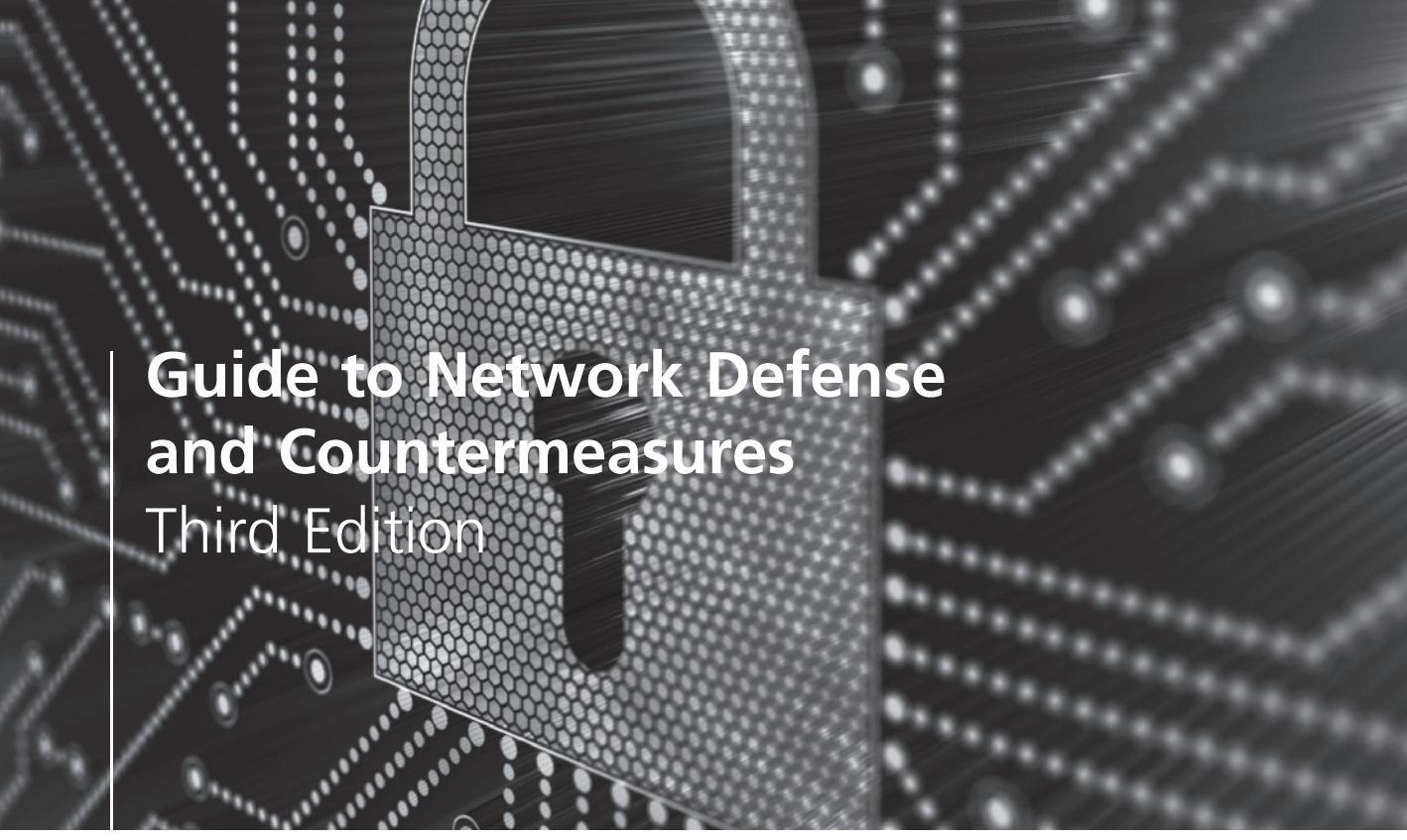
Third Edition

GUIDE TO NETWORK DEFENSE AND COUNTERMEASURES

Randy Weaver, Dawn Weaver, Dean Farwood

PREPARING TOMORROW'S INFORMATION SECURITY PROFESSIONALS



Guide to Network Defense and Countermeasures
Third Edition

Randy Weaver

Dawn Weaver

Dean Farwood

COURSE TECHNOLOGY
CENGAGE Learning®

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

Guide to Network Defense and Countermeasures, Third Edition

Randy Weaver, Dawn Weaver, Dean Farwood

Vice President, Careers & Computing: Dave Garza

Executive Editor: Steve Helba

Director, Development – Careers & Computing: Marah Bellegarde

Product Development Manager: Juliet Steiner

Product Manager: Natalie Pashoukos

Developmental Editor: Dan Seiter

Editorial Assistant: Jennifer Wheaton

Vice President, Marketing: Jennifer Ann Baker

Marketing Director: Deborah Yarnell

Production Director: Wendy A. Troeger

Production Manager: Andrew Crouth

Senior Content Project Manager: Andrea Majot

Senior Art Director: Jack Pendleton

Technology Project Manager: Joe Pliss

Media Editor: William Overocker

Library of Congress Control Number: 2012949396

ISBN-13: 978-1-133-72794-1

ISBN-10: 1-133-72794-8

Course Technology
20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: **international.cengage.com/region**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For your lifelong learning solutions, visit **www.cengage.com/coursetechnology**

Purchase any of our products at your local college store or at our preferred online store **www.cengagebrain.com**

Visit our corporate website at **cengage.com**.

Printed in the United States of America
1 2 3 4 5 6 7 16 15 14 13 12

Brief Contents

Table of Contents

Introduction

This book is intended to provide students and professionals with a solid foundation in the fundamentals of advanced network security. The previous edition of this book placed significant emphasis on intrusion detection, but this edition aims to provide a more balanced approach to the topic of network defense and countermeasures. As the range of threats to data systems becomes broader, depending on a limited number of security strategies becomes riskier. Information security professionals need to have a broad range of knowledge and skills. As a result, the third edition includes topics such as routing security and cryptography, which play an important role in network defense, as well as newer concepts such as IPv6 and unified threat management, which have begun to play a larger role and are expected to become more important in the future.

Intended Audience

Guide to Network Defense and Countermeasures, Third Edition is intended for students and professionals who need hands-on experience with installing routers, firewalls, proxy servers, and intrusion detection and prevention systems (IDPSs) as well as a strong conceptual understanding of routing, packet signature analysis, firewalls, VPNs, intrusion detection and prevention, wireless network security, cryptography, and security policy management. Readers should be familiar with basic networking concepts such as TCP/IP, gateways, routers, and Ethernet standards.

New to the Third Edition

This edition varies from the second edition in several ways:

- It includes a more balanced approach to network defense and includes new chapter topics.
- It includes new chapters on TCP/IP (Chapter 2), routing fundamentals (Chapter 4), cryptography (Chapter 5), wireless networking and security (Chapters 6 and 7), and Internet security (Chapter 12).
- Hands-on activities have been removed from the body of the chapters to facilitate continuity.
- Hands-on projects have been updated.

Chapter Descriptions

This book has 14 chapters and one appendix as follows:

Chapter 1, "Network Security Fundamentals," provides a review of fundamental security concepts, such as threats to network security, security controls to mitigate the risk of those threats, and the goals of network security.

Chapter 2, "TCP/IP," explains the fundamentals of the TCP/IP network protocol stack, including TCP/IP subprotocols, IP addressing, subnetting, supernetting, variable length subnet masking, and classless interdomain routing. This information provides a foundation for later discussion of packet analysis, such as examination of IP, ICMP, TCP, and UDP headers. The function and structure of IPv6 is addressed in detail.

Chapter 3, "Network Traffic Signatures," introduces students to packet analysis through identification of signatures associated with normal and abnormal traffic. The chapter discusses normal and abnormal findings in TCP, IP, and ICMP packet headers.

Chapter 4, "Routing Fundamentals," discusses the basics of address resolution and router functions, including routing protocols. Both IPv4 and IPv6 routing concepts are discussed. The chapter also covers routing security concepts, including access control lists, authentication, and encrypted router connections.

Chapter 5, "Cryptography," explains cryptographic concepts such as primitives, pseudorandom number generation, hashing, encryption algorithms, digital signatures, Public-key Infrastructure, cryptographic standards, Web security, IPsec, and attacks against cryptography.

Chapter 6, "Wireless Network Fundamentals," discusses concepts of radio frequency transmission, infrared transmission, and signal behavior. The chapter addresses analog and digital modulation along with wireless LANs and wireless standards.

Chapter 7, "Understanding Wireless Security," addresses wireless security concepts and common attacks against wireless networks. The chapter discusses security solutions that are available both for wireless networks and handheld wireless devices. IEEE 802.11 media access control is explained as well.

Chapter 8, "Intrusion Detection and Prevention Systems," identifies the role of IDPSs in network defense; typical detection and prevention methods, including anomaly and signature detection; network and host-based systems; the development of signature rules; and management procedures.

Chapter 9, "Firewalls," provides students with a strong foundation in software and hardware firewalls, with an emphasis on packet filtering and the creation of rule sets.

Chapter 10, "Firewall Design and Management," builds on the previous chapter to address firewall configuration design and proxy server installation and management. Students learn about bastion hosts, honeypots, and Network Address Translation. The chapter also discusses unified threat management concepts and practice.

Chapter 11, "VPN Concepts," presents basic VPN concepts, including encapsulation, encryption, and authentication. VPN configuration and deployment are discussed as well as VPN packet-filtering rules and VPN policies and procedures.

Chapter 12, "Internet and World Wide Web Security," addresses Internet vulnerabilities and the common attacks against these vulnerabilities, including Web server, buffer overflow, SQL injection, ActiveX, and Java Applet attacks. The chapter also discusses security controls, including DNSSEC.

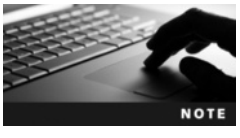
Chapter 13, "Security Policy Design and Implementation," describes the system development life cycle, risk analysis, determination of security controls, security policy concepts, and incident handling procedures.

Chapter 14, "Ongoing Security Management," discusses ways to improve network security through the management of security events. The chapter also addresses auditing and analyzing security procedures and controls as a means of keeping an organization's security posture up to date.

Features of the Book

- **Chapter Objectives**—Each chapter begins with a list of the concepts to be mastered. This list provides a quick reference to the chapter's contents and can be a useful study aid.
- **Chapter Summaries**—Following each chapter discussion is a summary of the concepts introduced in the chapter. These summaries provide students with a quick way to check their understanding of the chapter's main topics.
- **Key Terms**—All terms introduced in boldface text in a chapter are listed and defined after the chapter summary.
- **Review Questions**—The end-of-chapter assessments include a set of questions that allow students to demonstrate their mastery of the chapter's important concepts.
- **Hands-On Projects**—These challenging projects are an important element that gives students an opportunity to practice and research key concepts and skills, and to reinforce the chapter concepts through practical application.
- **Case Projects**—Each chapter contains one or more case projects that provide students with challenging situations for research and analysis.

Text and Graphic Conventions



The Note icon draws your attention to additional helpful material related to the subject being discussed.

Tips based on the author's experience provide extra information about how to approach a problem or what to do in real-world situations.

Each hands-on project in this book is preceded by the Hands-On icon and a description of the project.

This icon marks case projects, which are scenario-based assignments. In these extensive case examples, you are asked to implement independently what you have learned.

Instructor Resources

The following supplemental materials are available when this book is used in a classroom setting. All the supplements available with this book are provided to the instructor on a single CD-ROM (ISBN 978-1-1337-2795-8) and online at *www.cengage.com*.

Electronic Instructor's Manual. The Instructor's Manual that accompanies this textbook includes additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional activities.

Solutions. The answers to end-of-chapter material are provided. Solutions are provided for all review questions and for hands-on projects and case projects where applicable.

PowerPoint presentations. This textbook comes with Microsoft PowerPoint slides for each chapter. They are included as a teaching aid for classroom presentation, to make available to students on the network for chapter review, or to be printed for classroom distribution. Instructors, please feel free to add your own slides for additional topics you introduce to the class.

ExamView®. This textbook is accompanied by ExamView, a powerful testing software package that allows instructors to create and administer printed, computer (LAN-based), and Internet exams. ExamView includes hundreds of questions that correspond to the topics covered in this book, enabling students to generate detailed study guides that include page references for further review. The computer-based and Internet testing components allow students to take exams at their computers and save the instructor time by grading each exam automatically.

Figure files. All figures and tables in the textbook are reproduced on the Instructor Resources CD. Like the PowerPoint presentations, they are included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

Classroom Setup Guidelines

Most hands-on projects in this book are intended to be performed by pairs of students using two computers: one with Windows Server 2008 R2 Enterprise Edition installed as a domain controller, and one installed with Windows 7 Professional Edition as a member of the domain. Both systems

should have the latest updates installed; installation procedures for both operating systems are included later in this section.

Multiple pairs of students can work through the activities in a classroom network environment, or two computers can be connected using a hub or switch. Both students in each pair should work together on each element of the hands-on projects because all tasks are unique and students might not be able to repeat projects with the roles reversed. Alternatively, a single student can work with both systems to perform the hands-on projects.

Several hands-on projects require an additional computer that is set up to run Ubuntu Linux. Specific directions for these setup procedures are provided later in the book as needed.

This section also lists the hardware items and software programs required to complete the hands-on projects in the book. For most of the projects, you need three computers, each with the following features:

Hardware Requirements

- Intel or AMD 64-bit, 1.6 GHz, dual-core processor (4-core, 2.0 GHz or greater recommended)
- At least 2 GB of RAM (4 GB recommended)
- 80-GB hard disk
- Internet access
- DVD-ROM drive
- Super VGA (800 × 600) or higher-resolution monitor
- Video card with 128 MB of RAM and support for DirectX 9 or higher
- Keyboard and mouse or compatible pointing device
- One free USB port (optional)
- One USB wireless adapter (optional)
- One PCI Ethernet network interface card for each PC
- CD-R drive and burning software to create Ubuntu CDs for students

Software Requirements

You need the following operating systems and applications:

- Windows Server 2008 R2 Enterprise Edition
- Windows 7 Professional Edition
- Ubuntu Linux
- ZoneAlarm Free Firewall
- Nmap
- WinPcap
- Sawmill
- Wireshark
- TShark

- Toggit Router Simulator
- Microsoft Word 2010
- TrueCrypt
- inSSIDer
- Snort
- Samba
- Microsoft Forefront Threat Management Gateway 2010
- Apache
- Project Risk Analysis
- Network Asset Tracker

Network Setup

- Each system should be configured with a static IP address, subnet mask, and default gateway that are appropriate for the classroom network and that provide access to the Internet.
- All Windows Server 2008 and Windows 7 systems should be configured with an administrative account that has the username *administrator* and a password of *Pa$$word*.
- The instructor should assign each team of students a domain name of team*x*.net, where *x* is a unique number starting at 1. For example, the domain names should be team1.net, team2.net, and so on.
- Each system should be assigned a hostname based on the system and the team number. For example, the hostnames should be Team1Client.team1.net, Team1Srv.team1.net, Team2Client.team2.net, Team2Srv.team2.net, and so on.
- Although a central instructor server is not required, it may be wise to download required software programs to such a server so that download times are decreased for students and correct versions of the software are available for future classes.

Installing Windows Server 2008 R2

1. Turn on the computer.
2. Insert the Windows Server 2008 R2 Enterprise Edition DVD into the DVD-CD drive.
3. Boot to the DVD.

If your system does not boot to the DVD, you might need to alter the device boot order in the BIOS setup utility.

4. In the Install Windows window, verify that the correct language, time, and keyboard type are selected, and click **Next**. Click **Install now**.
5. The next window prompts you to enter your product key for activation. Enter the key number and click **Next**.

6. The next window prompts you to select the operating system you want to install. Click **Windows Server 2008 R2 Enterprise (Full Installation)**, and click **Next**.
7. In the Microsoft Software License Terms window, check the **I accept the license terms** box, and click **Next**. Click **Custom**.
8. The next window asks where you want to install Windows. Click **Drive options (advanced)**, click **New**, enter **30000** in the Size text box, and click **Apply**. Click **OK**. Click **Next**.
9. The system will reboot automatically several times. You are then prompted to change the user password. Click **OK**, enter **Pa$$word** in both text boxes, and press **Enter**. The password is for a user named *administrator* who has full access to the system. Click **OK** in the next window to confirm that your password has been changed.
10. The Initial Configuration Tasks window appears. In the Provide Computer Information section, click **Provide computer name and domain**. In the System Properties window, click the **Change** button. In the Computer Name/Domain Changes window, type **Server*x*** in the Computer name text box, where *x* is the team number assigned by your instructor. Click **OK**. At the prompt that discusses restarting, click **OK**. Click **Close** in the System Properties window, and click **Restart Later** in the Microsoft Windows window.
11. In the Initial Configuration Tasks window, click **Enable automatic updating and feedback** in the Update This Server section. In the Enable Windows Automatic Updating and Feedback window, click **Manually configure settings**. In the Manually Configure Settings window, click the **Change Setting** button in the Windows automatic updating section. In the Change settings window, click **Download updates but let me choose whether to install them** in the drop-down list under Important updates. Click **OK** and then click **Close** in the Manually Configure Settings window.
12. At the bottom of the Initial Configuration Tasks window, check the **Do not show this window at logon** box, and click **Close**.
13. Server Manager opens automatically. In the Server Summary/Computer Information section, check the **Do not show me this console at logon** box, and then close the Server Manager window.
14. Right-click the desktop, click **Screen Resolution**, and choose an appropriate resolution setting for yourself. Close the Screen Resolution window.
15. Click **Start**, and then click **Control Panel**. Type **desktop icons** in the Search Control Panel box. Click **Show or hide common icons on the desktop** under Display. Check the **Computer** and **Network** boxes, and then click **OK** to close the Desktop Icon Settings window. Close the Control Panel.
16. Click the **Start** button on the taskbar, click **Computer**, and double-click **Local Disk (C:)**. From the Organize menu, click **Folder and search Options**. On the View tab in the Folder views section, click **Apply to Folders**, click **Yes**, and click **OK**.
17. Click **Folder Options**, and click the **View** tab. Under Hidden files and folders, click the **Show hidden files, folders and drives** option button, remove the checks from the **Hide extensions for known file types** and **Hide protected operating system files (Recommended)** boxes, read the warning, and click **Yes**. (In a production environment, you should not show hidden files and folders or show protected operating system files on client workstations.) Click **OK** in the Folder Options window.

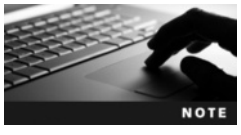
18. Click **Start**, and click **Network**. If an information bar appears and informs you that the network discovery and file sharing features are turned off, click the **information bar**, click **Turn on network discovery and file sharing**, and click **Yes, turn on network discovery and file sharing for all public networks**.

The setting described in Step 19 is appropriate in a lab setting, but it should be used with caution and only for a specific business need on a production network. Whenever this information bar appears in a hands-on project in this book, turn on network discovery and file sharing.

19. Click the **Network and Sharing Center** button. In the left pane, click **Change adapter settings**. Right-click **Local Area Connection**, click **Properties**, select **Internet Protocol Version 4 (TCP/IPv4)**, and click the **Properties** button. Click the **Use the following IP address** option button, and then enter the IP address, subnet mask, and default gateway as directed by your instructor. Click **OK** and then click **Close**.
20. Close all windows. Click **Start**, click the right arrow on the far right of the Start menu's bottom line, and click **Shut down**. In the Shut Down Windows window, type **Post-installation reboot** and click **OK**.
21. Upgrade the server to a domain controller using the naming conventions and procedure assigned by the instructor.

Installing Windows 7

1. Turn on the computer.
2. Insert the Windows 7 Professional Edition DVD into the DVD-CD drive.
3. Boot to the DVD.
4. In the Install Windows window, verify that the correct language, time, currency, and keyboard type are selected, and click **Next**. Click **Install now**.



If your system does not boot to the DVD, you might need to alter the device boot order in the BIOS setup utility.

5. In the license terms window, check the **I accept the license terms** box, and click **Next**.
6. When asked which type of installation you want, click **Custom (advanced)** and click **Next**.
7. When asked where you want to install Windows, accept the default location and click **Next**.
8. The system will reboot automatically several times. In the next window, you are prompted to choose a username for your account and to name your computer to distinguish it on the network. Type your first name as the username and type **Win7*x*** as the computer name, where *x* is the team number assigned by your instructor. Click **Next**.
9. In the next window, you set a password for your account. Type **Pa$$word** as the password and enter it again in the second text box. In the Type a password hint text box, type **Pa$$word** again. Note that in a production environment, you would not type the password itself as a hint. Click **Next**.

10. In the next window, enter the product key provided by your instructor. Click **Next**.
11. In the next window, click **Use recommended settings**.
12. In the time and date settings window, verify that the settings are correct and click **Next**.
13. In the window that prompts you to select the computer's current location, click **Work network**.
14. The system opens to the desktop. Right-click the desktop, click **Personalize**, click **Display**, click **Adjust resolution**, and then select a resolution that is appropriate for you. Click **OK** in the Screen Resolution window.
15. After approving the resolution, click **Personalization** in the left pane of the Display window. In the left pane of the Personalization window, click **Change desktop icons**, and check the **Computer** and **Network** boxes. Click **OK** and close the Personalization window.
16. Click the **Start** button on the taskbar, and then click **Control Panel**. Select **Small icons** from the View menu. In the left pane, click **Classic View**. Close the Control Panel.
17. Click **Start**, and then click **Computer**. From the Organize menu, click **Folder and search options**. Click the **View** tab. Under Hidden files and folders, click the **Show hidden files, folders and drives** option button, remove the checks from the **Hide extensions for known file types** and **Hide protected operating system files (Recommended)** boxes, read the warning, and click **Yes**. (In a production environment, you should not show hidden files and folders or show protected operating system files on client workstations.) Click **OK**. Close the Computer window.
18. Right-click the **Start** button, and click **Properties**. Click the **Customize** button. Scroll down, check the **Network** box, and click **OK**. Click **OK** in the next window. Click the **Start** button and click **Network**. If an information bar appears and informs you that the network discovery and file sharing features are turned off, click the **information bar** and then click **Turn on network discovery and file sharing**.

The setting described in Step 18 is appropriate in a lab setting, but it should be used with caution and only for a specific business need on a production network. Whenever this information bar appears in a hands-on project in this book, turn on network discovery and file sharing.

19. Click **Network and Sharing Center** in the menu bar, and click **Change adapter settings**. Right-click **Local Area Connection**, click **Properties**, select **Internet Protocol Version 4 (TCP/IPv4)**, and click the **Properties** button. Click the **Use the following IP address** option button, and then enter the IP address, subnet mask, and default gateway as directed by your instructor. Click **OK**, and then click **Close**.
20. Click the **Start** button, click **All Programs**, and click **Windows Update**. Follow the directions to install all recommended updates.
21. Join the domain created by your partner's server. Use the naming conventions and directions provided by your instructor.
22. Close all windows. Click **Start** and click **Shut down**.

Acknowledgments

I would like to thank authors Randy and Dawn Weaver, whose previous editions and vision for this third edition made my job a pleasure. Thanks, too, to the editorial and production staff of Cengage Learning, including Natalie Pashoukos and Andrea Majot, and Suwathiga Velayutham of Integra. In particular, thanks to editor Dan Seiter, whose talent allows me to pretend I'm a writer. I am indebted to reviewer Guy Garrett of Gulf Coast Community College, whose careful analysis and detailed suggestions improved this book significantly.

Thanks to my wife Lisa for letting me spend months of weekends being a desk jockey.

This book is dedicated to my students at Heald College, San Francisco.

chapter 1

Network Security Fundamentals

After reading this chapter and completing the exercises, you will be able to:

- Describe the threats to network security
- Explain the goals of network security
- Describe a layered approach to network defense
- Explain how network security defenses affect your organization

This chapter reviews the fundamental network security concepts you need to know. First, you learn about different kinds of intruders and threats to network security, such as threats within your organization, malicious code, and natural disasters. Attackers have many motivations for hacking into networks, and your job is to figure out what they are doing and prevent them from carrying out their plans. The Internet is widely used in most network environments, so you also review some concerns about Internet access.

Next, you learn about the goals of network security and the challenges of ensuring confidentiality, integrity, and availability for network resources. You then delve into the basics of network defense technologies. You discover how layering technologies can ensure better protection than any single technology used alone. The method of layering defensive technologies is called defense in depth (DiD), and includes physical, logical, and virtual security concepts. Auditing is the mainstay of monitoring and troubleshooting a network, so you also review log file basics. Finally, you see how security efforts affect an organization and learn that information security is not the sole domain of information technology (IT).

Examining Network Security Fundamentals

A variety of attackers might attempt network intrusions, causing loss of data, loss of privacy, and other consequences. You learn about these attackers in the following sections. These types of threats are becoming a concern for a growing number of corporate managers. More businesses are actively addressing information security, but many others have not taken steps to secure their systems from attack.

Threats to Network Security

When planning network security measures, knowing the types of attackers who might try to break into your network is important. This knowledge can help you anticipate threats and set up detection systems, firewalls, and other countermeasures to block attacks as effectively as possible. Similarly, understanding the motivation of attackers helps you prepare security controls:

- *Status*—Some attackers attempt to take over computer systems just for the thrill of it. They like to count the number of systems they have accessed as notches on their belt.
- *Revenge*—Disgruntled current or former employees might want to retaliate against an organization for policies or actions they consider wrong. They can sometimes gain entry through an undocumented account (back door) in the system.
- *Financial gain*—Other attackers have financial profit as their goal. Attackers who break into a network can gain access to financial accounts. They can steal individual or corporate credit card numbers and make unauthorized purchases. Just as often, attackers defraud people out of money with scams carried out via e-mail or other means.
- *Industrial espionage*—Proprietary information is often valuable enough that it can be sold to competing companies or other parties.

Hackers A **hacker** is anyone who attempts to gain access to unauthorized resources on a network, usually by finding a way to circumvent passwords, firewalls, or other protective measures. Hackers seek to break into computers for different reasons:

- "Old school" hackers consider themselves seekers of knowledge; they operate on the theory that knowledge is power, regardless of how they come by that knowledge. They are not out to destroy or harm; they want to discover how things work and open any sources of knowledge they can find. They believe the Internet was intended to be an open environment, and that anything online can and should be available to anyone.
- Other less "ethical" **crackers** pursue destructive aims, such as the proliferation of viruses and worms, much like vandals.
- Some bored young people who are highly adept with computers try to gain control of as many systems as possible for the thrill of it. They enjoy disrupting systems and keeping them from working, and they tend to boast about their exploits online.
- Criminals and industrial spies might be interested in selling information to the top bidder or using it to influence potential victims. Some companies would certainly be interested in getting the plans for a new product from their competitors.
- The term **script kiddie** is often used to describe relatively unskilled programmers who spread viruses and other malicious scripts to exploit weaknesses in computer systems. Script kiddies lack the ability to create viruses or Trojan programs on their own, but they can usually find these programs online.
- **Packet monkeys** are primarily interested in blocking Web site activities through a **distributed denial of service (DDoS) attack**. In a DDoS attack, many computers are hijacked and used to flood the target with so many false requests that the server cannot process them all, and normal traffic is blocked. Packet monkeys might also want to deface Web sites by leaving messages that their friends can read.
- **Hactivists** are computer attackers with political goals. Frequently they use denial of service attacks to shut down Web sites of organizations with whom they disagree. One of the best-known hactivist groups, named Anonymous, has successfully shut down sites of the U.S. Federal Trade Commission to express its opposition to proposed laws that combat digital piracy. Anonymous has also shut down sites that belong to the State of Alabama in protest of immigration laws. After discovering that the Central Intelligence Agency (CIA) was investigating the group, Anonymous shut down some of the CIA's sites as well.

Disgruntled Employees Disgruntled employees are usually unhappy over perceived injustices and want to exact revenge by stealing information. With the economic downturn, more current or former employees are stealing information for financial reasons. Often they give confidential information to new employers. When an employee is terminated, security measures should be taken immediately to ensure that the employee can no longer access the company network and telecommunications systems.

While most attacks come from outside a company, according to CyberSecurity Watch, insider attacks are more costly to a victimized company and are becoming increasingly more sophisticated. Theft, data loss, and network damage can result from the malicious actions of current or former employees. The following are just a few examples:

- A **logic bomb** is malware designed to start at a specific time in the future or when a specified condition exists. At Fannie Mae, the Federal National Mortgage Association,

a former engineer planted a logic bomb that could have shut the company down and cost millions by destroying all 4000 of the company's servers. Fortunately, the attack did not succeed. The former employee was sentenced to three years in jail.

- Ansir Khan, a former bank employee in Sheffield, England, attempted to steal $1.9 million after successfully stealing more than $1.1 million from the bank in April 2005 and May 2006. He extracted customer data and shared it with accomplices. He was sentenced to three years in jail.
- A former employee of United Way in Miami, Luis Robert Altamirano, accessed the United Way computer system a year after he left the organization. He deleted files and disabled the voicemail system. Altamirano pled guilty and was sentenced to 18 months in jail and fined $50,000 for computer fraud.
- Adeniyi Adeyemi, a contract employee of Bank of New York Mellon, stole the personal information of dozens of bank employees, mainly in the IT department. He used the information to open dummy financial accounts and receive funds stolen from the accounts of charities and nonprofit organizations.

Terrorists Until September 11, 2001, most people did not consider a terrorist attack on an information infrastructure (known as cyberterrorism) to be a likely threat. Since then, the threat posed by terrorists has been taken more seriously. A terrorist group might want to attack computer systems for several reasons: to make a political statement or accomplish a political goal, such as the release of a jailed comrade; cause damage to critical systems; or disrupt the target's financial stability. Attacking the World Trade Center certainly accomplished the latter goal, given the nature and location of the structures. Terrorists might also want simply to cause panic.

It might be hard to understand why a terrorist attack on computers would be considered a serious threat until you think about how many critical systems are controlled by computers. Consider the chaos that could result from a successful attack on a computer system that controls a nuclear power plant's reactors. The overall psychological effect could be just as detrimental as the infrastructure damage and even the loss of life.

Government Operations The shady world of international espionage is difficult to document, but it is becoming clear that a number of countries see computer operations as more than simply a spying technique; computer networks are a potential battleground. In 2010, a sophisticated malware program called Stuxnet was discovered. The Stuxnet worm was designed to attack Windows systems used in industrial and military settings. The goal was to infect the control systems of automated industrial processes. Security experts who analyzed Stuxnet concluded that it was probably the work of a government operation because of the complexity of the program and the amount of time and resources required to create and propagate it. Because Stuxnet was unusually prevalent in Iran, many observers believe that the United States and/or Israel were responsible for its creation and that it was intended to target Iran's nuclear industry.

Another focus of attention is the Chinese government, which is thought to be responsible for successful computer-based attacks on U.S. Department of Defense information systems as well as government, industrial, and military systems in Germany, France, and Britain.

Malicious Code In 2004, the MyDoom worm infected millions of computers in only a few days, costing $38.5 billion in cleanup, lost productivity, and other losses. MyDoom was believed to have been the fastest-spreading worm ever created. MyDoom is primarily transmitted via e-mail, with subject lines such as "Error," "Mail Delivery System," or "Mail Transaction Failed." If the user opens the attachment, the worm resends itself to e-mail addresses in the user's address book and local files. The first variant, MyDoom.A, contained a back door on port 3127/tcp and a denial of service attack on the SCO Group Web site that was timed to launch on February 1, 2004. The second variant, MyDoom.B, targeted the Microsoft Web site. It blocked access to Microsoft and some online antivirus sites, thus denying access to antivirus updates and virus-removal tools.

In 2008, a worm known as Conficker was discovered. This program attacked all Windows operating systems from Windows 2000 through Windows 7. An estimated 9 to 15 million computers were infected. In 2009, Microsoft offered a $250,000 reward for the identification of Conficker's authors. Conficker was designed to create **botnets**: networks of tens of thousands of infected computers that belong to unsuspecting victims and can be controlled from a central station. As of this writing, the authors of Conficker have not been identified, but because the program was designed not to infect systems with a Ukrainian keyboard, it is thought that the worm was developed in Eastern Europe.

Information security has improved since MyDoom and Conficker, but new vulnerabilities always lurk right around the corner, and security professionals must stay one step ahead of attackers. The following sections review the types of malware you might encounter.

Viruses, Worms, and Trojan Programs Although most users think of any type of virus, worm, or Trojan program as similar problems, they are completely different types of attacks. A **virus** is executable code that can replicate itself from one place to another surreptitiously and perform actions that range from benign to harmful. Viruses are spread by several methods, including running executable code, sharing disks or memory sticks, opening e-mail attachments, and viewing infected or malicious Web pages. Viruses can attach to other executables or replace them in order to spread or execute. Viruses require user intervention to run.

A **worm** creates files that copy themselves repeatedly and consume disk space. Worms do not require user intervention to be launched; they are self-propagating. Some worms can install **back doors**—a way of gaining unauthorized access to a computer or other resource, such as an unused port or terminal service, that makes it possible for attackers to gain control over the computer. A **port** is an area in random access memory (RAM) that is assigned a number (the port address) and is reserved for a program that runs in the background to listen for requests for the service it offers. Other worms can destroy data on a hard disk. Just like a cold or flu virus, computer viruses and worms can mutate or be altered to defeat antivirus software.

A **Trojan program** is also a harmful computer program, but one that appears to be something useful—a deception like the Trojan horse described in Greek legends. The difference between a virus and a Trojan program lies in how the malicious code is used. Viruses replicate and can potentially cause damage when they run on a user's