

《网络安全从入门到精通》

图书基本信息

书名：《网络安全从入门到精通》

13位ISBN编号：9787121073267

10位ISBN编号：7121073269

出版时间：2008-10

出版社：吴多胜、王杰、王帆 电子工业出版社 (2008-10出版)

页数：374

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《网络安全从入门到精通》

前言

计算机的普及和应用为人们的生活带来了方便。互联网技术的不断发展，使世界成为一个整体，人们可以通过网络学习、购物、交流。可以说，互联网的迅猛发展为人们带来了前所未有的便利。然而，网络也不是完美无缺的，网络给人们带来惊喜的同时，也带来了威胁。目前，网络安全问题在许多国家已经引起了普遍关注，成为当今网络技术的一个重要研究课题，关于网络安全的书籍也层出不穷。其实网络安全不仅仅是技术问题，也是社会问题和法律问题。要解决信息网络的安全问题，必须采取技术和法律等多种手段进行综合治理。本书是作者在信息系统安全方面教学和科研实践的基础上，参考了大量国内外文献资料充实整理而成。旨在使计算机应用、信息系统使用和维护的工程人员，以及大中专院校相关专业的师生重视网络的安全问题，更多地了解和掌握这门学科的基本原理、方法、技术和工具。全书共分10章，围绕计算机网络所涉及的安全问题，讲述了各种相关的安全技术以及具体应用。第1章介绍了网络安全威胁的相关概念；第2章介绍了操作系统的发展以及各操作系统的安全性及其漏洞和防范措施。

《网络安全从入门到精通》

内容概要

《网络安全从入门到精通》从实用的角度出发，内容翔实、有章可循、行文流畅、讲解清晰，具有很强的可读性和实际操作性，必能让读者受益匪浅。

随着网络的日益普及，网络安全防范的重要性和必要性也愈加突出。为了便于读者理解网络安全方面的原理，《网络安全从入门到精通》采用通俗易懂的方式介绍了网络安全涉及的知识。同时《网络安全从入门到精通》还提供了大量的实例和插图。《网络安全从入门到精通》旨在帮助普通计算机用户了解网络安全领域的相关知识，建立安全意识，对保证网络系统的安全具有实际的指导意义。

《网络安全从入门到精通》

书籍目录

入门篇第1章 网络安全概述1.1 网络安全简述1.1.1 物理安全1.1.2 逻辑安全1.1.3 操作系统安全1.1.4 联网安全1.2 安全威胁1.2.1 内部威胁1.2.2 外部威胁1.2.3 中国特色的安全威胁1.2.4 防范措施1.3 网络安全隐患的原因分析1.3.1 薄弱的认证环节1.3.2 系统的易被监视性1.3.3 易欺骗性1.3.4 有缺陷的局域网服务和相互信任的主机1.3.5 复杂的设置和控制1.3.6 无法估计主机的安全性1.4 小结第2章 操作系统安全2.1 操作系统安全基础2.1.1 操作系统概述2.1.2 操作系统的形成和发展2.1.3 操作系统发展现状2.1.4 安全等级标准2.2 漏洞和后门2.2.1 漏洞和后门的概念2.2.2 漏洞和后门的类型2.2.3 漏洞和后门对网络安全的影响2.2.4 漏洞与后门的区别2.3 WindowsNT系统安全2.3.1 WindowsNT的安全等级2.3.2 WindowsNT的安全性2.3.3 WindowsNT的安全漏洞2.4 UNIX系统安全2.4.1 UNIX系统的安全等级2.4.2 UNIX系统的安全性2.4.3 UNIX系统的安全漏洞2.5 Windows2000的安全2.5.1 Windows2000的安全性2.5.2 Windows2000的安全漏洞2.6 WindowsXP的安全2.6.1 WindowsXP的安全性2.6.2 WindowsXP的安全策略。2.7 WindowsVista的安全2.7.1 WindowsVista的安全性2.7.2 WindowsVista的安全漏洞2.8 小结第3章 网络通信协议与安全3.1 TCP / IP协议简介3.1.1 TCP / IP协议3.1.2 以太网和IEEE标准3.2 网络通信安全问题3.2.1 网络通信安全的隐患3.2.2 TCP / IP不同层的安全性3.2.3 网络服务安全漏洞3.2.4 网络窃听与电子欺骗3.2.5 Internet上的威胁3.3 网络协议安全问题3.3.1 IP协议3.3.2 TCP协议和UDP协议3.3.3 Internet控制报文协议(ICMP)3.3.4 简单邮件传输协议(SMTP)3.3.5 文件传输协议(FTP)3.3.6 远程登录协议(Telnet)3.3.7 简单网络管理协议(SNMP)3.3.8 域名系统(DNS)3.4 Web安全3.4.1 Web安全概述3.4.2 CGI安全3.4.3 ActiveX安全3.4.4 Cookies安全3.4.5 SSL加密安全性3.4.6 Web安全的其他问题3.5 WWW欺骗攻击与防御3.5.1 欺骗攻击3.5.2 Web欺骗3.5.3 防御措施3.6 小结提高篇第4章 计算机病毒及其防治4.1 计算机病毒简介4.1.1 计算机病毒的概念4.1.2 计算机病毒的发展及分类4.1.3 计算机病毒的特征4.1.4 计算机病毒的危害4.1.5 计算机病毒实例4.2 反病毒技术4.2.1 计算机病毒的检测4.2.2 计算机病毒的防范4.2.3 已感染病毒计算机的恢复4.3 小结第5章 木马及蠕虫5.1 木马5.1.1 木马概述5.1.2 木马的特征5.1.3 木马的藏匿地点5.1.4 中木马后出现的症状5.1.5 木马的入侵方法5.2 蠕虫5.2.1 蠕虫概述5.2.2 蠕虫病毒的入侵及模式分析5.2.3 蠕虫病毒的解析和防范5.2.4 蠕虫病毒的手工清除5.3 网页恶意代码5.3.1 网页恶意代码概述5.3.2 网页恶意代码防范5.4 小结第6章 网络攻击及防范措施第7章 网络安全防护与检测第8章 Windows系统安全维护第9章 网络病毒及防护第10章 应用安全

章节摘录

网络安全是一门新兴的交叉性学科，综合运用了数学、物理、生物、通信及计算机技术等诸多学科的基础理论和最新研究成果，同时还涉及政治、法律、军事等复杂层面。网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续、可靠、正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据，提高网络系统的安全性已经成为所有计算机网络应用必须考虑和必须解决的一个重要问题，网络信息的保密性、完整性、可用性、真实性和可控性等相关技术问题都成为网络安全研究的重要课题。下面就对这几方面进行说明。(1)保密性：信息的安全性，即不能将信息泄露给非授权用户。(2)完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

《网络安全从入门到精通》

编辑推荐

《网络安全从入门到精通》适用于一切希望了解和学习网络安全的读者使用，既可作为普通计算机用户上网指导方面的参考书，也可作为网络安全培训教材。

《网络安全从入门到精通》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu111.com