Preface

INTRODUCTION

Enterprises today are linking their systems across enterprise-wide networks and VPNs as well as increasing their exposure to customers, competitors, browsers and hackers on the Internet. Each connection magnifies the vulnerability to attack. With the increased connectivity to the Internet and the wide availability of automated cracking tools, enterprises can no longer simply rely on operating system security to protect their valuable corporate data. Furthermore, the exploding use of Web technologies for enterprise intranets and Internet sites has escalated security risks to enterprise data and information systems. It is imperative that Web professionals are trained in techniques to effectively protect their sites from internal and external threats.

PURPOSE

The purpose of this book is to show globally how the Internet is paving the way for secure communications within enterprises and on the public Internet. In addition, the book will provide the fundamental knowledge you need to analyze risks to your system and implement a workable security policy that protects your information assets from potential intrusion, damage or theft. Through dozens of real life scenarios and/or examples, you will learn which countermeasures to deploy to thwart potential attacks. In this book, you will also gain extensive hands-on experience in securing Web communications and Web sites. You will learn the common vulnerabilities of Web sites; as well as, how to carry out secure communications across unsecured networks.

SCOPE

This book will illustrate the importance of Internet security as a method of protection for Internet and intranet based applications. In addition to commercial enterprises and governments, the book will also address, but not be limited to the following line items

as part of extensive hands-on examples that will provide you with practical experience in establishing Internet security:

- Maintaining strong authentication and authenticity.
- Preventing eavesdropping.
- Retaining integrity of information.
- Minimizing the effects of denial-of-service attacks.
- Selecting a firewall topology.
- Evaluating computer and hacker ethics.
- Installing and configuring Microsoft IIS, Netscape iPlanet or Apache.
- Securing your Web browser.
- Auditing and hardening your server operating system.
- Configuring user authentication.
- Implementing host-based access restrictions.
- Using SSL to encrypt Web traffic.
- Creating a certificate authority (CA).
- Implementing a client certificate.
- Configuring your Web server to require client certificates.
- Protecting browsers and servers with a proxy-based firewall.

This book will leave little doubt that a new world infrastructure in the area of Internet security is about to be constructed. No question, it will benefit enterprises and governments, as well as their advanced citizens. For the disadvantaged regions of the world, however, the coming Internet security revolution could be one of those rare technological events that enable traditional societies to leap ahead and long-dormant economies to flourish in security.

TARGET AUDIENCE

This book is primarily targeted toward domestic and international system administrators, government computer security officials, network administrators, senior managers, engineers, sales representatives, marketing staff, WWW Developers, military senior top brass, and other Internet users. This book is valuable for those who require the fundamental skills to develop and implement security policies designed to protect their enterprise's information from attacks, including managers, network and system administrators, technical staff and support personnel. This book is also valuable for those involved in securing Web sites, including Web developers, Webmasters, and systems, network and security administrators. Some experience with Web servers and technologies is required. Basically, the book is targeted for all types of people and organizations around the world that have Internet, extranet, and intranet security concerns. In addition, the targeted audience also includes the following:

- Scientists.
- Engineers.
- Educators.

- Top Level Executives.
- Computer and network security personnel and IT/IS directors.
- Information Technology (IT) and Department Managers.
- Programmers and Technical Staff.
- The massive target market of more than 600 million Internet and intranet users around the world.

ORGANIZATION OF THIS BOOK

The book is organized into fifteen parts as well as an extensive glossary of security, wireless network and Internet networking terms and acronyms at the back. It provides a step-by-step approach to everything you need to know about Internet security. The following detailed organization speaks for itself:

Part I: Introduction To Internet Security

Part One discusses Internet technologies and basic security issues.

Chapter 1, "Internet technologies," discusses securing dynamic content on a Web server. Topics include security considerations that apply to all dynamic content in general, Server Side Includes, Common Gateway Interface, and two ways to wrapper CGI content.

Chapter 2, "Basic Security Issues," is intended to help management successfully navigate a course, by providing an overview of security principles and the technologies which are appropriate for securing the Internet and networks today.

Part II: Establishing Your Organization's Security

Part Two discusses real threats that impact security and the security policy itself, which is the foundation for your protection.

Chapter 3, "Real Threats That Impact Security," discusses, what can you do about all of these real security threats.

Chapter 4, "A Security Policy: The Foundation Of Your Protection," provides technical professionals with the information they need to explain Internet policy issues to policy makers. It provides a construct for linking high-level policy to detailed technical decisions.

Part III: Developing Your Security Policy

The third part of this book discusses the steps you can take now and how to respond to attacks.

Chapter 5, "Steps To Take Now," provides a methodology for the steps you must take now to rapidly develop a risk profile for your enterprise; and, the enterprise requirements you must adhere to in developing an Internet security policy.

Chapter 6, "Responding To Attacks," contains hypothetical sample policy statements that address Internet-based security.

Part IV: Securing The Web Client

Part Four covers threats and vulnerabilities and how to protect your web browser.

Chapter 7, "Threats And Vulnerabilities," presents an overview of these vulnerabilities and threats, and is a marked deviation from the previous Top-20 lists. In addition to Windows and UNIX categories, SANS and NIPC have also included cross-platform applications and networking products.

Chapter 8, "Protecting Your Web Browser," focuses on the security aspects, particularly the risks involved with running any web browser and how to overcome some of these security shortcomings. Internet Explorer and Firefox will be used as examples, as these are the most commonly used, and therefore the most commonly exploited.

Part V: Network Interconnections: A Major Point Of Vulnerability

Part Five covers the basic operating system and TCP/IP concepts; as well as, early system security improvements.

Chapter 9, "Basic Operating System And TCP/IP Concepts," provides you with a much better understanding of the real-world risks of TCP/IP reset attacks. In other words, to better understand the reality of this threat, the aim of this chapter is to provide some background into the basic workings of operating systems and of TCP/IP concepts, and then to build upon this foundation to understand how resets attacks work.

Chapter 10, "Early System Security Improvements," focuses on early system security improvements like DES, shadow passwords and dialback/dialer passwords.

Part VI: Deterring Masqueraders And Ensuring Authenticity

Part six covers the impersonation of users, how masqueraders can iniltrate your system and how to hold your defensive line.

Chapter 11, "Impersonating Users" focuses on the impersonation of users by stolen passwords and the borrowing of IP addresses.

Chapter 12, "How Masqueraders Infiltrate A System," deals with a broad sweep of technologies and issues connected with policing, profiling and privacy as applicable to cyber surveillance and the infiltration of masqueraders.

Chapter 13, "Holding Your Defensive Line," shows you how to thwart blended threats, where a defense-in-depth strategy is the preferred approach. Defense-in-depth relies on the premise that multiple layers of security afford more comprehensive protection than any single mechanism.

Part VII: Preventing Eavesdropping To Protect Your Privacy

Part Seven covers unauthorized listening and looking and the countering or not countering the eavesdropper.

Chapter 14, "Unauthorized Listening And Looking," describes instant messaging and offers a brief overview of some of the security threats associated with the service. It covers the unauthorized listening and looking of IM: Yeah! Eavesdropping!

Chapter 15, "Countering Or Not Countering The Eavesdropper: That's The Question?," answers that question, and provides recommendations to counter or provide support for the eavesdropper either way.

Part VIII: Thwarting Counterfeiters And Forgery to Retain Integrity

Part Eight covers the forger's arsenal and how to shield your asets.

Chapter 16, "The Forger's Arsenal," focuses on the forger's arsenal (hacking e-mail messages; censoring system logs; and, scrambling the routing tables); as well as, the enhancement of the Internet Protocol (IP), called Path Enhanced IP (PEIP), which is designed to eliminate source forgery.

Chapter 17, "Shielding Your Assets," focuses on how to shield your assets through patch management.

Part IX: Avoiding Disruption Of Service To Maintain Availability

Part Nine covers denial-of-service attacks, how to construct your bastions and the importance of firewalls.

Chapter 18, "Denial-Of-Service Attacks," provides information and defenses against Denial of Service (DoS) attacks, which cause networked computers to disconnect from the network or just outright crash due to the delivery of viruses and bombs (nukes) via the Internet and data flooding.

Chapter 19, "Constructing Your Bastions," discusses how to protect your site against the growing community of black-hat hackers, by thinking like they do and seeing the same information.

Chapter 20, "The Importance Of Firewalls," focuses on the importance of firewalls, how they work and what kinds of threats they can protect you from, how to use a packet filter to shield against bombardment, and how to use application proxies to manage Internet communications.

Part X: Configuring Operating System And Network Security

Part Ten discusses operating systems that pose a security risk and network security.

Chapter 21, "Operating Systems That Pose A Security Risk," discusses the problem of operating system security and the social and economic implications for risk management and policy.

Chapter 22, "Network Security," covers network security abuses.

Part XI: Enhancing Web Server Security

Part Eleven discusses how to control access, extend web site security functionality and how to secure web communications with SSL VPNs.

Chapter 23, "Controlling Access," explores how a comprehensive approach simplifies network access management, creates a secure, intelligent wired and wireless environment

and provides affordable network security that detects all users and enforces all enterprise policies at every access point.

Chapter 24, "Extended Web Site Security Functionality," investigates spoofing and phishing attacks and present countermeasures, with regards to extended web site security functionality, while focusing on solutions that protect naïve as well as expert users.

Chapter 25, "Securing Web Communications With SSL VPNs," examines the security risks that arise from securing web communications with SSL VPNs and proposes strategies for remediation.

Part XII: Issuing And Managing Certificates

Part Twelve discusses why digital certificates are used; as well as, certificate authorities and trusting CAs in servers and browsers.

Chapter 26, "Why Digital Certificates Are Used," takes a look at digital certificates (past, present and future) and their potential for deterring phishing attacks and online fraud. It demonstrates the severe pitfalls from First Generation manual vetting of certificate holders and the inherent unreliability of the identity information they contain (which can easily be faked).

Chapter 27, "Certificate Authorities," discusses the use of CAs to verify that the site is who it claims to be.

Chapter 28, "Trusting Cas In Servers And Browsers," briefly touches on some common shared certificate configurations.

Part XIII: Firewalls And Firewall Topologies

Part Thirteen discusses how to provide protecting servers and clients with firewalls, how to choose the right firewall, firewall topologies and how to select the right firewall security topology policy.

Chapter 29, "Protecting Servers And Clients With Firewalls," presents a brief overview of firewall components, types available, and the relative advantages and disadvantages of each. It is intended to lay out a general road map for administrators who wish to publish information for public consumption with regards to protecting servers and clients, while preventing unauthorized access to their private or confidential network.

Chapter 30, "Choosing The Right Firewall," explores, in depth, the aspects of security and exemplifies several existing solutions.

Chapter 31, "Firewall Topologies," focuses on independent utilities that may be assembled to provide an in depth defense against intrusion, extrusion, and collusion.

Chapter 32, "Selecting Firewall Security Topology Policy," helps the responsible manager and firewall administrator create useful policy for the firewall.

Part XIV: Security Management Solutions And Future Directions

Part Fourteen discusses how to identify and respond to security violations; conduct real-time monitoring and auditing; how to limit damage; keep up to date on new threats and

emerging technologies; and, finally the summary, conclusions, and recommendations for the book.

Chapter 33, "Identifying And Responding To Security Violations," describes Internet security tool technology (as part of Internet security management solutions and future directions); and demonstrates how it can help administrators identify potential problems; as well as, make well-informed security decisions that strengthen the Internet's security posture.

Chapter 34, "Real-Time Monitoring And Auditing," focuses on "theoretical best-practices" combined with "real-world practicality" to define a usable policy for the real-time auditing and monitoring of databases. By following the policies outlined in this chapter, you can properly implement a database system that will work well, and provide adequate security for the data it houses.

Chapter 35, "Limiting Damage," focuses on how to limit damage to your computer.

Chapter 36, "Keeping Up ToDate On New Threats," examines components of a comprehensive framework that enables enterprises to enhance their threat-mitigation capabilities, while increasing the return on investment of existing information technology infrastructures. This chapter also looks at the role of a multilayered approach to building and maintaining an effective security ecosystem for enterprises.

Chapter 37, "Emerging Technologies," examines differing views on how to deal with weaknesses in the Internet (specifically Internet security).

Chapter 38, "Summary, Conclusions And Recommendations," focuses on these security principles and presents a summary, conclusion and recommendation for each.

Part XV: Appendices

Seven appendices provide additional resources that are available for Internet security. Appendix A shows how to configure Internet authentication service on Microsoft Windows 2003 server windows 2003 / enhanced. Appendix B discusses Internet security management, resiliency and security. Appendix C contains a list of top Internet security implementation and deployment companies. Appendix D contains a list of Internet security products. Appendix E contains a list of Internet security standards. Appendix F contains a list of miscellaneous Internet security resources. The book ends with Appendix G – a glossary of Internet security related terms and acronyms.

CONVENTIONS

This book uses several conventions to help you find your way around, and to help you find important sidebars, facts, tips, notes, cautions, disclaimers and warnings. They alert you to critical information and warn you about problems.

John R. Vacca
Author and IT Consultant
e-mail: jvacca@hti.net
visit us at http://www.johnvacca.com/

http://www.springer.com/978-0-387-40533-9

Practical Internet Security

Vacca, J.R.

2007, XXI, 536 p. 145 illus., Hardcover
ISBN: 978-0-387-40533-9