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

CompTIA Security+ SY0-301 Authorized Cert Guide

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

Contents at a Glance

On the DVD:

Appendix A: Memory Tables

Appendix B: Memory Tables Answer Key

Table of Contents

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

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.

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.

CompTIA. Security+ ™

- **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 Knowledge and Skills Gets Jobs	Retain your Job and Salary	Want to Change Jobs	Stick Out from the Resume Pile
IT is ubiquitous, needed by most organizations. Globally, there are over 600,000 IT job openings.	Certifications are essential credentials that qualify you for jobs, increased compensation, and promotion.	Make your expertise stand above the rest. Competence is usually retained during times of change.	Certifications qualify you for new opportunities, whether locked into a current job, see limited advancement, or need to change careers.	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.
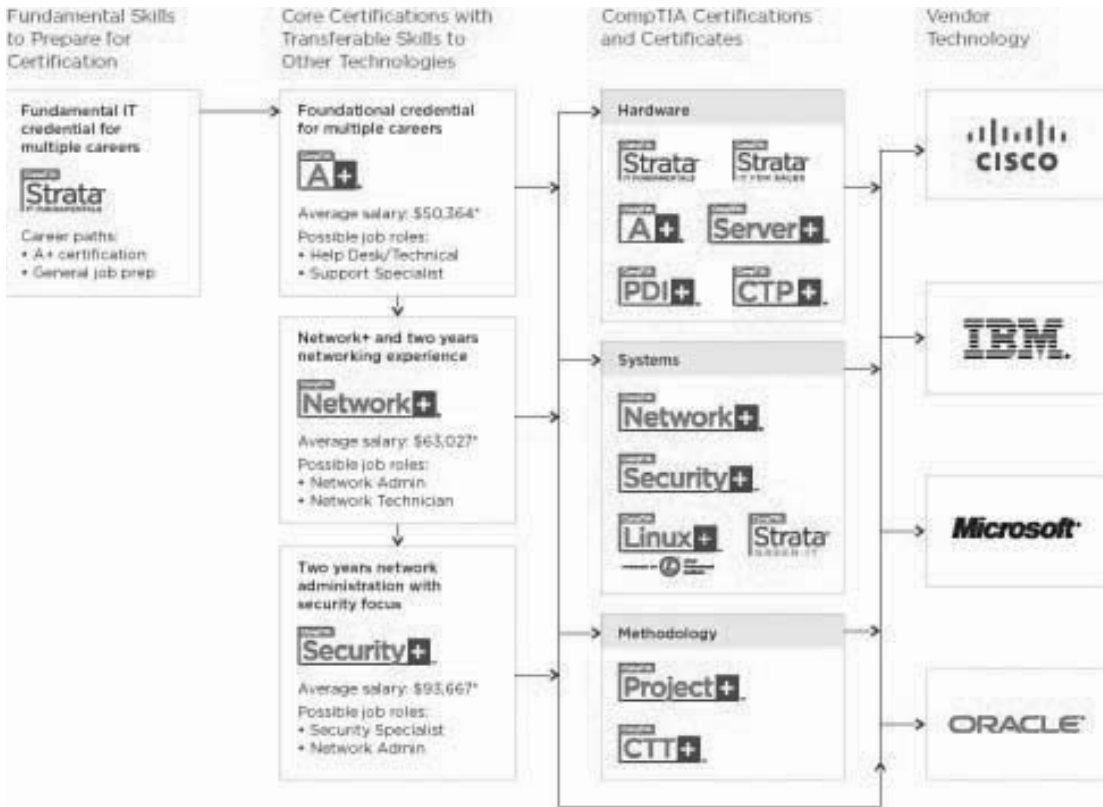
Source: Computerworld Salary Survey 2010—U.S. salaries only

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 :**

Introduction

Welcome to the *CompTIA Security+ SY0-301 Authorized Cert Guide*. The Comp-TIA 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 Comp-TIA 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	n/a
	Think Like a Hacker	
2	Computer Systems Security Threats	Objectives 3.1, 3.2, 4.2, 4.3
	Implementing Security Applications	
	Securing Computer Hardware and Peripherals	
3	Hardening Operating Systems	Objectives 3.6, 4.1, 4.2
	Virtualization Technology	
4	Securing the Browser	Objective 3.5, 4.1, 4.2
	Securing Other Applications	
	Secure Programming	
5	Network Design	Objectives 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 3.2, 3.5, 4.3
	Ports and Protocols	
	Malicious Attacks	
6	Firewalls and Network Security	Objectives 1.1, 1.2, 3.6
	NIDS Versus NIPS	

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 page intentionally left blank

This chapter covers the following subjects:

- **Security 101**—School is in session. This section discusses some of the basic principles of information security such as CIA and AAA, some basic threats, and various ways to mitigate those threats.

- **Think Like a Hacker**—To know your enemy, you must think like the enemy. Sometimes the hacker is your adversary, sometimes not. This section describes the various hats worn in the hacker society.

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.

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.
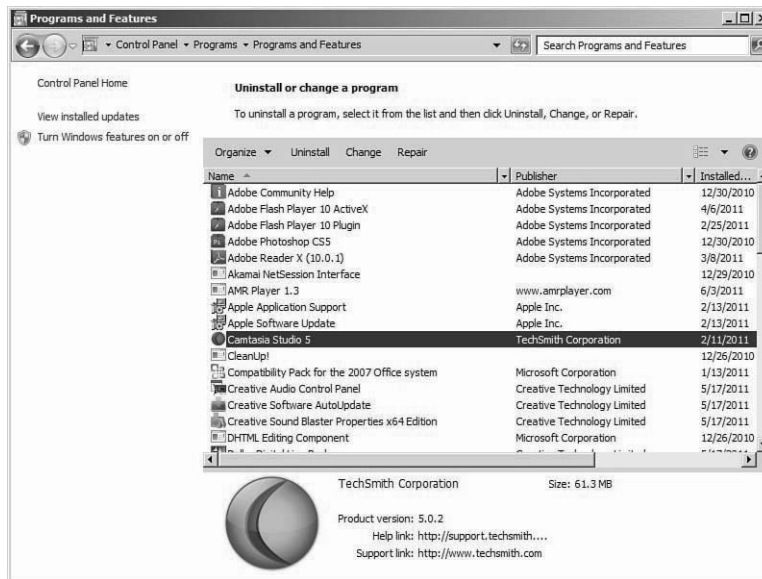
Figure 3-1   Windows 7 Programs and Features Window

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.
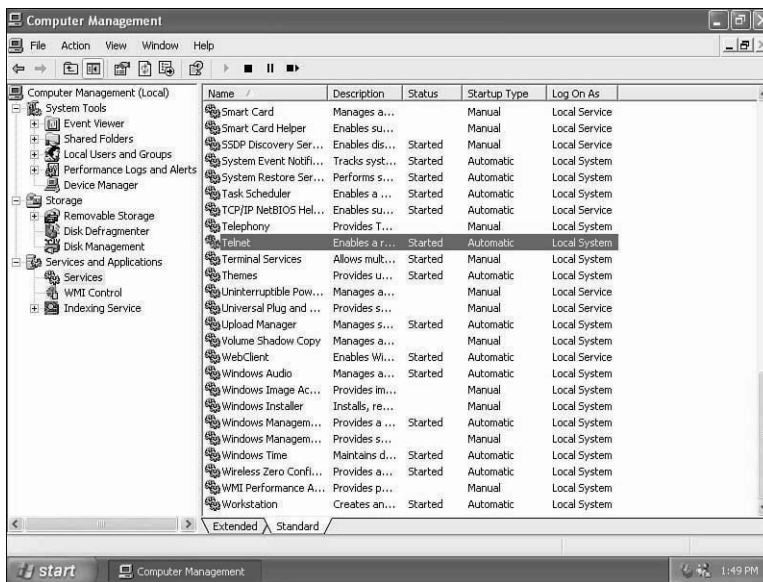
Figure 3-2   Services Window in Windows XP

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.
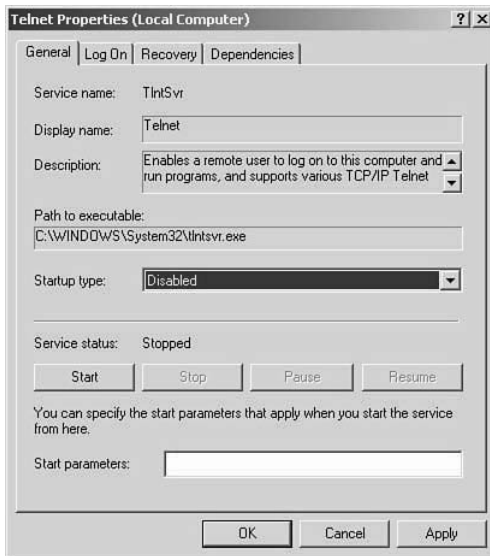
Figure 3-3   Telnet Properties Dialog Box

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 open-ing the System Information tool (open the Run prompt and type **msinfo32.exe**). It will be listed directly in the system summary. In addition, you can use the **systeminfo** command in the Command Prompt (a GREAT information gatherer!).

Key Topic
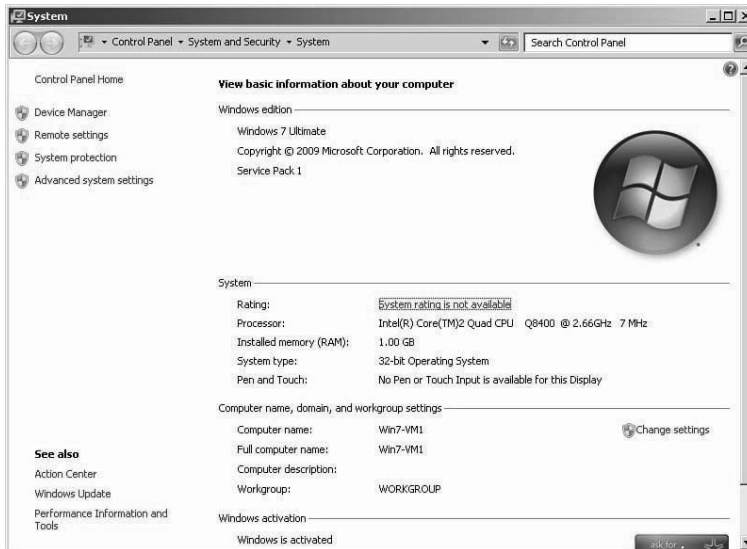
Figure 3-4   Windows 7 System Window

Key Topic
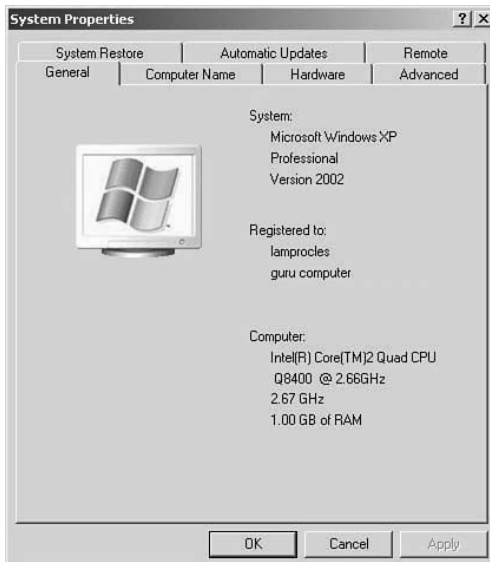
Figure 3-5   Windows XP System Properties Dialog Box

To find out what SP a particular version of Office is running, click **Help** on the menu bar and select **About Microsoft Office <Application Name>** where the application name could be Outlook, Word, and so on, depending on what app you use. An example of this in Outlook is shown in Figure 3-6. Office SPs affect all the applications within the Office suite.

Figure 3-6   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 slip-streamed 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.

```
                              [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.
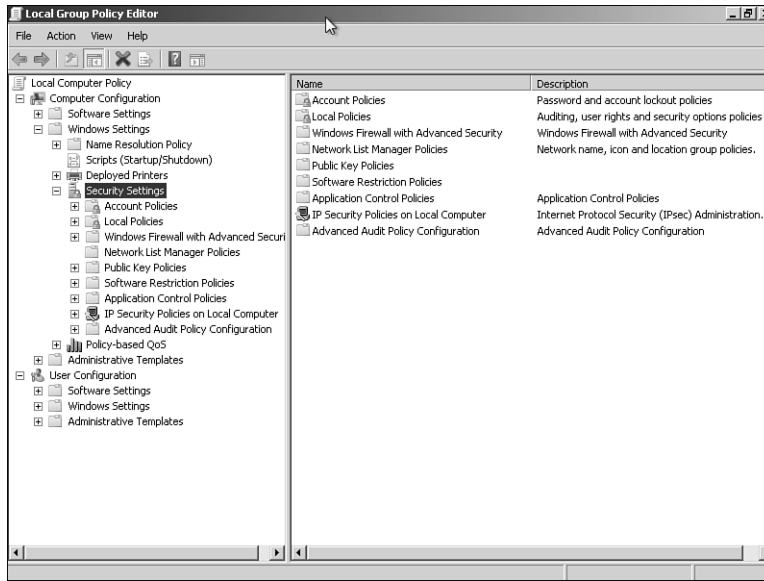
Figure 3-8   Local Group Policy Editor in Windows 7

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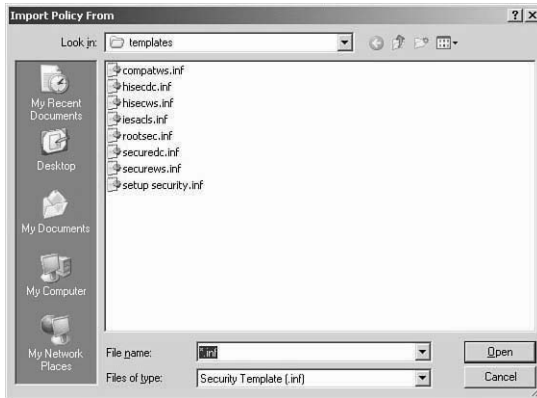
Figure 3-9   Import Policy From Window in Windows Server 2003

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

Key Topic

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

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

Step 2.   **Update the BIOS**—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.

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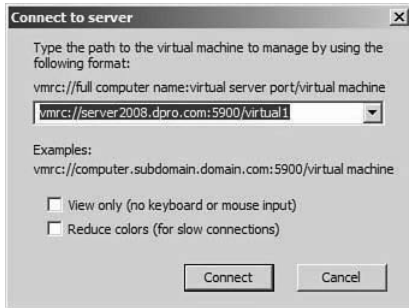
Figure 3-12   Virtual Machine Remote Client in Virtual Server 2005

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.
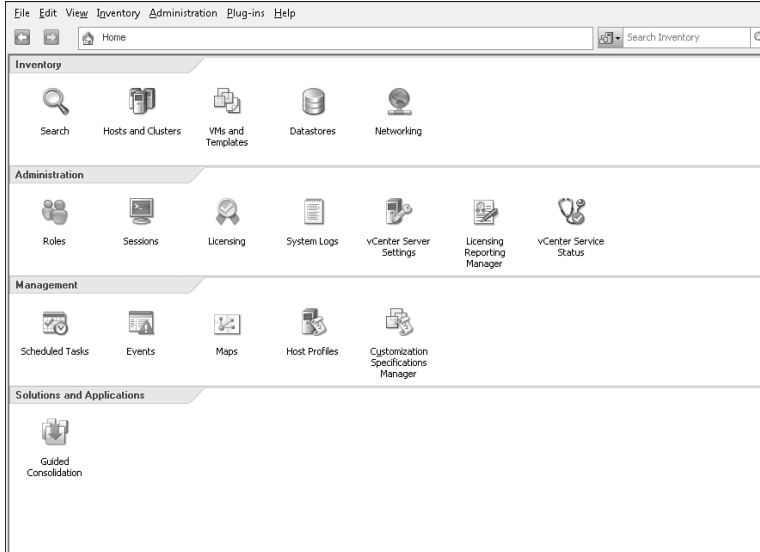
Figure 3-13   VCenter Management Console Window

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.

Key Topic

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 re-cover 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

D