66GHz 7 MHz

Installed memory (RAM): 1.00 GB

System type: 32-bit Operating System

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: Win7-VM1

Full computer name: Win7-VM1

Computer description:

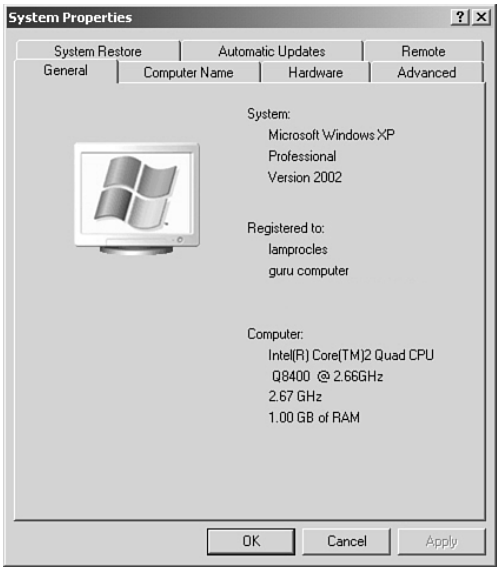
Workgroup: WORKGROUP

Windows activation

Windows is activated

Figure 3-4 Windows 7 System Window

Key Topic



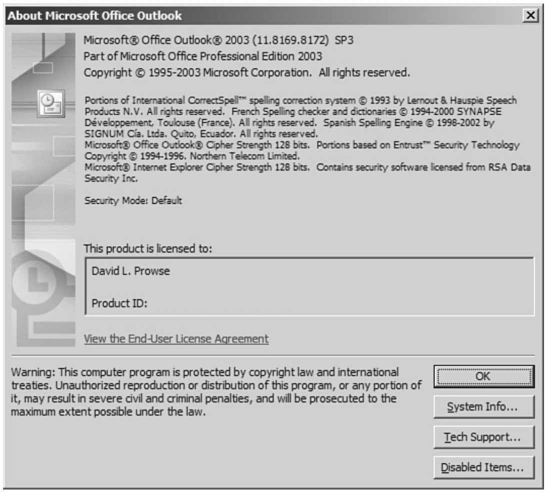
System:
Microsoft Windows XP
Professional
Version 2002

Registered to:
lamprocles
guru computer

Computer:
Intel(R) Core(TM)2 Quad CPU
Q8400 @ 2.66GHz
2.67 GHz
1.00 GB of RAM

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.



About Microsoft Office Outlook

Microsoft® Office Outlook® 2003 (11.8169.8172) SP3
Part of Microsoft Office Professional Edition 2003
Copyright © 1995-2003 Microsoft Corporation. All rights reserved.

Portions of International CorrectSpell™ spelling correction system © 1993 by Lernout & Hauspie Speech Products N.V. All rights reserved. French Spelling checker and dictionaries © 1994-2000 SYNAPSE Développement, Toulouse (France). All rights reserved. Spanish Spelling Engine © 1998-2002 by SIGNUM Cía. Ltda. Quito, Ecuador. All rights reserved.
Microsoft® Office Outlook® Cipher Strength 128 bits. Portions based on Entrust™ Security Technology Copyright © 1994-1996. Northern Telecom Limited.
Microsoft® Internet Explorer Cipher Strength 128 bits. Contains security software licensed from RSA Data Security Inc.

Security Mode: Default

This product is licensed to:

David L. Prowse

Product ID:

View the End-User License Agreement

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Figure 3-6 Microsoft 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 2011. 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 Microsoft SPs as of August 2011

Operating System	Service Pack
Windows 7	SP1
Windows Vista	SP2
Windows XP	SP3
Windows Server 2008	SP1
Windows Server 2003	SP2
Windows 2000 (Server and Professional)	SP4
Windows NT 4.0 (Server and Workstation)	SP6
Office 201	SP1
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 whether 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:

Key Topic

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

Step 2. Different OSs have different results at this point. For example, Windows 7/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, the latest version of Internet Explorer, Windows 7 SP1, or Windows 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 7/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.

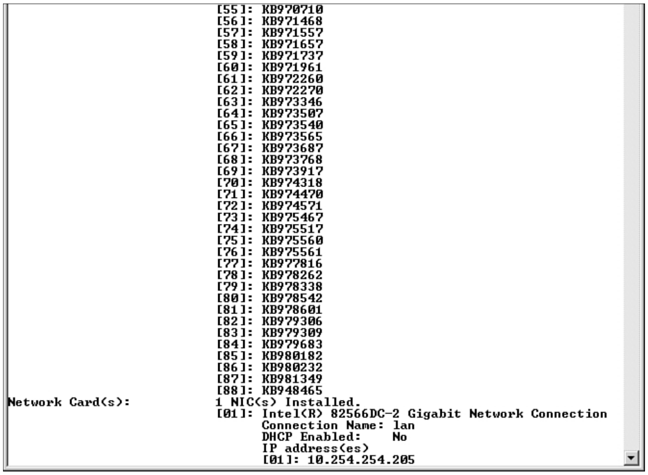
- **Download Updates but Let Me Choose Whether to Install Them**—This automatically downloads updates when they become available, but Windows prompts you to install them instead of installing them automatically. Each update has a checkbox, so you can select individual updates to install.
- **Check for Updates but Let Me Choose Whether to Download and Install Them**—This enables you 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 simply opens the Windows Update program on your 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



```
                           [55]: KB970710
                           [56]: KB971468
                           [57]: KB971557
                           [58]: KB971657
                           [59]: KB971737
                           [60]: KB971961
                           [61]: KB972260
                           [62]: KB972270
                           [63]: KB973346
                           [64]: KB973507
                           [65]: KB973540
                           [66]: KB973565
                           [67]: KB973687
                           [68]: KB973768
                           [69]: KB973917
                           [70]: KB974318
                           [71]: KB974470
                           [72]: KB974571
                           [73]: KB975467
                           [74]: KB975517
                           [75]: KB975560
                           [76]: KB975561
                           [77]: KB977816
                           [78]: KB978262
                           [79]: KB978338
                           [80]: KB978542
                           [81]: KB978601
                           [82]: KB979306
                           [83]: KB979309
                           [84]: KB979683
                           [85]: KB980182
                           [86]: KB980232
                           [87]: KB981349
                           [88]: KB948465
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82566DC-2 Gigabit Network Connection
                                 Connection Name: lan
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.254.254.205
```

Figure 3-7 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. This concept also applies to blogging applications and forums (otherwise known as bulletin boards). As new threats are discovered (and they are extremely common in the blogging world), new patch versions are released. They should be downloaded by the administrator, tested, and installed without delay. Admins should keep in touch with their software manufacturers, either through phone or e-mail, or by frequenting their web pages. This keeps the admin "in the know" when it comes to the latest updates. And this applies to server and client operating systems, server add-ons such as Microsoft Exchange or SQL Server, Office programs, web browsers, and the plethora of third-party programs that an organization might use. Your job just got a bit busier!

Of course, we are usually not concerned with updating games in the working world; they should be removed from a computer if they are found (unless perhaps 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 whether it is compatible with other systems. Microsoft Baseline Security Analyzer (MBSA) is one example of a program that can identify security misconfigurations on the computers in your network, letting you know whether patching is needed. If the patch is deemed necessary, the plan should consist of a way to test the patch in a "clean" network on clean systems, how and when the patch will be implemented, and how the patch will be checked after it is installed.

- **Testing**—Before automating the deployment of a patch among a thousand computers, it makes sense to test it on a single system or small group of systems first. These systems should be reserved for testing purposes only and should not be used by "civilians" or regular users on the network. I know, this is asking a lot, especially given the amount of resources some companies have. But the more you can push for at least a single testing system that is not a part of the main network, the less you will be to blame if a failure occurs!

- **Implementing**—If the test is successful, the patch should be deployed to all the necessary systems. In many cases this is done in the evening or over the weekend for larger updates. Patches can be deployed automatically using software such as Microsoft's 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.

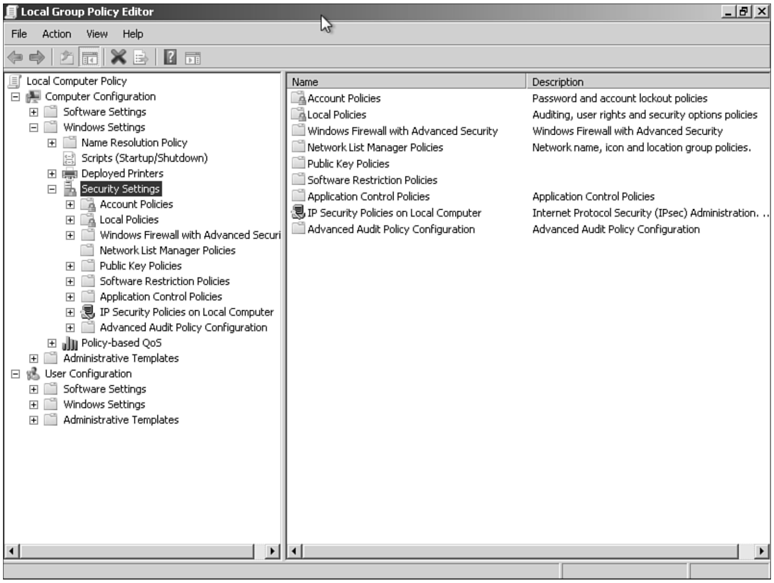
Group Policies, Security Templates, and Configuration Baselines

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 7.

Although there are many configuration changes you can make, this figure focuses on the computer's security settings that can be accessed by navigating to **Local Computer Policy > Computer Configuration > Windows Settings > Security Settings**. From here you can make changes to the password policies, for example, how long a password lasts before having to be changed, account lockout policies, public key policies, and so on. We talk about these different types of policies and the best way to apply them in future chapters. The group policy editor in the figure is known as the Local Group Policy 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 2008/2003 domain controllers that have Active Directory loaded.

Key Topic



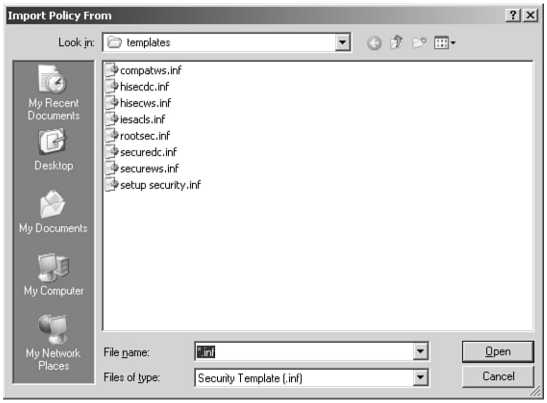
Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administration. ..
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

Figure 3-8 Local Group Policy Editor in Windows 7

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, the file securedc.inf is an information file filled with policy configurations more secure than the default you would find in a Windows Server 2003 domain controller that runs Active Directory. And 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. Server 2003 Templates are generally stored in %systemroot%\Security\templates.

There are only three default security templates in Server 2008: Defltbase.inf (uncommon), defltsv.inf (used on regular servers), and defltdc.inf (used in domain controllers). By default, these templates are stored in %systemroot%\inf. They are imported in the same manner as in Server 2003.

Key Topic



Import Policy From

Look in: templates

compatws.inf
hisecdc.inf
hisecws.inf
iesacls.inf
rootsec.inf
securedc.inf
securews.inf
setup security.inf

File name: *.inf

Files of type: Security Template (.inf)

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 many ways to measure this, but I could possibly use a protocol analyzer to find out how many packets cross through the server's network adapter. This could be run for 1 hour (during business hours of course) every day for 2 weeks. Selecting different hours for each day would add more randomness to the final results. By averaging the results together, we get a baseline. Then we can compare future measurements of the server to the baseline. This can help us to define what the standard load of our server is and the requirements our server needs on a consistent basis. It can also help when installing additional, 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 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 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 7/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 7/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, cause a decrease in performance, and pose a security threat. It is recommended that Disk Cleanup or a similar program be used. Policies can be configured (or written) to run Disk Cleanup every day or at logoff for all the computers on the network.

- **Periodically check system files**—Every once in a while it's a good idea to verify the integrity of operating system files. This can be done in the following ways:
  - With the **chkdsk** command in Windows. This checks the disk and fixes basic issues such as lost files, and some errors with the **/F** option.
  - With the **SFC** (System File Checker) command in Windows. This utility checks and if necessary replaces protected system files. It can be used to fix problems in the OS, and in other applications such as Internet Explorer. A typical command is **SFC /scannow**. Use this if **chkdsk** is not successful at making repairs.
  - With the **fsck** command in Linux. This command is used to check and repair a Linux file system. The synopsis of the syntax is **fsck [-sAVRTNP] [-C [fd]] [-t fstype] [filesys ...] [--] [fs-specific-options]**. More information about this command can be found at the corresponding MAN page: http://linux.die.net/man/8/fsck. A derivative, **e2fsck**, is used to check a Linux ext2fs (second extended file system). Also open source data integrity tools can be downloaded for Linux such as Tripwire.
- **Defragment drives**—Applications and files on hard drives become fragmented over time. For a server, this could be a disaster, because the server cannot serve requests in a timely fashion if the drive is too thoroughly fragmented. Defragmenting the drive can be done with Microsoft's Disk Defragmenter, with the command-line **defrag** command, or with other third-party programs.
- **Back up data**—Backing up data is critical for a company. It is not enough to rely on a fault tolerant array. Individual files or the entire system can be backed up to another set of hard 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 reinstalled without worrying about data loss, and applications can always be reloaded. Of course, settings should be backed up (or stored on the second drive). If a second drive isn't available, consider configuring the one hard drive as two partitions, one for the OS (or system) and one for the data. By doing this, and keeping a well-maintained computer, you are effectively hardening the OS.

Keeping a Well-Maintained Computer

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

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 whether the hard disk needs to be defragmented from once a week to once a month depending on the amount of usage. It also means creating restore points, doing Complete PC Backups, or using third-party backup or drive imaging software.

Step 7. **(Optional) Create an image of the system**—After all your configurations and hardening of the OS are complete, you might consider creating an image of the system. Imaging the system is like taking a snapshot of the entire system partition. That information is saved as one large file, or a set of compressed files that can be saved anywhere. It's kind of like system restore but at another level. The beauty of this is that you can reinstall the entire image if your system fails or is compromised, quickly and efficiently, with very little configuration necessary—only the latest security and AV updates since the image was created need be applied. Of course, most imaging software has a price tag involved, but it can be well worth it if you are concerned about the time it would take to get your system back up and running in the event of a failure. This is the basis for standardized images in many organizations. By applying mandated security configurations, updates, and so on, and then taking an image of the system, you can create a snapshot in time that you can easily revert to if necessary, while being confident that a certain level of security is already embedded into the image.

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

Many types of virtualization exist, from network and storage to hardware and software. The CompTIA Security+ exam focuses mostly on virtual machine software. The *virtual machines (VMs)* created by this software run operating systems or individual applications. These virtual OSs (also known as hosted OSs or guests) are designed to run *inside* 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. Many organizations have policies that define standardized virtual images, especially for servers. As I alluded to earlier, the main benefit of having a standardized server image is that mandated security configurations will have been made to the OS from the beginning—creating a template so to speak. This includes a defined set of security updates, service packs, patches, and so on, as dictated by organizational policy. So when you load up a new instance of the image, a lot of the configuration work will already have been done, and just the latest updates to the OS and AV software need to be applied. This image can be used in a virtual environment, or copied to a physical hard drive as well. For example, you might have a server farm that includes two physical Windows Server 2008 systems, and four virtual Windows Server 2008 systems, each running different tasks. It stands to reason that you will be working with new images from time to time as you need to replace servers or add them. By creating a standardized image once, and using it many times afterward, you can save yourself a lot of configuration time in the long run.

Virtual machines can be broken down into two categories:

- **System virtual machine**—A complete platform meant to take the place of an entire computer 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 Network 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. A common 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

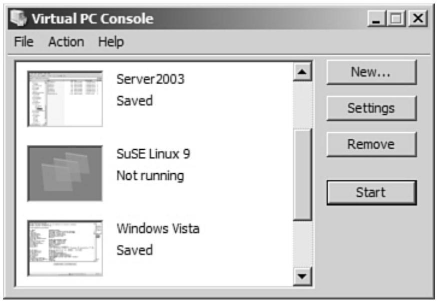


Figure 3-10 Virtual PC Console

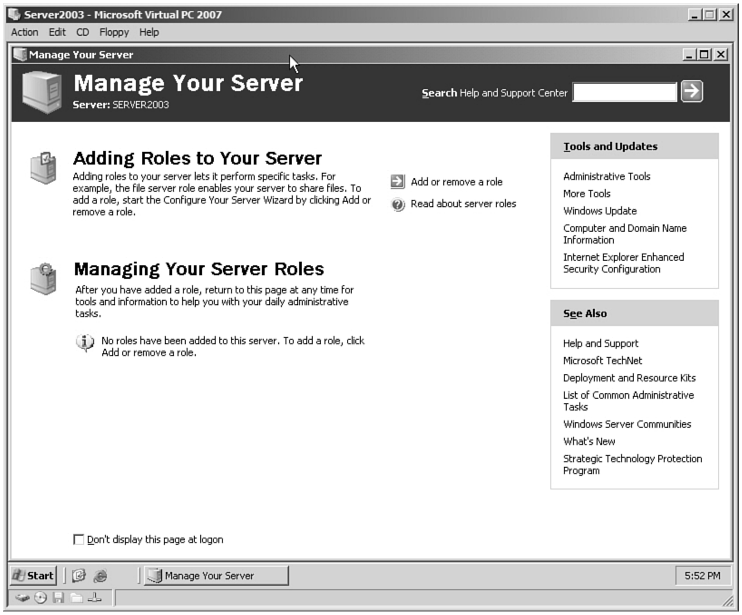
After a fresh install of Virtual PC, there won't be any virtual machines listed. However, in Figure 3-10, you can note a Windows Server 2003 VM, a SuSE Linux 9 VM, and a Windows Vista VM. Virtual software such as this allows a person to run less used or older operating systems without the need for additional physical hardware. 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 need 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, which is called "Server2003" as shown at the top of the Virtual PC software window in the title bar.

See Lab 3-2 in the "Hands-On Labs" section near the end of this chapter for a quick tutorial/lab on using Virtual PC to create a virtual machine.


Server2003 - Microsoft Virtual PC 2007
Action Edit CD Floppy Help
Manage Your Server
Manage Your Server
Server: SERVER2003
Search Help and Support Center
Add or remove a role
Read about server roles
Tools and Updates
Administrative Tools
More Tools
Windows Update
Computer and Domain Name Information
Internet Explorer Enhanced Security Configuration
See Also
Help and Support
Microsoft TechNet
Deployment and Resource Kits
List of Common Administrative Tasks
Windows Server Communities
What's New
Strategic Technology Protection Program
Start
Manage Your Server
5:52 PM

Adding Roles to Your Server

Adding roles to your server lets it perform specific tasks. For example, the file server role enables your server to share files. To add a role, start the Configure Your Server Wizard by clicking Add or remove a role.

Managing Your Server Roles

After you have added a role, return to this page at any time for tools and information to help you with your daily administrative tasks.

No roles have been added to this server. To add a role, click Add or remove a role.

☐ Don't display this page at logon

Figure 3-11 Windows Server 2003 Virtual Machine

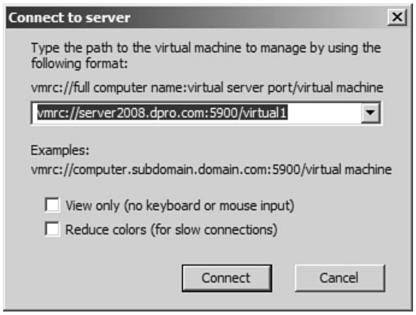
NOTE Also, if you are interested, I have demonstrations of several virtual machine OS installations at my website: www.davidlprowse.com

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 far more powerful and 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.



Connect to server

Type the path to the virtual machine to manage by using the following format:

vmrc://full computer name:virtual server port/virtual machine

vmrc://server2008.dpro.com:5900/virtual1

Examples:
vmrc://computer.subdomain.domain.com:5900/virtual machine

□ View only (no keyboard or mouse input)

□ Reduce colors (for slow connections)

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. An example of the VCenter server main management console window in VMware is shown in Figure 3-13.

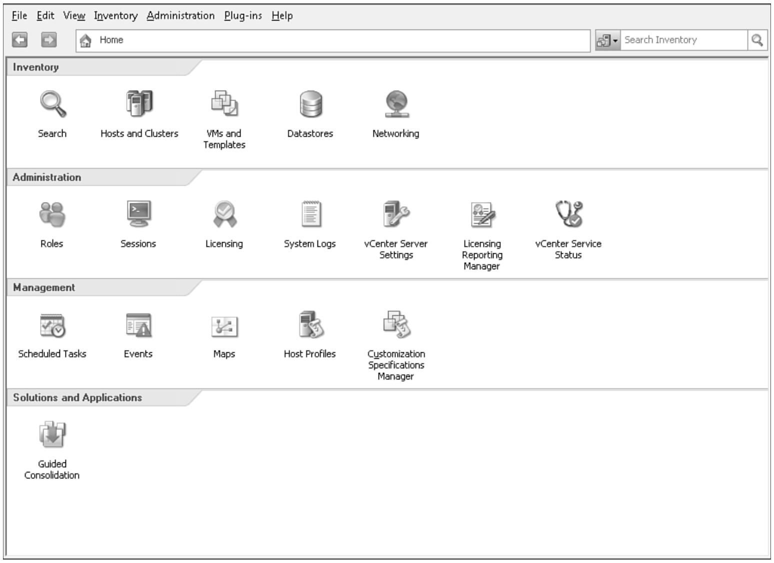


Figure 3-13 VCenter Management Console Window

Hypervisor

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

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

Generally, Type 1 is a much faster and efficient solution than Type 2. Because of this, Type 1 hypervisors are the kind used by web-hosting companies and by companies that offer cloud computing solutions such as infrastructure as a service (IaaS). It makes sense too. If you have ever run a powerful operating system such as Windows Server 2008 within a Type 2 hypervisor such as Virtual PC 2007, you will have noticed that a ton of resources are being used that are taken from the hosting operating system. It is not nearly as efficient as running the hosted OS within a Type 1 environment. However, keep in mind that the hardware/software requirements for a Type 1 hypervisor are more stringent and more costly. Because of this, some developing and testing environments use Type 2-based virtual software.

Securing Virtual Machines

In general, the security of a virtual machine operating system is the equivalent to that of a physical machine OS. The VM should be updated to the latest service pack, should have the newest AV definitions, perhaps have a personal firewall, have strong passwords, and so on. However, there are several things to watch out for that, if not addressed, could cause all your work compartmentalizing OSs to go down the drain. This includes considerations for the virtual machine OS as well as the controlling virtual machine software.

First, make sure you are using current and updated virtual machine software. Update to the latest patch or service pack for the software you are using (for example, Virtual PC 2007 SP1). Configure any security settings or options in the virtual machine software. Once this is done, you can go ahead and create your virtual machines, keeping in mind the concept of standardized imaging mentioned earlier.

Next, keep an eye out for network shares and other connections between the virtual machine and the physical machine, or between two VMs. Normally, malicious software cannot travel between a VM and another VM or a physical machine as long as they are properly separated. But if active network shares are between the two, malware could easily spread from one system to the other. If a network share is needed, map it, use it, and then disconnect it when you are finished. If you need network shares between two VMs, document what they are and which systems (and users) connect to them. Review the shares often too see whether they are still necessary. If a virtual host is attached to a NAS device or to a SAN, it is recommended to segment the storage devices off the LAN either physically, or with a secure VLAN. Regardless of where the virtual host is located, secure it with a strong firewall and disallow unprotected file transfer protocols such as FTP and Telnet.

Consider disabling any unnecessary hardware from within the virtual machine such as optical drives, USB ports, and so on. If some type of removable media is necessary, enable the device, make use of it, and then disable it immediately after finishing. Also, devices can be disabled from the virtual machine software itself. The boot priority in the virtual BIOS should also be configured so that the hard drive is booted from first, and not any removable media or network connection (unless necessary in your environment).

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

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

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

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

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

http://www.vmware.com/technical-resources/security/index.html

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

Exam Preparation Tasks

Review Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 3-2 lists a reference of these key topics and the page number on which each is found.

Table 3-2 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
Figure 3-2	Services Window in Windows XP	70
Figure 3-3	Telnet Properties Dialog Box	71
Bullet list	Stopping services in Linux	71
Figures 3-4 and 3-5 and Note	Identifying the SP level	73
Table 3-1	Latest Microsoft Service Packs	75
Step list	Windows update	76
Figure 3-7	systeminfo Command in Windows Vista	78
Bulleted list	Patch management four steps	79

Key Topic Element	Description	Page Number
Figure 3-8	Local Group Policy Editor in Windows 7	81
Figure 3-9	Import Policy from Window in Windows Server 2003	82
Numbered list	Keeping a well-maintained computer	85
Figure 3-10	Virtual PC Console	89

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, hypervisor

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 ask them at my website: www.davidlprowse.com

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 such as Windows 7 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. F rom 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 http://support.microsoft.com.

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

Watch the video solution on 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 that you want into the VM.

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 want 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 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 video solution on the DVD.

Lab 3-3: Securing a Virtual Machine

In this lab, you secure a virtual machine (VM) in Virtual PC 2007. This lab assumes that you have already downloaded and installed Virtual PC 2007, created a virtual machine, and installed an OS. This lab refers to Windows 7 Ultimate.

The steps are as follows:

Step 1. Start Virtual PC 2007 and check its SP level.

A. Access the **Control Panel** and find your list of installed programs. For example, in Windows 7 the path to this is **Control Panel > Programs > Programs & Features**.

B. If it says "Microsoft Virtual PC 2007 SP1," you can continue to Step 2. If it does not say "SP1" on the end, then continue to Step 1C.

C. Upgrade to the latest SP from the following link: www.microsoft.com/download/en/details.aspx?displaylang=en&id=24439

NOTE Be sure to fully shut down all VMs in the console. If any are in a saved state during the SP install, they could become corrupted.

NOTE It might be difficult to tell whether an SP was installed to Virtual PC 2007 (this might not be displayed in the About Virtual PC window). Aside from checking in the Control Panel, you could also attempt to create a Server 2008 virtual machine. If the Virtual PC console doesn't have Server 2008 listed as a possible option, then SP1 is not installed. If it is listed, then SP1 (at least) is installed.

Step 2. Set security options in the Virtual PC console.

- **A.** Click **File > Options**; this opens the Virtual PC Options window.
- **B.** Select **Security**.
- **C.** Select all four administrative permissions checkboxes.
- **D.** Click **OK** for the Virtual PC Options window.

Step 3. Disable unnecessary hardware within the Virtual PC console for the VM in question. For example, the sound card, COM ports, LPT ports, and floppy disks.

- **A.** Click **Action > Settings** (or simply highlight the VM and click the Settings button). This opens the Settings for %virtual machine% window where virtual machine is whatever VM you select.
- **B.** Click **Sound**. Deselect the Enable sound card checkbox.
- **C.** Disable any other unnecessary devices such as COM1, LPT1, and so on, if they are enabled and you do not need them.
- **D.** Click **OK** to close the window.

Step 4. Start the virtual machine and secure the virtual BIOS.

- **A.** Press **DEL** immediately after starting the VM. This should display the BIOS Setup Utility screen.
- **B.** Set the hard drive to first in the boot order:
  - **a.** Press the right arrow key to navigate to the Boot menu. With the Boot Device Priority option highlighted press **Enter**.
  - **b.** Modify the list so that the Hard Drive is listed first. Use the legend on the right to figure out which keys to use.
  - **c.** Press **Esc** to return to the main menu.

C. Disable removable media devices such as the floppy drive:

  a. Select the **Advanced** menu.

  b. Select **Floppy configuration**.

  c. Disable Floppy A.

  d. Press **Esc** to return to the main menu.

D. Set passwords:

  a. Select the **Security** menu.

  b. Configure a Supervisor password.

E. Press **F10** to save your settings and exit. This reboots the VM into the OS.

Step 5. Start the virtual machine and check the SP level of the OS.

A. Click **Start**. Then right-click **Computer**. This brings up the System window. If no service pack is listed, then none is installed.

B. Install the latest SP for the OS in question.

Step 6. Disable unnecessary hardware within the VM OS, such as optical drives or USB devices.

A. Click **Start**. Then right-click **Computer** and select Manage. This displays the Computer Management window.

B. Click **Device Manager**.

C. Locate the optical drive, right-click it, and select **Disable**. For some devices you might have to restart the OS.

Step 7. Remove any network sharing connections between the VM and the physical host.

A. Look for shared folders on the VM:

  a. While in the Computer Management window click **Shared Folders > Shares.**

  b. Remove any unnecessary shares by right-clicking them and selecting **Stop Sharing**. However, leave the ADMIN$, C$, and IPC$ shares alone.

  c. While in this window click on **Sessions** to see whether the computer has any unwanted outbound sessions to other computers.

  d. Close the Computer Management window.

B. Look for mapped network drives in Windows Explorer and disconnect them by right-clicking the drive and selecting **Disconnect**.

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

A. Set permissions on the folder:

a. Right-click the folder and select **Properties**.

b. Click the **Security** tab and modify permissions as you see fit. The fewer permissions the better!

c. Verify that the folder is not shared by accessing the Sharing tab.

d. Remain in the Properties window for the folder.

B. Encrypt and/or Digitally sign the VM folder:

a. Click the **General** tab; then click the **Advanced** button.

b. Select the checkbox that says **Encrypt** contents to secure data.

c. Close the Properties window.

d. Consider other encryption (or FDE) and digital signing methods from organizations such as PGP and TrueCrypt.

Watch the video solution on the DVD.

View Recommended Resources

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

- Prowse, David L. *CompTIA A+ Exam Cram*, Fifth Edition. Que Publishing. 2011.

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/
- Securing Hyper-V: http://technet.microsoft.com/en-us/library/dd569113.aspx
- Securing VMware: www.vmware.com/technical-resources/security/index.html

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. 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 7, Vista, and XP, 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 2008. Which of the following is the best answer to accomplish this?

    A. Update antivirus software.
    B. Install service packs.
    C. Disable unnecessary services.
    D. Install network intrusion detection systems.

14. You finished installing the operating system for a home user. What are three good methods to implement to secure that operating system? (Select the three best answers.)

    A. Install the latest service pack.
    B. Install a hardware- or software-based firewall.
    C. Install the latest patches.
    D. Install 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

16. Which of the following is one example of verifying new software changes on a test system?

    A. Application hardening

    B. Virtualization

    C. Patch management

    D. HIDS

17. You have been tasked with protecting an operating system from malicious software. What should you do? (Select the two best answers.)

    A. Disable the DLP.

    B. Update the HIPS signatures.

    C. Install a perimeter firewall.

    D. Disable unused services.

    E. Update the NIDS signatures.

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 7, Vista, and XP. 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.** 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.

16. **C.** Patch management is an example of verifying any new changes in software on a test system (or live systems for that matter.) Verifying the changes (testing) is the second step of the standard patch management strategy. Application hardening might include updating systems, patching them, and so on, but to be accurate, this question is looking for that particular second step of patch management. Virtualization is the creating of logical OS images within a working operating system. HIDS stands for host-based intrusion detection system, which attempts to detect malicious activity on a computer.

17. **B and D.** Updating the host-based intrusion prevention system is important. Without the latest signatures, the HIPS will not be at its best when it comes to protecting against malware. Also, disabling unused services will reduce the attack surface of the OS, which in turn makes it more difficult for attacks to access the system and run malicious code. Disabling the data leakage prevention device would not aid the situation, and it would probably cause data leakage from the computer. Installing a perimeter firewall won't block malicious software from entering the individual computer. A personal firewall would better reduce the attack surface of the computer, but it is still not meant as an antimalware tool. Updating the NIDS signatures will help the entire network, but might not help the individual computer. In this question we want to focus in on the individual computer, not the network. In fact, given the scenario of the question, you do not even know if a network exists.

Index

A

AAA (authentication, authorization, accounting), 5-6

acceptable use policies, 525

access control

authentication. *See* authentication

best practices, 310-313

physical security, 267-271

biometric readers, 270-271

building security, 267-268

door access systems, 268-270

server room security, 267-268

policies, 322-325

UAC (User Account Control), 325-326

usernames/passwords, 318-322

users, groups, permissions, 313-317

access control lists (ACLs), 154, 315

access control models, 306-313

centralized versus decentralized, 310

DAC (discretionary access control), 306-308

MAC (mandatory access control), 308-309

RBAC (role-based access control), 309-310

Account lockout threshold, 324

accounting, 6

accounts

Administrator accounts, passwords for, 321

default accounts, 234-235

guest accounts, 235

guest accounts, disabling, 321-322

restrictions, configuring, 328-330

user accounts, expiration, 314

ACK, 385

ACLs (access control lists), 154, 315

Active Directory Users and Computers (ADUC), 313-314

active fingerprinting, 347

active interception, as malware delivery method, 23

active security analysis, 347

ActiveX controls in Internet Explorer, 119-120

ad filtering, 41

add-ons

in Firefox, 124

in Internet Explorer, 119

addresses

IP addresses

public versus private, 154-156

subnetting, 162-163

IPv6 addresses, types of, 155

network socket addresses, 169

administration interface for wireless access points, 244

administrative shares, securing, 397

Administrator accounts, passwords for, 321

ADUC (Active Directory Users and Computers), 313-314

Advanced Encryption Standard (AES), 424-425

adware, 21

AES (Advanced Encryption Standard), 424-425

agents (SNMP), 388

AH (authentication header), 461

air-conditioning systems, 513-514

ALE (annualized loss expectancy), 345

alerts, 384

ALG (application-level gateway), 209

algorithms

asymmetric key algorithms, 421

Diffie-Hellman key exchange, 427

ECC, 428

RSA, 426-427

defined, 417

hashes

LANMAN hash, 433-435

MD5, 432

NTLM hash, 435

NTLM 2 hash, 435

one-time pads, 428-429

PGP, 429-430

public key cryptography, 421-422

SHA, 432

symmetric key algorithms, 420-421

AES, 424-425

DES and 3DES, 424

RC, 425

all-in-one security appliances, 215

annualized loss expectancy (ALE), 345

annualized rate of occurrence (ARO), 345

anomaly-based monitoring, 381

anonymous access control, 310

antimalware software, 8

antispyware software, 30

antivirus (AV) software, 26-30

AP isolation, 249

application firewalls, 211

Application logs, 393

application security, 124-126. *See also* browser security

disabling with policies, 138-140

secure coding concepts, 126-136

Systems Development Life Cycle (SDLC), 128-130

testing methods for, 130-132

vulnerabilities and attacks, 132-136

application-level gateway (ALG), 209

applications, removing, 68-72

archival methods, 494

armored viruses, 19

ARO (annualized rate of occurrence), 345

ARP poisoning, 184

ArpON, 184

assessing risk. *See* risks

assessments. *See* audits

asymmetric key algorithms, 421

Diffie-Hellman key exchange, 427

ECC, 428

RSA, 426-427

attack surface area, minimizing, 129

attacks. *See also* vulnerabilities

ARP poisoning, 184

brute force attacks, 361

client-side attacks, 182

cryptanalysis attacks, 361

DDoS attacks, 178

dictionary attacks, 361

DNS poisoning, 183-184

DoS attacks, 175-178

network attacks, 186, 237

null sessions, 181-182

on program code, 132-136

backdoors, 132

buffer overflows, 132-133

code injection, 133-134

directory traversal, 134

XSS and XSRF, 133

zero day attacks, 135

replay attacks, 181

session hijacking, 179-181

spoofing attacks, 178-179

TCP reset attacks, 174

transitive access, 182

audit trails, 392

audits, 389-398
of files, 389-392
log files for, 392-396, 394-396
in patch management, 80
steps in, 389
on system security settings, 396-398
authentication, 5, 8, 265
localized technologies, 273-279
IEEE 802.1X standard, 273-276
Kerberos, 277-278
LDAP, 276-277
Terminal Services, 279
methods of, 266
models for, 271-273
remote technologies, 279-286
RADIUS versus TACACS, 284-285
RAS, 280-281
VPNs, 281-284
usernames/passwords, 318-322
authentication agents (802.1X connections), 274
authentication header (AH), 461
authentication servers (802.1X connections), 274
authenticators (802.1X connections), 274
authorization, 5, 265
automated monitoring, 380
AV (antivirus) software, 26-30
availability, 5

B

backdoors, 24, 132, 237
backoffice applications, securing, 126
back-to-back perimeter DMZ, 158
backup generators, 481-483
backup plans in disaster recovery, 490-494
backup sites, 490
backups, 8, 84, 490-494
badware, 32
baiting, 519
Barracuda Networks Spam Firewall, 33
Basel I and II accords, 346
baseline reporting, 381
baselining, 82, 381-384
battery-inverter generators, 482
behavior-based monitoring, 381
Bell-La Padula access control model, 309
best practices
in access control, 310-313
passwords, 324
Biba Integrity Model access control model, 309
biometric readers, 270-271
BIOS, securing, 43-44, 51-53
birthday attacks, 432-433
BitLocker, 46-47
black book analogy (cryptography), 416-417
black hats, 9
black-box testing, 130, 350
blacklists, 34
blackouts, 479
blind hijacking, 180
block ciphers, 420
blue hats, 10
Bluejacking, 48, 251
Bluesnarfing, 48, 251
Bluetooth vulnerabilities, 48, 250-251
boot sector viruses, 19, 29-30
botnets, 25, 178
Bro, 217
broadcast storms, 385
broadcasting, 150
brownouts, 479

browser security, 110-124, 137-138

Firefox, 121-124

Internet Explorer, 116-120

proxy servers and content filters, 114-115

security policies, implementing, 111-113

user education, 114

brute force attacks, 361

buffer overflows, 132-133

building loss (disaster recovery), 495

building security, 267-268

bulletin boards, policies for, 325

butt sets, 242

C

CA (certificate authorities), 453-456

cabling

STP cables, 514

vulnerabilities, 238-244

crosstalk, 240

data emanation, 241

interference, 239

tapping into data, 241-244

CAC (Common Access Card), 269

caching proxy servers, 213

Cain & Abel password recovery tool, 360

California SB 1386, 524

CAM (Content Addressable Memory) table, 151

CAPTCHA, 325

carbon dioxide (CO2) extinguishers, 511

cardkey access systems, 269

castle analogy (network security), 205-206

CCI (co-channel interference), 240

cell phones, securing, 47-49

centralized access control, 310

certificate authorities (CA), 453-456

certificate revocation list (CRL), 454-455

certificates, 422, 452-453

dual-sided certificates, 456

revoking, 454-455

single-sided certificates, 456

validation of, 453

chain of custody, 533

change management policies, 525-526

CHAP (challenge-handshake authentication protocol), 280-281, 286

cheat sheet for exam preparation, 553

Check Point Security Appliances, 218

checklist for exam preparation, 554

chkrootkit, 33

chromatic dispersion, 243

CIA triad, 4-5, 128

cipher locks, 268

ciphers, 417. *See also* algorithms

circuit-level gateway, 209

Clark-Wilson access control model, 309

classification of data, policies concerning, 522-523

clean agent fire extinguishers, 512-513

clean machines, 29

clearing data, 531

clear-text passwords, 387-388

client-side attacks, 182

closing

pop-up windows, 114

ports, 173-174

cloud computing, securing, 159-162

clusters, 488

CO2 (carbon dioxide) extinguishers, 511

coaxial cables, 238, 241-242

co-channel interference (CCI), 240

code injection, 133-134

cold aisles, 514

cold sites, 489

collisions in hashes, 432

combustible metal fires, extinguishing, 511

command injection, 134

Common Access Card (CAC), 269

complexity of passwords, 324

computer disposal policies, 528-531

computer forensics, 533

computer security audits. *See* audits

computer telephony integration (CTI), 165

confidence tricks, 518

confidential information, sensitivity of, 523

confidentiality, 5

configuration baselines, 80-82

configuring

- BIOS, 44
- inbound filters, 223
- log files, 394
- NAT firewalls, 222
- password policies, 328-330
- proxy server connections in Firefox, 123
- RAID, 498-500
- security zones (Internet Explorer), 116-117
- user and group permissions, 330-331
- VPNs, 289-291

containment (incident response), 532

Content Addressable Memory table, 151

content filtering, 41, 153, 214

content filters in browser security, 114-115

contracts with vendors, 528

converting NTFS to FAT32, 83

cookies

- in Firefox, 121
- in Internet Explorer, 117-119
- stealing, 179

cooking oil fires, extinguishing, 511

copying files/folders, permissions for, 318

corrective security controls, 348

cracking passwords, 366-367

CRL (certificate revocation list), 454-455

cross-site request forgery (XSRF), 133

cross-site scripting (XSS), 118, 133, 181

crosstalk, 240

cryptanalysis attacks, 361

cryptographic blinding, 427

cryptographic hash functions, 431-433

cryptography. *See also* encryption

- asymmetric key algorithms, 421
  - *Diffie-Hellman key exchange, 427*
  - *ECC, 428*
  - *RSA, 426-427*
- black book analogy, 416-417
- defined, 417
- key management, 422
- public key cryptography, 421-422
- steganography, 423
- symmetric key algorithms, 420-421
  - *AES, 424-425*
  - *DES and 3DES, 424*
  - *RC, 425*
- terminology, 417-419

CTI (computer telephony integration), 165

Ctrl+Alt+Del logon, 322

D

DAC (discretionary access control), 306-308

data, separating from operating system, 28, 84-85

data backups, 8, 84, 395, 490-494

data classification policies, 522-523

data emanation, 241
Data Encryption Standard (DES), 424
data failure, avoiding with RAID, 483-486, 498-500
data leak prevention (DLP) devices, 216
data loss prevention (DLP) systems, 42, 216
data removal, 8, 531
data security. *See* security
data sensitivity policies, 522-523
data validation, 131
DDoS (Distributed Denial of Service) attacks, 178
decentralized access control, 310
decryption, 417
default accounts, 234-235
default browser, setting, 121
default configurations, securing for routers, 153
Default Domain Policy, 323
defaults, securing, 129
defense in depth, 9
defragmenting hard drives, 84
delivery methods for malware, 23-25
active interception, 23
backdoors, 24
botnets, 25
logic bombs, 24-25
privilege escalation, 24
removable media, 23
software, 23
zombies, 25
Demilitarized Zone (DMZ), 157-158
Denial of Service (DoS) attacks, 175-178
DES (Data Encryption Standard), 424
designing networks. *See* network design
destruction of computer equipment, 531
detective security controls, 348
devices. *See* network devices
dial-up connections, RAS, 280-281
dictionary attacks, 361
differential backups, 491
Diffie-Hellman encryption, 422, 427
digital forensics, 533
Digital Signature Algorithm (DSA), 428
digital signatures, 422
Directory Service log, 393
directory traversal, 134
dirty power, 480
disabling
applications with policies, 138-140
file sharing, 83
Guest accounts, 321-322
LANMAN hash storage, 433-438
services
in Linux, 71
in Mac OS X, 72
Telnet, 70-72
disaster recovery. *See also* environmental controls; redundancy planning
data backups, 490-494
incident response procedures, 531-534
planning for, 494-496
types of disasters, 494-495
disaster-tolerant disk systems, 486
discretionary access control (DAC), 306-308
disposal of equipment, policies concerning, 528-531
Distributed Denial of Service (DDoS) attacks, 178
diversion theft, 516
DLP (data loss prevention) systems, 42, 216
DMZ (Demilitarized Zone), 157-158
DNS poisoning, 183-184

DNS Server log, 393

documentation

in incident response, 532

of network, 251, 352-355

domain name kiting, 184

door access systems, 268-270

DoS (Denial of Service) attacks, 175-178

Dragon IPS, 218

drills, fire, 513

drive lock technology, 44

dry pipe systems, 512

DSA (Digital Signature Algorithm), 428

dual-sided certificates, 456

due care, 527

due diligence, 527

due process, 527

dumpster diving, 519

E

EAP (Extensible Authentication Protocol), 273-276

EAP-FAST (flexible authentication via secure tunneling) authentication, 276

EAP-MD5 authentication, 275

EAP-TLS (Transport Layer Security) authentication, 275

EAP-TTLS (Tunneled Transport Layer Security) authentication, 276

Easter eggs, 25

eavesdropping, 241, 518-519

ECC (elliptic curve cryptography), 428

electrical fires, extinguishing, 510

electromagnetic interference (EMI), 239

elite hackers, 10

elliptic curve cryptography (ECC), 428

e-mail addresses, removing from websites, 34

e-mail messages, S/MIME, 457

e-mail spam, 21-22, 33-35

emergency response detail, 532

EMI (electromagnetic interference), 239, 514-515

employee security policies. ***See*** **personnel security policies**

employee training. ***See*** **training employees**

emulators, 88

enabling

file auditing, 390

IEEE 802.1X standard, 288-289

MAC filtering, 224

packet filtering, 222

Encapsulating Security Payload (ESP), 461

encapsulation, 358

encrypting log files, 396

encryption, 8. ***See also*** **cryptography; hashes**

asymmetric key algorithms

Diffie-Hellman key exchange, 427

ECC, 428

RSA, 426-427

defined, 417

hardware security modules, 45-47

one-time pads, 428-429

PGP, 429-430

PKI, 452-456, 462-463

certificate authorities, 453-456

certificates, 452-453

dual-sided certificates, 456

single-sided certificates, 456

web of trust, 456

security protocols

IPsec, 460-461

L2TP, 460

PPTP, 460
S/MIME, 457
SSH, 459, 463-464
SSL/TLS, 458-459
of smartphone data, 48
symmetric key algorithms
AES, 424-425
DES and 3DES, 424
RC, 425
website encryption notification, 114
whole disk encryption, 45-47, 84
on wireless access points, 246-247
endpoint-based DLP (data loss prevention), 42, 216
Enterasys, 217-218
environmental controls, 510-515
fire suppression, 510-513
fire extinguishers, 510-512
hazard protection systems, 512-513
sprinkler systems, 512
HVAC, 513-514
shielding, 514-515
equipment disposal policies, 528-531
eradication (incident response), 532
error handling, securing, 129
ESP (Encapsulating Security Payload), 461
Ethereal. *See* Wireshark
events, incidents versus, 531-532
evidence gathering (incident response), 532
evidence preservation (incident response), 533
Evil Maid Attack, 21
evil twin wireless access points, 246
exam preparation
cheat sheet, 553
checklist, 554
Security+ certification requirements, 552
tips for, 553-558
Excel, securing, 127
expiration of user accounts, 314
Extensible Authentication Protocol (EAP), 273-276
external security testing, 350
extranets, securing, 159-160
extrusion prevention systems, 216

F

fail-closed, 477
fail-open, 152, 477
fail-over clusters, 488
fail-over redundancy, 477
failure of power supplies, 479
failure-resistant disk systems, 486
failure-tolerant disk systems, 486
false negatives, 39, 219, 272
false positives, 39, 219, 272
far end crosstalk (FEXT), 240
Faraday cages, 241, 514
FAT32, converting to NTFS, 83
FEXT (far end crosstalk), 240
fiber-optic cables, 238, 243
File Replication Service log, 393
file sharing, disabling, 83
file systems, hardening, 82-85
files
auditing, 389-392
moving/copying, permissions, 318
FileZilla, 172
filtering
ad filtering, 41
content filtering, 41
filters in browser security, 114-115
fingerprinting, 347
fire drills, 513
fire extinguishers, 510-512
class A, 510
class B, 510

class C, 510
class D, 511
class K, 511
fire suppression, 510-513
fire extinguishers, 510-512
hazard protection systems, 512-513
sprinkler systems, 512
Firefox
Internet Explorer versus, 110-111
securing, 121-124
fires (disaster recovery), 494
firewall logs, 393-394
firewalls, 27-28, 206-212
configuring inbound filters, 223
enabling MAC filtering, 224
NAT firewalls, configuring, 222
personal firewalls, 35-38
for router security, 153
first responders, 532
flammable liquid/gas fires, extinguishing, 510
Flash scripts in Internet Explorer, 120
flashing the BIOS, 44
flood attacks, 175-177
floods (disaster recovery), 494
Fluke Networks, 359
folders, moving/copying, 318
fork bomb attacks, 177
Fraggle attacks, 176
FreeBSD, 308
FreeNAC, 162
FTP connections
ports and protocols for, 169-172
securing, 174-175
FTPS (FTP Secure), 174
full backups, 490
fuzzing, 131

G

gaseous fire suppression systems, 512-513
generators. *See* backup generators
Gnutella, 210
GPS tracking of smartphones, 48
Gramm-Leach-Bliley Act, 524
grandfather-father-son backup rotation method, 493
gray hats, 10
gray-box testing, 130, 350
grayware, 21
GRC's ShieldsUP!, 173, 208
green hats, 10
group policies, 80-82
groups
in access control, 313-317
permissions, configuring, 330-331
guessing passwords, 361
guest accounts, 235, 321-322

H

hackers, types of, 9-10
Halon extinguishers, 512
handheld devices, protocol analyzers, 359
handheld fire extinguishers. *See* fire extinguishers
hands-on labs
applications, disabling with policies, 138-140
BIOS, securing, 51-53
browsers, securing, 137-138
IEEE 802.1X standard, enabling, 288-289
inbound filters, configuring, 223
LANMAN hash, disabling, 437-438
MAC filtering, enabling, 224
malware, scanning for, 50-51

NAT firewalls, configuring, 222
network mapping, 365
packet filtering, enabling, 222
password cracking, 366-367
password policies and user account restrictions, configuring, 328-330
PKI (public key infrastructure), 462-463
ports, scanning, 190-191
protocol analyzers, 401-403
RAID, configuring, 498-500
service packs, updating, 96
SSH connections, 463-464
user and group permissions, configuring, 330-331
virtual machines, creating in Virtual PC 2007, 96-98
virtual machines, securing, 98-101
VPNs, configuring, 289-291
wardriving, 256
wireless access points, securing, 254-256

hard drives
defragmenting, 84
hardening, 82-85
sanitizing, 530-531

hardening operating systems, 68-85
file systems and hard drives, 82-85
with group policies, security templates, configuration baselines, 80-82
installing service packs, 72-75
installing updates, patches, hotfixes, 75-80
maintenance, 85-86
removing applications and services, 68-72

hardware security modules (HSMs), 45-47

hashes, 430-431
cryptographic hash functions, 431-433
password hash functions, 433-435

hazard protection systems, 512-513

HDD passwords, 44

header manipulation, 385

Health Insurance Portability and Accountability Act (HIPAA), 524

HICCUPS system (Hidden Communication System for Corrupted Networks), 423

hidden files/folders, 83

hidden shares, securing, 397

hiding protected system files, 83

HIDS (host-based intrusion detection systems), 35, 38-40

high-availability clusters, 488

HIPAA (Health Insurance Portability and Accountability Act), 524

hoaxes, 518

honeyfarms, 215

honeynets, 215-216

honeypots, 215-216

horizontal privilege escalation, 236

host-based intrusion detection systems (HIDS), 35, 38-40

hosted hypervisors, 92

hosts file attacks, 183

hot aisles, 514

hot sites, 489

hotfixes, installing, 75-80

HouseCall, 29

HSMs (hardware security modules), 45-47

HTTP connections, ports and protocols for, 172

HTTP proxy servers, 213. *See also* proxy servers

HTTPS (Hypertext Transfer Protocol Secure), 459

hubs, securing, 150-151

humidity controls, 513

HVAC shielding, 514

HVAC systems, 513-514

hybrid cryptosystems, 429

Hypertext Transfer Protocol Secure (HTTPS), 459

Hyper-V, 94

hypervisors, 92

I

IA (information assurance), 342

IaaS (Infrastructure as a Service), 161

ICMP flood attacks, 175

identification, 265, 532

identity proofing, 266

IDS (intrusion detection systems), 35, 38-40, 217-218

IE. *See* Internet Explorer

IEEE 802.1Q standard, 164

IEEE 802.1X standard, 162, 249, 273-276, 286-289

ILP (information leak prevention) devices, 216

IM spam, 22

impact assessment, 343

impersonation, 516

implementing in patch management, 79

implicit deny, 173, 310-311

inbound filters, configuring, 223

inbound ports, 169

incident response procedures, 531-534

incremental backups, 490

information assurance (IA), 342

information leak prevention (ILP) devices, 216

information security. *See* security

Infrastructure as a Service (IaaS), 161

inheritance of permissions, 317

initialization in 802.1X authentication, 275

initiation in 802.1X authentication, 275

input validation, 131

installing

- Network Monitor for Server 2003, 402
- service packs, 72-75
- service packs and updates, 26-27
- updates, patches, hotfixes, 75-80

instant messaging programs, 68

integrity, 5

interconnections in network design, 156-162

- cloud computing, 159-162
- DMZ, 157-158
- Internet, 157
- intranets/extranets, 159-160
- LANs versus WANs, 157

interference, 239, 514-515

internal information, sensitivity of, 523

Internet

- content filtering, 214
- in network security, 157

Internet Explorer

- Firefox versus, 110-111
- securing, 116-120
- security policies, implementing, 111-113
- security settings, 30

Internet Optimizer, 21

Internet Protocol Security (IPsec), 460-461

intranets, securing, 159-160

intrusion detection systems (IDS), 35, 38-40, 217-218

intrusion prevention systems (IPS), 40

- NIPS, 218-219
- for router security, 153

investigation (incident response), 532

IP addresses

- public versus private, 154-156
- spoofing, 179
- subnetting, 162-163

IP masquerading, 154

IP proxy servers, 213

ipfirewall, 37

IPS (intrusion prevention systems), 40

NIPS, 218-219

for router security, 153

IPsec (Internet Protocol Security), 460-461

IPv6 addresses, types of, 155

Ironkey, 45

ISO/IEC 27002:2005 standard, 523, 533

isolation mode, 249

ISP (Internet service providers), redundancy planning, 488

IT security audits. *See* audits

IV attacks, 250

J–K

job rotation, 312, 526

Kerberos, 277-278, 286, 420

key algorithms. *See* algorithms

key escrow, 455

key generators, 20

key management, 422

keys, defined, 419

kitchen fires, extinguishing, 511

L

L2TP (Layer 2 Tunneling Protocol), 282, 460

label-based access control, 309

LACK (Lost Audio Packets Steganography), 423

LAN Surveyor, 352

LANMAN hash, 433-438

LANs, WANs versus, 157

lattice-based access control, 309

Layer 2 Tunneling Protocol (L2TP), 282, 460

LDAP (Lightweight Directory Access Protocol), 276-277, 286

LDAP injection, 134

LEAP (Lightweight EAP), 276

least privilege, 311-312, 317

legislative policies. *See* policies

length of passwords, 324

Lightweight Directory Access Protocol (LDAP), 276-277, 286

Lightweight EAP (LEAP), 276

line conditioners, 480

Linux, disabling services in, 71

load-balancing clusters, 488

local area networks (LANs), wide area networks (WANs) versus, 157

localized authentication technologies, 273-279

IEEE 802.1X standard, 273-276

Kerberos, 277-278

LDAP, 276-277

Terminal Services, 279

locking computers, 325

logic bombs, 24-25

logon process, locking computers, 325

logs

for audits, 392-396, 394-396

firewall logs, 210

security logs in file auditing, 390

long-term power loss (disaster recovery), 495

Lost Audio Packets Steganography (LACK), 423

Love Bug virus, 19

M

MAC (mandatory access control), 308-309

address spoofing, 179

filtering, 211, 224

flooding, 151

Mac OS X, disabling services in, 72
macro viruses, 19
maintenance in hardening operating systems, 85-86
maintenance phase (SDLC), 129
maintenance release, 78
malicious attacks (disaster recovery), 495
malware, 6, 18-36
  delivery methods for, 23-25
    active interception, 23
    backdoors, 24
    botnets, 25
    logic bombs, 24-25
    privilege escalation, 24
    removable media, 23
    software, 23
    zombies, 25
  preventing and troubleshooting, 26-36
    rootkits, 32-33
    spam, 33-35
    spyware, 30-32
    viruses, 26-30
    worms and Trojan horses, 30
  rootkits, 21
  scanning for, 50-51
  spam, 21-22
  spyware, 21
  Trojan horses, 20
  viruses, 18-19
  worms, 19-20
managed devices, 388
management security controls, 348
mandatory access control (MAC). ***See*** **MAC (mandatory access control)**
Mandatory Security Policy, 308
mandatory vacation policies, 526-527
man-in-the-middle attacks, 178, 180
mantraps, 270, 519
manual monitoring, 380
many-to-one mapping, 455
mapping the network, 352-355, 365
McAfee IntruShield, 218
MD5 (Message-Digest algorithm 5), 432
message authentication code, 421
message digests, 430
Message-Digest algorithm 5 (MD5), 432
metal fires, extinguishing, 511
Microsoft Sysinternals Rootkit Revealer, 33
Microsoft Update, 77
Microsoft Virtual PC, 88-90
Microsoft Virtual Server, 90
Microsoft Windows XP Mode, 90
minimal privilege, 317
minimizing attack surface area, 129
mining log files, 394
MITM. ***See*** **man-in-the-middle attacks**
modems, securing, 166
monitoring
  in incident response, 532
  in intrusion detection, 39
  methdologies for, 380-382
    anomaly-based monitoring, 381
    behavior-based monitoring, 381
    signature-based monitoring, 380-381
  tools for
    Network Monitor, 386-388
    performance baselining, 381-384
    protocol analyzers, 384-388
    SNMP, 388
    Wireshark, 385-386
moving files/folders, permissions for, 318
MS-CHAP, 280-281
multifactor authentication, 272
multihomed connections, 211
multipartite viruses, 19
mutual authentication, 277

N

NAC (Network Access Control), 162

NAS (network attached storage), securing, 45

NAT (network address translation), 154-156

NAT filtering, 209

NAT firewalls, configuring, 222

National Cyber Alert System website, 48

native hypervisors, 92

near end crosstalk (NEXT), 240

negotiation in 802.1X authentication, 275

Nessus, 355-356

netmon. *See* Network Monitor

netstat command, 358

Network Access Control (NAC), 162

network address translation (NAT), 154-156

network attached storage (NAS), securing, 45

network attacks, 237

network connections, redundancy planning, 486-488

network design, 150-167

- interconnections, 156-162
  - *cloud computing, 159-162*
  - *DMZ, 157-158*
  - *Internet, 157*
  - *intranets/extranets, 159-160*
  - *LANs versus WANs, 157*
- NAC, 162
- NAT, 154-156
- network devices, 150-154
  - *hubs, 150-151*
  - *routers, 152-154*
  - *switches, 151-152*
- subnetting, 162-163
- telephony devices, 165
  - *modems, 166*
  - *PBX equipment, 166-167*
  - *VoIP, 167*
- VLAN, 164-165

network devices, 150-154

- hubs, 150-151
- routers, 152-154
- switches, 151-152
- vulnerabilities, 234-238
  - *backdoors, 237*
  - *default accounts, 234-235*
  - *network attacks, 237*
  - *privilege escalation, 236-237*
  - *weak passwords, 235-236*

network DLP systems, 42

network intrusion detection systems (NIDS), 38, 217-219

network intrusion prevention system (NIPS), 218-219

Network Magic, 353

network management system (NMS), 388

network mapping, 352-355, 365

network masquerading, 154

Network Monitor, 386-388

Network Monitor for Server 2003, installing, 402

Network Monitor for Server 2008, 402

network monitoring

- in incident response, 532
- in intrusion detection, 39
- methdologies for, 380-382
  - *anomaly-based monitoring, 381*
  - *behavior-based monitoring, 381*
  - *signature-based monitoring, 380-381*
- tools for
  - *Network Monitor, 386-388*
  - *performance baselining, 381-384*
  - *protocol analyzers, 384-388*

SNMP, 388

Wireshark, 385-386

network perimeter, 205-206

network security

ARP poisoning, 184

attacks, list of, 186

castle analogy, 205-206

client-side attacks, 182

data loss prevention systems, 216

DDoS attacks, 178

DNS poisoning, 183-184

DoS attacks, 175-178

firewalls, 206-212

honeypots and honeynets, 215-216

network design. *See* network design

network documentation, 251

NIDS, 217-218

NIPS, 218-219

null sessions, 181-182

ports and protocols, 167-175

protocol analyzers, 220

proxy servers, 212-215

replay attacks, 181

session hijacking, 179-181

spoofing attacks, 178-179

transitive access, 182

wired networks, 234-244

cable vulnerabilities, 238-244

device vulnerabilities, 234-238

wireless network security, 244-251

Bluetooth vulnerabilities, 250-251

wireless access point vulnerabilities, 244-249

wireless access points, securing, 254-256

wireless transmission vulnerabilities, 250

network sniffers. *See* protocol analyzers

network socket addresses, 169

network-based DLP (data loss prevention), 216

network-based firewalls. *See* firewalls

NEXT (near end crosstalk), 240

NIDS (network intrusion detection systems), 38, 217-219

Nimda worm, 20

NIPS (network intrusion prevention system), 218-219

NIST penetration testing, 351

Nmap, 173, 208, 356-357

NMS (network management system), 388

nonpromiscuous mode, 385

nonrepudiation, 6, 391

NOOP sleds, 132

NOP slides, 132

NoScript, 124

NTFS

converting FAT32 to, 83

permissions, 316

NTLM hash, 435

NTLM 2 hash, 435

null sessions, 181-182

O

one-time pads, 428-429

one-to-one mapping, 154, 455

one-way functions, 431

online scanners, 29

open mail relays, 34

open ports on twisted-pair cables, 243

Open Source Security Testing Methodology Manual (OSSTMM), 350

Open Vulnerability and Assessment Language (OVAL), 351

operating systems

fingerprinting, 347

hardening, 68-85

file systems and hard drives, 82-85

with group policies, security templates, configuration baselines, 80-82 *installing service packs, 72-75*

installing updates, patches, hotfixes, 75-80

maintenance, 85-86

removing applications and services, 68-72

separating from data, 28, 84-85

operational security controls, 348

optical splitters, 243

The Orange Book, 306, 308

organizational policies. *See* policies

OS. *See* operating systems

OSI model, 152

OSSTMM (Open Source Security Testing Methodology Manual), 350

outbound ports, 169

Outlook, securing, 127

OVAL (Open Vulnerability and Assessment Language), 351

P

PaaS (Platform as a Service), 161

packet filtering, 208, 222

packet sniffers. *See* protocol analyzers

PacketFence, 162

padding schemes in RSA encryption, 427

PAP, 280

passive fingerprinting, 347

passive security analysis, 347

password analysis, 359-362, 366-367

password crackers, 360

password hash functions, 433-435

passwords

in access control, 318-322

best practices, 324

BIOS passwords, 43-44

clear-text passwords, 387-388

complexity and length of, 324

frequency of changes, 321

guessing, 361

HDD passwords, 44

policies for, 322-325, 328-330

storing in web browsers, 122

strong passwords, 319-321

weak versus strong passwords, 235-236

PAT (port address translation), 154

patches

installing, 75-80

management, 79-80

versions, 78

PBX (private branch exchange) equipment, securing, 166-167

PDAs, securing, 47-49

PDoS (permanent DoS) attacks, 177

PEAP (protected extensible authentication protocol), 276

penetration tests, 130, 350-351

performance baselining, 381-384

Performance Monitor tool, 383-384

permanent DoS (PDoS) attacks, 177

permanently installed generators, 482

permissions, 313-317

auditing, 397

inheritance and propagation, 317

types of, 316

user and group permissions, configuring, 330-331

when moving/copying files and folders, 318

personal firewalls, 35-38

Personal Identity Verification (PIV) card, 269

personally identifiable information (PII), 528

personnel security policies, 523-525

acceptable use, 525

change management, 525-526

due care, 527

due diligence, 527

due process, 527

mandatory vacations, 526-527
separation of duties, 526
training employees, 527-528
types of, 528

PGP (Pretty Good Privacy), 429-430

Phage virus, 28

pharming attacks, 184

phishing, 178, 516-518

Phlashing, 177

phone cloning, 48

physical security, 267-271
biometric readers, 270-271
building security, 267-268
door access systems, 268-270
server room security, 267-268
of switches, 152

piggybacking, 519

PII (personally identifiable information), 528

ping flood attacks, 175

ping of death (POD) attacks, 177

PIV card (Personal Identity Verification), 269

PKCS (public key cryptography standards), 427

PKI (Public Key Infrastructure), 422, 452-456, 462-463
certificate authorities, 453-456
certificates, 452-453
dual-sided certificates, 456
single-sided certificates, 456
web of trust, 456

planning
for disaster recovery, 494-496
in patch management, 79
security plans, 7

Platform as a Service (PaaS), 161

PNAC (port-based Network Access Control), 162

POD (ping of death) attacks, 177

point release, 78

Point-to-Point Tunneling Protocol (PPTP), 282, 460

policies. *See also* procedures
for access control, 322-325
in application security, 124-125
auditing, 398
for browsers, implementing, 111-113
configuring, 328-330
data sensitivity and classification, 522-523
disabling applications with, 138-140
in disaster recovery plans, 495-496
equipment disposal, 528-531
example of, 521
group policies, 80-82
personnel security policies, 523-525
acceptable use, 525
change management, 525-526
due care, 527
due diligence, 527
due process, 527
mandatory vacations, 526-527
separation of duties, 526
training employees, 527-528
types of, 528
privacy policies, 525
vendor contracts, 528

polymorphic viruses, 19

POP3 connections, ports and protocols for, 173

pop-up blockers, 35, 40-42
in Firefox, 124
in Internet Explorer, 119

pop-up windows, closing, 114

port address translation (PAT), 154

port forwarding, 208

port scanning, 173, 356-357

port zero, securing, 174

portable gas-engine generators, 482

port-based Network Access Control (PNAC), 162

ports

- closing, 173-174
- inbound ports, 169
- outbound ports, 169
- protocol associations, list of, 170-169
- range of, 167
- scanning, 190-191
- securing, 167-175

power supplies

- failure of, 479
- redundancy planning, 478-483
  - *backup generators, 481-483*
  - *redundant power supplies, 479-480*
  - *UPS, 480-481*

PPTP (Point-to-Point Tunneling Protocol), 282, 460

pre-action sprinkler systems, 512

precomputation, 361

preparing for exam. *See* exam preparation

preservation of evidence (incident response), 533

pretexting, 516

Pretty Good Privacy (PGP), 429-430

preventing

- BIOS attacks, 43-44
- malware, 26-36
  - *rootkits, 32-33*
  - *spam, 33-35*
  - *spyware, 30-32*
  - *viruses, 26-30*
  - *worms and Trojan horses, 30*

preventive security controls, 348

previous logon notification, 325

principle of defense in depth, 129

principle of least privilege, 129

Privacy Act of 1974, 523, 525

privacy policies, 525

private addresses, public addresses versus, 154-156

private branch exchange (PBX) equipment, securing, 166-167

private keys, defined, 419

private-key algorithms. *See* symmetric key algorithms

privilege de-escalation, 237

privilege escalation, 24, 236-237

procedures, 531-534. *See also* policies

process virtual machines, 87

program viruses, 19

programming, securing. *See* secure coding concepts

programs. *See* applications

promiscuous mode, 217, 385

propagation of permissions, 317

protected extensible authentication protocol (PEAP), 276

protected system files, hiding, 83

protocol analyzers, 150, 220, 358-359, 384-388, 401-403

- Network Monitor, 386-388
- SNMP, 388
- Wireshark, 385-386

protocol associations, list of, 170-169

protocols

- FTP, securing, 174-175
- securing, 167-175
- wireless protocols, 246

proximity sensors, 269

proximity-based door access systems, 270

proxy servers, 212-215

- for browser security, 114-115
- configuring connections in Firefox, 123

public addresses, private addresses versus, 154-156

public information, sensitivity of, 523

public key cryptography, 421-422

public key cryptography standards (PKCS), 427

Public Key Infrastructure (PKI), 422, 452-456, 462-463

certificate authorities, 453-456

certificates, 452-453

dual-sided certificates, 456

single-sided certificates, 456

web of trust, 456

public keys, defined, 419

punch block connections, 242

Pure-FTPd, 172

purging data, 531

Q–R

qualitative risk assessments, 344

quantitative risk assessments, 344-346

RA (registration authority), 455

radio frequency interference (RFI), 239

RADIUS (Remote Authentication Dial-In User Service), 284-286

RAID (redundant array of independent disks), 483-486, 498-500

Rainbow Tables, 361

RAS (Remote Access Service), 280-281, 286

RATs (remote access Trojans), 20

raw socket programming, 174

RBAC (role-based access control), 309-310

RC (Rivest Cipher), 425

RC4, 425

RC5, 425

RC6, 425

Real-time Transport Protocol (RTP), 169

recovery (incident response), 532. *See also* disaster recovery

recycling computers, policies concerning, 528-531

The Red Book, 306

reduced sign-on, 272

redundancy planning, 476-490. *See also* disaster recovery

network connections, 486-488

power supplies, 478-483

backup generators, 481-483

redundant power supplies, 479-480

UPS, 480-481

RAID, 483-486, 498-500

servers, 488-489

single points of failure, 476

sites, 489-490

redundant array of independent disks (RAID), 483-486, 498-500

redundant ISP, 488

redundant power supplies, 479-480

registration authority (RA), 455

Remote Access Service (RAS), 280-281, 286

remote access Trojans (RATs), 20

Remote Authentication Dial-In User Service (RADIUS), 284-286

remote authentication technologies, 279-286

RADIUS versus TACACS, 284-285

RAS, 280-281

VPNs, 281-284

remote ports, 238

remote wipe programs, 48

removable media

as malware delivery method, 23

securing, 44-45

removing. *See also* data removal

applications and services, 68-72

e-mail addresses from websites, 34

temporary files, 83, 119

web browsers, 120

replay attacks, 181
requirements for Security+ certification, 552
residual risk, 343
restoration for backup tapes, 492
restore points, 84
restrictions on user accounts, configuring, 328-330
revoking certificates, 454-455
RFI (radio frequency interference), 239
risks, 342-343
 acceptance, 343
 assessments, 342-351
  qualitative risk assessments, 344
  quantitative risk assessments, 344-346
  security analysis methodologies, 346-347
  security controls, 347-349
  vulnerability management, 349-351
 avoidance, 342
 management, 342
 mitigation, 344
 reduction, 343
 retention, 343
 sharing, 342
 transference, 342
Rivest Cipher (RC), 425
rogue wireless access points, 245-246
role-based access control (RBAC), 309-310
rootkits, 21, 32-33
rotation schemes for backups, 492-493
routers, securing, 152-154
Routing and Remote Access Service (RRAS), 283
RRAS (Routing and Remote Access Service), 283
RSA (Rivest, Shamir, Adleman) encryption, 426-427
RTP (Real-time Transport Protocol), 169
rule-based access control, 309

S

SA (security association), 461
SaaS (Software as a Service), 161
safety. *See* environmental controls
sags, 479
salting, 361
sandboxes, 130
sanitizing
 hard drives, 530-531
 smartphones, 48
Sarbanes-Oxley Act (SOX), 523
saving log files, 394
SCA (side channel attacks), 428
scanning
 for malware, 50-51
 network, 365
 ports, 173, 190-191, 356-357
 for vulnerabilities, 355-358
SCP (Secure copy), 175
SDLC (Systems Development Life Cycle), 128-130
secret information, sensitivity of, 523
secret-key encryption, 417. *See also* symmetric key algorithms
secure code reviews, 128
secure coding concepts, 126-136
 Systems Development Life Cycle (SDLC), 128-130
 testing methods for, 130-132
 vulnerabilities and attacks, 132-136
  backdoors, 132
  buffer overflows, 132-133
  code injection, 133-134
  directory traversal, 134
  XSS and XSRF, 133
  zero day attacks, 135

Secure copy (SCP), 175

Secure FTP (SFTP), 174

Secure Hash Algorithm (SHA), 432

Secure HTTP (SHTTP), 459

Secure LDAP, 277

secure padding schemes in RSA encryption, 427

Secure Shell (SSH), 459, 463-464

Secure Sockets Layer (SSL), 458-459

- certificates, 454
- settings in Internet Explorer, 119

Secure/Multipurpose Internet Mail Extensions (S/MIME), 457

security

- AAA (authentication, authorization, accounting), 5-6
- access control. *See* access control
- application security, 124-126, 138-140
- authentication models, 271-273
- of BIOS, 43-44, 51-53
- browser security. *See* browser security
- of cell phones and PDAs, 47-49
- CIA triad, 4-5
- of log files, 396
- network design. *See* network design
- network security. *See* network security
- physical security. *See* physical security
- plans, 7
- policies. *See* policies
- protocols
  - *IPsec, 460-461*
  - *L2TP, 460*
  - *PPTP, 460*
  - *S/MIME, 457*
  - *SSH, 459, 463-464*
  - *SSL/TLS, 458-459*
- risk assessments. *See* risks
- secure coding concepts. *See* secure coding concepts
- of storage devices. *See* storage devices
- technologies. *See* technologies
- templates, 80-82
- threats
  - *malware, 18-36*
  - *types of, 6-7*
- of virtual machines, 92-94, 98-101
- wired network security. *See* wired network security
- wireless network security. *See* wireless network security

security analysis methodologies, 346-347

security association (SA), 461

security audits. *See* audits

security controls, 347-349

security logs, 390, 392

security permissions, 316. *See also* permissions

Security Posture Assessments (SPA), 381

security settings (Internet Explorer), 30

security tokens, 269

security zones (Internet Explorer), configuring, 116-117

Security+ certification requirements, 552

SELinux (Security-Enhanced Linux), 40, 308

sensitivity of data, policies concerning, 522-523

separating data and operating system, 28, 84-85

Separation of Duties (SoD), 312, 526

server room security, 267-268

servers, redundancy planning, 488-489

service level agreement (SLA), 528

service packs

- installing, 26-27, 72-75
- services versus, 72
- updating, 96

Service Set Identifier (SSID) broadcasting, 211, 245

services

removing, 68-72

service packs versus, 72

session cookies, 119

session hijacking, 179-181

Session Initiation Protocol (SIP), 167

session theft, 179

session-key algorithms. *See* symmetric key algorithms

SFTP (Secure FTP), 174

SHA (Secure Hash Algorithm), 432

shared folders, auditing, 396-397

shared-key algorithms. *See* symmetric key algorithms

sharing

files, disabling, 83

permissions, 316

risk, 342

shielded twisted pair (STP) cables, 240, 514

shielding, 514-515

ShieldsUP!, 173, 208

shoulder surfing, 518

SHTTP (Secure HTTP), 459

side channel attacks (SCA), 428

signal emanation, 241

signature-based monitoring, 39, 380-381

SIM cloning, 48

Simple Network Management Protocol (SNMP), 388

single loss expectancy (SLE), 344

single points of failure, 476

single sign-on (SSO), 272

single-key algorithms. *See* symmetric key algorithms

single-sided certificates, 456

SIP (Session Initiation Protocol), 167

sites, redundancy planning, 489-490

SLA (service level agreement), 528

SLE (single loss expectancy), 344

slipstreaming, 74

smart cards, 269

smartphones, theft of, 48-49

S/MIME (Secure/Multipurpose Internet Mail Extensions), 457

SMTP open relays, 34

SMTP relay, 181

Smurf attacks, 176

SNMP (Simple Network Management Protocol), 388

Snort, 217, 218

social engineering, 7, 515-521

baiting, 519

diversion theft, 516

dumpster diving, 519

eavesdropping, 518-519

hoaxes, 518

phishing, 516-518

piggybacking, 519

pretexting, 516

shoulder surfing, 518

training employees against, 520-521

types of, 519

SoD (Separation of Duties), 312, 526

Software as a Service (SaaS), 161

software as malware delivery method, 23

software versions, explained, 78

SOX (Sarbanes-Oxley) Act, 523

SP. *See* service packs

SPA (Security Posture Assessments), 381

spam, 21-22, 33-35

spam filters, 33-34

spam honeypots, 215

SPAP, 280

spear phishing, 517

spectral analyzers, 243

SPI (stateful packet inspection), 208
spikes, 478
spim, 22
splitting
fiber-optic cables, 243
twisted-pair cable wires, 243
spoofing attacks, 178-179
sprinkler systems, 512
spyware, 21
preventing and troubleshooting, 30-32
symptoms of, 31
SQL injection, 133
SSH (Secure Shell), 459, 463-464
SSH FTP, 174
SSID (Service Set Identifier) broadcasting, 211, 245
SSL (Secure Sockets Layer), 458-459
certificates, 454
settings in Internet Explorer, 119
SSO (single sign-on), 272
standard load, 383
standby generators, 482
stateful packet inspection (SPI), 208
stateless packet inspection, 208
static NAT (network address translation), 154
statistical anomaly-based monitoring, 39, 381
stealth viruses, 19
steganography, 423
storage devices
hardware security modules, 45-47
network attached storage, securing, 45
removable media, securing, 44-45
whole disk encryption, 45-47
storage-based DLP (data loss prevention), 42, 216
STP (shielded twisted pair) cables, 240, 514
stream ciphers, 420
strong passwords, 235-236, 319-321
subnetting, 162-163
subversion errors, 219
supplicants (802.1X connections), 274
surges, 478
switches, securing, 151-152
symmetric key algorithms, 420-421
AES, 424-425
DES and 3DES, 424
RC, 425
symptoms
of spyware, 31
of viruses, 28-29
SYN, 385
SYN flood attacks, 176
system failure, 6
system files, verifying, 84
System logs, 393
System Monitor, 384
System Restore, 84
system security settings, audits on, 396-398
system virtual machines, 87
Systems Development Life Cycle (SDLC), 128-130

T

TACACS (Terminal Access Controller Access-Control System), 284-286
TACACS+, 285-286
tailgating, 519
tape backups, types of, 490-491
tapping into data, 241-244
TCB (trusted computing base), 308
TCP reset attacks, 174
TCP/IP fingerprinting, 347
TCP/IP hijacking, 180
TDEA (Triple Data Encryption Algorithm), 424

teardrop attacks, 177
technical security controls, 348
technologies
data loss prevention systems, 42
intrusion detection systems, 38-40
localized authentication technologies, 273-279
IEEE 802.1X standard, 273-276
Kerberos, 277-278
LDAP, 276-277
Terminal Services, 279
monitoring tools
performance baselining, 381-384
protocol analyzers, 384-388
personal firewalls, 35-38
pop-up blockers, 40-42
remote authentication technologies, 279-286
RADIUS versus TACACS, 284-285
RAS, 280-281
VPNs, 281-284
types of, 7-9
for vulnerability assessments, 352-362
network mapping, 352-355
password analysis, 359-362
protocol analyzers, 358-359
vulnerability scanning, 355-358
telephony devices, securing, 165-167
modems, 166
PBX equipment, 166-167
VoIP, 167
Telnet, 70-72, 166, 238
TEMPEST standards, 241, 515
templates, security, 80-82
temporary files, removing, 83, 119
10 tape rotation backup method, 492
Terminal Access Controller Access-Control System (TACACS), 284-286
Terminal Services, 279
test systems, importance of, 20
testing in patch management, 79
testing methods for secure coding concepts, 130-132
testing phase (SDLC), 129-132
theft
disaster recovery, 495
of smartphones, 48-49
threats
malware, 18-36
delivery methods for, 23-25
preventing and troubleshooting, 26-36
rootkits, 21
spam, 21-22
spyware, 21
Trojan horses, 20
viruses, 18-19
worms, 19-20
modeling, 129
types of, 6-7
3DES (triple DES), 424
3-leg perimeter DMZ, 157-158, 210
tickets (Kerberos), 278, 420
time bombs, 24
TLS (Transport Layer Security), 458-459
top secret information, sensitivity of, 523
Towers of Hanoi backup rotation method, 493
tracking cookies, 119
training employees
for browser security, 114
on policies, 527-528
against social engineering, 520-521
spam prevention, 35
spyware prevention, 31
transitive access, 182
transparent testing, 130

Transport Layer Security (TLS), 458-459

Trend Micro OSSEC, 39

Trend Micro's HouseCall, 29

Triple Data Encryption Algorithm (TDEA), 424

Trojan horses, 20, 30

troubleshooting malware, 26-36

- rootkits, 32-33
- spam, 33-35
- spyware, 30-32
- viruses, 26-30
- worms and Trojan horses, 30

true negatives, 273

true positives, 273

TrueCrypt, 45

trusted computing base (TCB), 308

Trustworthy Computing, 25

tunneling protocols (VPNs), 282

twisted-pair cables, 238, 240

- open ports on, 243
- splitting wires of, 243

U

UAC (User Account Control), 124, 325-326

UDP flood attacks, 176

unauthorized access, 6

unicast, 151

uninterruptible power supplies (UPS), 480-481

unshielded twisted pair (UTP) cables, 240

updates, installing, 26-27, 75-80

updating

- BIOS, 44
- service packs, 96

UPS (uninterruptible power supplies), 480-481

URL spoofing attacks, 178

USB devices, securing, 44-45

User Account Control (UAC), 124, 325-326

user accounts

- expiration, 314
- restrictions, configuring, 328-330

user awareness, 7

user education

- for browser security, 114
- on policies, 527-528
- against social engineering, 520-521
- spam prevention, 35
- spyware prevention, 31

user input validation, 129

usernames in access control, 318-322

users

- in access control, 313-317
- permissions, configuring, 330-331

UTP (unshielded twisted pair) cables, 240

V

vacation policies, 526-527

validation

- of certificates, 453
- input validation, 129, 131

vampire taps, 241-242

vendor contracts, 528

verifying system files, 84

Verisys, 39

versions of patches, explained, 78

vertical privilege escalation, 236

virtual appliances, 88

virtual local area network (VLAN), 164-165

virtual machine manager (VMM), 92

virtual machines (VMs), 85-87

- creating in Virtual PC 2007, 96-98
- hypervisors, 92
- Microsoft Virtual PC, 88-90

Microsoft Virtual Server, 90
Microsoft Windows XP Mode, 90
securing, 92-94, 98-101
VMware, 91

Virtual PC, 88-90

Virtual PC 2007, creating virtual machines, 96-98

virtual private networks (VPNs), 281-284
configuring, 289-291
IPsec, 460-461
L2TP, 460
PPTP, 460
for router security, 153

Virtual Server, 90

virtual servers, 208

virtualization, 85-94
hypervisors, 92
Microsoft Virtual PC, 88-90
Microsoft Virtual Server, 90
Microsoft Windows XP Mode, 90
securing virtual machines, 92-94, 98-101
types of, 85-88
VMware, 91

viruses, 18-19
preventing and troubleshooting, 26-30
symptoms of, 28-29

vishing, 517

VLAN (virtual local area network), 164-165

VLAN hopping, 164-165

VMM (virtual machine manager), 92

VMs (virtual machines), 85-87
creating in Virtual PC 2007, 96-98
hypervisors, 92
Microsoft Virtual PC, 88-90
Microsoft Virtual Server, 90
Microsoft Windows XP Mode, 90
securing, 92-94, 98-101
VMware, 91

VMware, 91, 94

voice encryption, 48

VoIP (voice over Internet Protocol), securing, 167

VPNs (virtual private networks), 281-284
configuring, 289-291
IPsec, 460-461
L2TP, 460
PPTP, 460
for router security, 153

vulnerabilities, 341. *See also* attacks
of Bluetooth, 250-251
of cabling, 238-244
crosstalk, 240
data emanation, 241
interference, 239
tapping into data, 241-244
of network devices, 234-238
backdoors, 237
default accounts, 234-235
network attacks, 237
privilege escalation, 236-237
weak passwords, 235-236
to program code, 132-136
backdoors, 132
buffer overflows, 132-133
code injection, 133-134
directory traversal, 134
XSS and XSRF, 133
zero day attacks, 135
of wireless access points, 244-249
of wireless transmission, 250

vulnerability assessments, tools for, 352-362
network mapping, 352-355
password analysis, 359-362
protocol analyzers, 358-359
vulnerability scanning, 355-358

vulnerability management, 349-351

vulnerability scanning, 355-358

W

WANs, LANs versus, 157

WAP (wireless access points), vulnerabilities, 244-249

wardialing, 166, 517

wardriving, 250, 256

warm sites, 489

weak encryption on wireless access points, 246-247

weak passwords, 235-236, 361

web browser security. *See* browser security

web of trust, 456

web proxy servers, 213

web security gateways, 214

websites

- encryption notification, 114
- pop-up blocking, 40-42
- pop-up windows, closing, 114
- removing e-mail addresses from, 34

well-known ports, list of, 170-169

wet pipe systems, 512

whaling, 517

white hats, 9

white-box testing, 130, 350

whitelists, 34, 121

whole disk encryption, 45-47, 84

wide area networks (WANs), local area networks (LANs) versus, 157

Windows Firewall, 27-28, 37

Windows Update, 26-27, 75-80

Windows XP Mode, 90

wire tapping, 241-244

wired network security, 234-244

- cable vulnerabilities, 238-244
  - *crosstalk, 240*
  - *data emanation, 241*
  - *interference, 239*
  - *tapping into data, 241-244*
- device vulnerabilities, 234-238
  - *backdoors, 237*
  - *default accounts, 234-235*
  - *network attacks, 237*
  - *privilege escalation, 236-237*
  - *weak passwords, 235-236*

wireless access points

- securing, 254-256
- vulnerabilities, 244-249

wireless network security, 244-251

- Bluetooth vulnerabilities, 250-251
- vulnerability assessments, 353
- wireless access point vulnerabilities, 244-249
- wireless transmission vulnerabilities, 250

Wireshark, 358, 385-386

wood fires, extinguishing, 510

Word, securing, 127

worms, 19-20, 30

WWN (World Wide Name) spoofing, 179

X

X.509 standard, 452

XML injection, 134

XSRF (cross-site request forgery), 133

XSS (cross-site scripting), 118, 133, 181

Z

zero day attacks, 135

zombies, 25, 178

Zone Alarm, 37

zone transfers, 183