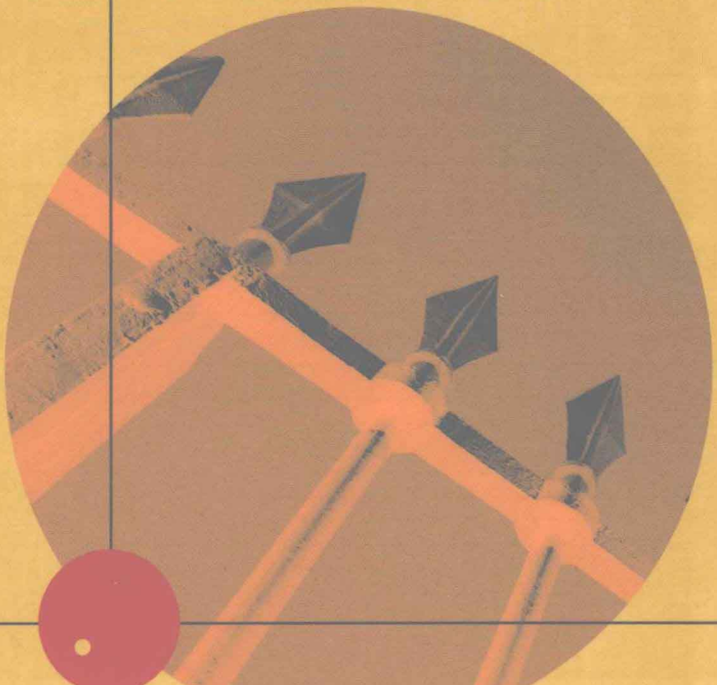
THOMSON
COURSE TECHNOLOGY

GUIDE TO NETWORK DEFENSE AND COUNTERMEASURES

SECOND EDITION

RANDY WEAVER



Guide to
Network Defense and Countermeasures, Second Edition

by
Randy Weaver

THOMSON
COURSE TECHNOLOGY

Australia • Canada • Mexico • Singapore • Spain • United Kingdom • United States

THOMSON
COURSE TECHNOLOGY™

Guide to Network Defense and Countermeasures, Second Edition
is published by Thomson Course Technology

Managing Editor:
William Pitkin III

Production Editor:
Danielle Slade

Technical Editor:
Sydney Shewchuk

Editorial Assistant:
Allison Murphy

Compositor:
GEX Publishing Services

Product Manager:
Sarah Santoro

Senior Manufacturing Coordinator:
Justin Palmeiro

Quality Assurance Coordinator:
Christian Kunciw

Cover Design:
Abby Scholz

Developmental Editor:
Lisa M. Lord

Product Marketing Manager:
Gayathri Baskaran

Copyeditor:
Lori Cavanaugh

Proofreader:
Marc Masse

Indexer:
Sharon Hildenberg

Printed in the United States.

1 2 3 4 5 6 7 8 9 CS 09 08 07 06 05

For more information, contact Thomson Course Technology, 25 Thomson Place, Boston, Massachusetts, 02210.

Or find us on the World Wide Web at:
www.course.com

Disclaimer
Thomson Course Technology reserves the right to revise this publication and make changes from time to time in its content without notice.

ISBN 1-4188-3679-6

Introduction

This book is an introduction to one of the most important and urgent concepts in protecting computers and networks: intrusion detection. In a narrow sense, intrusion detection is the capability of hardware and software to alert users to suspicious connection attempts that could represent attackers trying to gain unauthorized access to a computer and/or its resources. This specific function is covered extensively throughout several chapters of this book, along with other key security topics. However, in a wider sense, the practice of intrusion detection encompasses virtually all aspects of network security, and these activities—such as risk analysis, security policies, damage assessment, intrusion response, anticipating future attacks, and prosecuting intruders—are also examined.

This book was written with two goals. The first goal is to give students a solid foundation in advanced network security fundamentals. Although emphasis is placed on intrusion detection, the book also covers essential practices, such as developing a security policy and carrying out that policy by performing Network Address Translation (NAT) and packet filtering and by installing proxy servers, firewalls, and virtual private networks (VPNs). The second goal is to prepare students to take the Network Defense and Countermeasures exam, which is the second exam for the Security Certified Network Professional (SCNP) certification.

Intended Audience

Guide to Network Defense and Countermeasures, Second Edition is intended for students and professionals who need hands-on introductory experience with installing firewalls and intrusion detection systems (IDSs). This book assumes that students are familiar with the Internet and fundamental networking concepts, such as TCP/IP, gateways, routers, and Ethernet. It also assumes that students have fulfilled the prerequisites for exam SC0-402, which include IP troubleshooting; subnetting, subnet masking, IP datagram structure, routing, Web security, and common attack techniques.

Overview

Chapter 1 should be a review for students. It covers IP addressing, subnetting, routing, IP packet structure, and different types of network attacks that a perimeter security configuration should defend against. Chapters 2 and 3 cover risk analysis and the development of a well-defined security policy. Chapter 4 explains network traffic signatures, an essential concept to understand before planning intrusion detection and firewall configurations. Chapters 5 and 6 address using VPNs for secure remote access, and Chapters 7 and 8 explain the use of IDSs. Chapters 9 to 11 explore firewalls and include installation guidelines for Check Point NG and Microsoft ISA Server 2000. Students also learn about Linux's built-in command-line tool for packet filtering, Iptables. Chapter 12 discusses ongoing security management, including auditing, maintaining and monitoring systems, and managing security events. Most chapters incorporate encryption, authentication, and other security concepts that contribute to intrusion detection and countermeasures.

How To Use This Book

This book should be studied in sequence. The first chapter offers a solid refresher on network security and establishes the basis for the running case project (discussed later in "The Running Case Project"). Each chapter builds on the previous one and expands the basic knowledge students already have from prerequisite courses. Additionally, the sequence of chapters has been arranged to conform more closely to accepted information security best practices.

About the Organization of Topics

You might have noticed that the risk analysis and security policy chapters have been placed at the front of the book, unlike most security books. The reason for this is simple: Best practices state that your security policy dictates what security measures are needed to support organizational security goals. Your policy is the basis for security, so it follows that security policies should be learned first. To formulate an accurate and comprehensive security policy, you must first do the following:

(1) Identify, evaluate, and prioritize assets to be protected.

(2) Assess vulnerabilities and threats to assets, and evaluate the potential impact if threats become a reality.

(3) Determine how to manage risks.

(4) Create a security policy based on your risk assessment and the organization's needs and security stance.

This process can be more detailed, but these steps are the basic procedure for developing an initial security policy. Keep in mind, too, that a security policy is never truly completed. Risk analysis and policy review should be conducted regularly, especially in response to security incidents or changes. Your security policy must be updated to address your network's current needs.

After a security policy is in place, you can begin securing the network. At this stage, you begin evaluating hardware and software approaches to securing resources, such as VPNs for remote access, IDSs to monitor for unauthorized access, and firewalls to filter traffic.

The Running Case Project

The running case project is designed so that students can benefit from immediate practical application of newly learned skills and concepts. At the end of Chapter 1, students are asked to design a basic network for a fictitious company, LedGrafix. LedGrafix is a small video game design company that has recently released a new game that's a huge success. This explosive success means the company will be expanding rapidly and needs a new location. You have been hired to design and secure its new home. Throughout the book, you'll be working on a full-scale network design and security project.

The project attempts to mirror a real-life setting as closely as possible. In Chapter 1, you use your existing security knowledge and network design skills to draft an initial diagram for the new site and develop a full hardware and software inventory. Using this initial design, in subsequent chapters you conduct a risk analysis, draft a security policy, research equipment, plan a VPN deployment, and modify your security policy at each step to reflect the changes in your plan. You also design your IDS and firewall and update your security policy with the new VPN, IDS and firewall policies.

Although this project sounds time consuming, doing this same job in a real-world setting would be much more time intensive. At times it might seem that you don't have all the information you need to complete the project, but as in real life, answers aren't always definitive. You need to make judgment calls based on your own expertise, and choose the best solution you can when there doesn't seem to be a right answer. Real networks and businesses seldom have clear answers or needs.

The case project has three primary goals:

- To teach students how to find and use resources such as information security Web sites, newsgroups, mailing lists, and so forth
- To teach students how to apply concepts to solving problems and how to document their work effectively
- To guide students in carrying out an information security project in a logical and structured manner so that outcomes are more predictable and manageable

Throughout the project, your instructor can guide you with information, templates, or other materials the author has provided and will let you know his or her expectations for the final deliverable, a complete security policy and procedures manual for the LedGrafix network.

Chapter Descriptions

Here is a summary of the topics covered in each chapter of this book:

Chapter 1, "Network Defense Fundamentals," is intended as a review of previously learned concepts. Basic TCP/IP networking concepts that play a role in thwarting intrusions and attacks are covered, including IP addressing, subnetting, IP packet structure, DNS, and routing and access control. It also examines the goals of a network security program, which balances the need for connectivity and access with the need to maintain privacy and integrity. Chapter 1 also explores common security threats and vulnerabilities that intrusion detection systems (IDSs) and other security devices need to address and offers an overview of the basic tools for blocking those threats, including packet filters, antivirus software, log files and analysis software, and IDSs.

Chapter 2, "Security Policy Design: Risk Analysis," explains a key factor in security design: a comprehensive risk analysis. Often neglected, risk analysis provides key information needed to determine what security methods are best suited to the resources to be protected. An initial security policy is based largely on a comprehensive risk analysis and risk assessment.

Chapter 3, "Security Policy Implementation," examines the development of a security policy that tells organization members what resources must be protected, how to protect critical resources, and how to respond if an intrusion occurs.

Chapter 4, "Network Traffic Signatures," delves into the approaches IDS hardware and software use to detect unauthorized access attempts and block them. In particular, you examine different types of intrusion detection signatures. You learn how to capture packets, compare normal traffic signatures to suspicious ones, and develop filters based on traffic signatures.

Chapter 5, "Virtual Private Network (VPN) Concepts," discusses the basic concepts of VPNs, including the three core activities a VPN performs: encapsulation, encryption, and authentication. You also learn about tunneling protocols, IP Security (IPSec), and Internet Key Exchange (IKE), and then explore some advantages and disadvantages of VPNs.

Chapter 6, "Virtual Private Network (VPN) Implementation," explains how business needs figure into the equation of designing and deploying VPN connectivity. You learn about client security and see how to configure VPNs, how to use different topologies to secure a network, and how VPNs and firewalls work together. Finally, you learn how a VPN policy should be incorporated into your overall security policy.

Chapter 7, "Intrusion Detection System Concepts," introduces fundamental IDS concepts, including the components that make up an IDS and the basic step-by-step process of intrusion detection. Different options for setting up an IDS are covered, such as network-based, host-based, and hybrid IDS implementations. Finally, you examine some widely used IDS packages, ranging from freeware software to expensive hardware systems that use multiple network sensors to detect suspicious traffic.

Chapter 8, "Intrusion Detection: Incident Response," explains how to develop and refine IDS filtering rules. The primary task of the IDS is to detect suspicious activity, but it's still up to the response team to determine whether the activity is a problem or a false alarm and take steps to respond to the incident. You learn options for assembling a response team and see how to deal with false alarms. You also learn some guidelines for preparing evidence for prosecution.

Chapter 9, "Choosing and Designing Firewalls," explains the functions of a firewall and describes how perimeter networks are designed. This chapter provides an overview of basic types of firewalls and their primary functions so that you can choose the right one to meet your needs. You also learn about the firewall rule base, the heart of a firewall's operation, and the basic firewall security function—packet filtering.

Chapter 10, "Firewall Topology," discusses how proxy servers work to shield hosts on an internal network and explains how to select and configure a bastion host. You also learn about other common security functions that firewalls perform, including NAT, authentication, and encryption.

Chapter 11, "Strengthening and Managing Firewalls," discusses how to maintain and edit a rule base, manage log files, and improve firewall performance. This chapter also offers guidelines on installing Check Point NG and Microsoft ISA Server 2000 and using Linux's built-in packet-filtering tool, Iptables.

Chapter 12 "Strengthening Defense Through Ongoing Management," discusses the management of security measures so that they continue operating efficiently and continue detecting and protecting against attacks. You learn about real-time event monitoring and developing an IDS to keep pace with a growing network. This chapter also covers the importance of conducting regular security audits, enhancing a defense in depth strategy, and keeping your knowledge base up to date.

Appendix A, "SC0-402 Objectives," maps the objectives in the Security Certified Professional (SCP) SC0-402 Network Defense and Countermeasures exam to this book's corresponding chapter and section. If you need to brush up on a specific topic to prepare for the exam, you can use this appendix as a handy reference.

Appendix B, "Security Resources," lists several security-related organizations, groups, and information sources. If you're looking for up-to-the-minute news about virus attacks or security problems, turn to the resources listed in this appendix as a good starting point, but remember to develop your own security resources, too.

Features

To help you fully understand networking security concepts, this book includes many features designed to enhance your learning experience:

- **Chapter Objectives.** Each chapter begins with a detailed list of the concepts to be mastered in that chapter. This list gives you a quick reference to the chapter's contents and serves as a useful study aid.
- **Figures and Tables.** Numerous diagrams of networking configurations help you visualize common perimeter defense setups. In addition, tables provide details and comparisons in an organized, easy-to-grasp manner. Some tables include specific examples of packet-filtering rules you can use to build a firewall rule base. Because most labs use Microsoft operating systems, Microsoft products are used for most of the screen shots and Hands-on Projects in this book; however, some Linux coverage is included as well.
- **In-Chapter Activities.** Each chapter has short projects integrated into the main text. The purpose of these short activities is to provide immediate reinforcement of a newly learned skill or concept and give students an opportunity to apply knowledge and skills as a way to maintain interest and motivation.
- **Chapter Summaries.** Each chapter's material is followed by a summary of the concepts introduced in that chapter. These summaries are a helpful way to review the ideas covered in each chapter.
- **Key Terms.** Following the Chapter Summary, a list of all terms introduced in the chapter with boldfaced text are gathered together in the Key Terms list, with full definitions for each term. This list encourages a more thorough understanding of the chapter's key concepts and is a useful reference.
- **Review Questions.** The end-of-chapter assessment begins with a set of review questions that reinforce the main concepts in each chapter. These questions help you evaluate and apply the material you have learned.
- **Hands-On Projects**. Although understanding the theory behind networking technology is important, practice in real-world applications of this theory is essential. Each chapter includes projects aimed at giving students experience in planning and development tasks or hands-on configuration tasks.
- **Case Projects.** Each chapter closes with the corresponding segment of this book's running case project (described previously in "The Running Case Project"), which gives you a chance to draw on your common sense as well as skills and knowledge you have learned. Some chapters contain additional scenario-based Case Projects on intrusion detection and security-related situations to help you sharpen your decision-making and troubleshooting skills, which are essential in network security systems administration.

Lab Setup

The lab setup for this book is straightforward, requiring each student to have access to a computer capable of supporting Windows XP Professional with Service Pack 2 and Fedora Core 3 in a dual-boot configuration. Students also need access to the Internet for projects and research.

Text and Graphic Conventions

Where appropriate, additional information and exercises have been added to this book to help you better understand the topic at hand. Icons throughout the text alert you to additional materials. The following icons are used in this book:

NOTE

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

TIP

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

CAUTION

The Caution icon warns you about potential mistakes or problems and explains how to avoid them.

HANDS-ON PROJECTS

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

CASE PROJECTS

These icons mark Case Projects, which are scenario-based assignments. In these case examples, you're asked to apply independently what you have learned.

Instructor's Materials

The following supplemental materials are available when this book is used in a classroom setting. All supplements available with this book are provided to instructors on a single CD. You can also retrieve these supplemental materials from the Thomson Course Technology Web site, *www.course.com*, by going to the page for this book, under "Download Instructor Files & Teaching Tools."

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

Solutions. Solutions to all end-of-chapter material are included with answers to Review Questions and, when applicable, Hands-on Activities, Hands-on Projects, and Case Projects.

ExamView. This book is accompanied by ExamView, a powerful testing software package that instructors can use 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 have them graded automatically to save instructors time.

PowerPoint Presentations. This book comes with Microsoft PowerPoint slides for each chapter. These slides are meant to be used as a teaching aid for classroom presentation, to be made available to students on the network for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides for other topics introduced to the class.

Figure Files. All figures in the book are reproduced on the Instructor's Resources CD. Similar to 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.

Coping with Change on the Web

Sooner or later, all the specific Web-based resources mentioned in this book will become out of date or be replaced by newer information. In some cases, the URLs listed here might lead you to their replacements; in other cases, the URLs will lead nowhere, leaving you with the dreaded 404 error message, "File not found."

When that happens, don't give up! There's always a way to find what you want on the Web, if you're willing to invest some time and energy. Most Web sites offer a search engine, and if you can get to the main site, you can use this tool to help you find what you need. You can also use general search tools, such as *www.google.com*, *www.hotbot.com*, or *www.lycos.com*, to find related information. In addition, although standards organizations offer the most specific information about their standards, many third-party sources of information, training, and assistance are also available. The bottom line is that if you can't find something where the book says it's located, start looking around. It's an excellent way to improve your research skills.

Visit Our World Wide Web Site

Additional materials designed especially for you might be available for your course on the World Wide Web. Go to *www.course.com* periodically and search for this book title for more details.

Acknowledgments

I would like to thank Thomson Course Technology for the opportunity to write this book on a topic of such value and importance. Thanks also go to the editorial and production staff, including Sarah Santoro, Product Manager; Danielle Slade, Production Editor; and the testers in the Manuscript Quality Assurance Department: Christian Kunciw, John Freitas, and Danielle Shaw. Thanks also to Lisa Lord, Development Editor, for her guidance, her words of encouragement, and her periodic reminders that kept me on track. Sydney Shewchuk, the Technical Editor, went above and beyond the call of duty to provide suggestions based on his experience and knowledge. I would also like to thank the following reviewers, who guided me with helpful feedback on each chapter:

Michael Anderson, ECPI College of Technology, Newport News
Robert Bruen, Springfield Technical Community College
Dr. Philip Craiger, University of Central Florida
Mark Krawcyzk, Greenville Technical College
David Pope, Ozarks Technical Community College

Special thanks goes to my best friend, wife, and co-writer, Dawn, whose skills and insight made this project possible. Also, thanks to my family for their patience and support and to Ann Marie for starting this journey.

TABLE OF Contents

CHAPTER FIVE

CHAPTER SIX

CHAPTER SEVEN
Intrusion Detection System Concepts 231

CHAPTER EIGHT
Intrusion Detection: Incident Response 271