Introduction

The network security lifecycle requires specialized support and a commitment to best practice standards. In this book, you will learn best practices that draw upon disciplined processes, frameworks, expert advice, and proven technologies that will help you protect your infrastructure and organization. You will learn end-to-end security best practices, from strategy development to operations and optimization.

This book covers the six-step methodology of incident readiness and response. You must take a proactive approach to security; an approach that starts with assessment to identify and categorize your risks. In addition, you need to understand the network security technical details in relation to security policy and incident response procedures. This book covers numerous best practices that will help you orchestrate a long-term strategy for your organization.

Who Should Read This Book?

The answer to this question is simple—everyone. The principles and best practices covered in this book apply to every organization. Anyone interested in network security should become familiar with the information included in this book—from network and security engineers to management and executives. This book covers not only numerous technical topics and scenarios, but also covers a wide range of operational best practices in addition to risk analysis and threat modeling.

How This Book Is Organized

Part I of this book includes Chapter 1 which covers an introduction to security technologies and products. In Part II, which encompasses Chapters 2 through 7, you will learn the six-step methodology of incident readiness and response. Part III includes Chapters 8 through 11 which cover strategies used to protect wireless networks, IP telephony implementations, data centers, and IPv6 networks. Real-life case studies are covered in Part IV which contains Chapter 12.

The following is a chapter-by-chapter summary of the contents of the book.

Part I, "Introduction to Network Security Solutions," includes:

- **Chapter 1, "Overview of Network Security Technologies."** This chapter covers an introduction to security technologies and products. It starts with an overview of how to place firewalls to provide perimeter security and network segmentation while enforcing configured policies. It then dives into virtual private network (VPN) technologies and protocols—including IP Security (IPsec) and Secure Socket Layer (SSL). In addition, this chapter covers different technologies such as intrusion detection systems (IDS), intrusion protection systems (IPS), anomaly detection systems, and network telemetry features that can help you identify and classify security threats. Authentication, authorization, and accounting (AAA) offers different solutions that provide access control to network resources. This chapter introduces AAA and identity management concepts. Furthermore, it includes an overview of the Cisco Network Admission Control solutions that are used to enforce security policy compliance on all devices that are designed to access network computing resources, thereby limiting damage from emerging security threats. Routing techniques can be used as security tools. This chapter provides examples of different routing techniques, such as Remotely Triggered Black Hole (RTBH) routing and sinkholes that are used to increase the security of the network and to react to new threats.

Part II, "Security Lifecycle: Frameworks and Methodologies," includes:

- **Chapter 2, "Preparation Phase."** This chapter covers numerous best practices on how to better prepare your network infrastructure, security policies, procedures, and organization as a whole against security threats and vulnerabilities. This is one of the most important chapters of this book. It starts by teaching you risk analysis and threat modeling techniques. You will also learn guidelines on how to create strong security policies and how to create Computer Security Incident Response Teams (CSIRT). Topics such as security intelligence and social engineering are also covered in this chapter. You will learn numerous tips on how to increase the security of your network infrastructure devices using several best practices to protect the control, management, and data plane. Guidelines on how to better secure end-user systems and servers are also covered in this chapter.

- **Chapter 3, "Identifying and Classifying Security Threats."** This chapter covers the next two phases of the six-step methodology for incident response—identification and classification of security threats. You will learn how important it is to have complete network visibility and control to successfully identify and classify security threats in a timely fashion. This chapter covers different technologies and tools such as Cisco NetFlow, SYSLOG, SNMP, and others which can be used to obtain information from your network and detect anomalies that might be malicious activity. You will also learn how to use event correlation tools such as CS-MARS and open source monitoring systems in conjunction with NetFlow to allow you to gain better visibility into your network. In addition, this chapter covers details about anomaly detection, IDS, and IPS solutions by providing tips on IPS/IDS tuning and the new anomaly detection features supported by Cisco IPS.
- **Chapter 4, "Traceback."** Tracing back the source of attacks, infected hosts in worm outbreaks, or any other security incident can be overwhelming for many network administrators and security professionals. Attackers can use hundreds or thousands of botnets or zombies that can greatly complicate traceback and hinder mitigation once traceback succeeds. This chapter covers several techniques that can help you successfully trace back the sources of such threats. It covers techniques used by service providers and enterprises.
- **Chapter 5, "Reacting to Security Incidents."** This chapter covers several techniques that you can use when reacting to security incidents. It is extremely important for organizations to have adequate incident handling policies and procedures in place. This chapter shows you several tips on how to make sure that your policies and procedures are adequate to successfully respond to security incidents. You will also learn general information about different laws and practices to use when investigating security incidents and computer crimes. In addition, this chapter includes details about different tools you can use to mitigate attacks and other security incidents with your network infrastructure components including several basic computer forensics topics.
- **Chapter 6, "Postmortem and Improvement."** It is highly recommended that you complete a postmortem after responding to security incidents. This postmortem should identify the strengths and weaknesses of the incident response effort. With this analysis, you can identify weaknesses in systems, infrastructure defenses, or policies that allowed the incident to take place. In addition, a postmortem helps you identify problems with communication channels, interfaces, and procedures that hampered the efficient resolution of the reported problem. This chapter covers several tips on creating postmortems and executing post-incident tasks. It includes guidelines for collecting post-incident data, documenting lessons learned during the incident, and building action plans to close gaps that are identified.
- **Chapter 7, "Proactive Security Framework."** This chapter covers the Security Assessment, Validation, and Execution (SAVE) framework. SAVE, formerly known as the Cisco Operational Process Model (COPM), is a framework initially developed for service providers, but its practices are applied to enterprises and organizations. This chapter provides examples of techniques and practices that can allow you to gain and maintain visibility and control over the network during normal operations or during the course of a security incident or an anomaly in the network.

Part III, "Defense-In-Depth Applied," includes:

- **Chapter 8, "Wireless Security."** When designing and deploying wireless networks, it is important to consider the unique security challenges that can be inherited. This chapter includes best practices to use when deploying wireless networks. You will learn different types of authentication mechanisms, including 802.1x, which is used to enhance the security of wireless networks. In addition, this chapter includes an overview of the Lightweight Access Point Protocol (LWAPP), Cisco Location Services, Management Frame Protection (MFP), and other wireless features to consider when designing security within your wireless infrastructure. The chapter concludes with step-by-step configuration examples of the integration of IPS and the Cisco NAC Appliance on the Cisco Unified Wireless Network solution.
- **Chapter 9, "IP Telephony Security."** IP Telephony solutions are being deployed at a fast rate in many organizations. The cost savings introduced with Voice over IP (VoIP) solutions are significant. On the other hand, these benefits can be heavily impacted if you do not have the appropriate security mechanisms in place. In this chapter, you will learn several techniques used to increase the security of IP Telephony networks. This chapter covers how to secure different IP telephony components such as the Cisco Unified CallManager, Cisco Unified CME, Cisco Unity, Cisco Unity Express, and Cisco Unified Personal Assistant. In addition, it covers several ways to protect against voice eavesdropping attacks.
- **Chapter 10, "Data Center Security."** In this chapter, you will learn the security strategies, technologies, and products designed to protect against attacks on your data center from both inside and outside the enterprise. Integrated security technologies, including secure connectivity, threat defense, and trust and identity management systems, create a Defense-in-Depth strategy to protect each application and server environment across the consolidated IP, storage, and interconnect data center networking infrastructure. Configuration examples of different solutions such as the Firewall Services Module (FWSM), the Intrusion Detection/Prevention System Module (IDSM), and the Application Control Engine (ACE) module for the Catalyst 6500 series switches are covered in detail. This chapter also covers the use of Layer 2 to Layer 7 security features in infrastructure components to successfully identify, classify, and mitigate security threats within the data center.
- **Chapter 11, "IPv6 Security."** This chapter covers an introduction to security topics in Internet Protocol Version 6 (IPv6) implementations. Although it is assumed that you already have a rudimentary understanding of IPv6, this chapter covers basic IPv6 topics. This chapter details the most common IPv6 security threats and the best practices that many organizations adopt to protect their IPv6 infrastructure. IPsec in IPv6 is also covered, with guidelines on how to configure Cisco IOS routers to terminate IPsec in IPv6 networks.

Part IV, "Case Studies," includes:

- **Chapter 12, "Case Studies."** This chapter covers several case studies representing small, medium-sized, and large-scale enterprises. Detailed example configurations and implementation strategies of best practices learned in earlier chapters are covered to enhance learning.