<<网络安全技术>>

图书基本信息

书名：<<网络安全技术>>

13位ISBN编号：9787111304661

10位ISBN编号：7111304667

出版时间：2010-6

出版时间：刘化君 机械工业出版社 (2010-06出版)

作者：刘化君

页数：394

前言

随着网络系统及其应用逐渐复杂和庞大，网络攻击和破坏行为也日益普遍和多样化，并不断产生大量新颖的攻击形式，网络安全面临严峻挑战。
网络安全不仅是国内外研究的重大科学问题之一，也已成为影响社会经济发展和国家发展战略的重要因素。
“国之大事，死生之地，存亡之道，不可不察也”（摘自《孙子兵法》）。
正因为如此，网络安全技术教学如何与时俱进，如何使初学者不仅能够较快地达到一个较高的水准，并使其知识和技能与业界当前技术状况和未来发展趋势相一致，已成为一个越来越不容易达到但又必须为之努力追求的目标。
本书面向初学者，以将读者最终引领到一个较高水准为目标，把网络安全理论、安全技术与安全工具几方面的内容有机地结合在一起，通过大量的实例讨论网络安全理论与技术，并对当前网络安全领域所遇到的一些典型问题及解决这类问题的典型方法做了较深入的讨论与阐述。
在力求系统讲解网络安全知识的基础上，理论基础方面的选材和阐述原则是“够用”；技术性内容的选材原则是“典型”和“有发展潜力”，强调的是技术和应用。
学习本书虽不需要读者具备任何网络安全基础知识，但考虑到网络安全是一个高度综合的领域，与计算机科学与技术的其他分支密不要分建议读者先修读操作系统、计算机网络与通信以及有关网络编程方面的知识。
通过阅读本书，读者不仅可以从理论上对网络安全有较深刻的理解，而且可以根据应用实例对网络安全攻击、防护技术有更直观的认识。
网络安全是一门综合性很强的新兴学科，涉及的内容较多。
本书按照网络安全理论基础、网络攻击与防护、网络安全应用和网络安全实验4个部分架构了一个网络安全知识体系，共包含9章内容。
第1部分为网络安全理论基础，包含第1-4章，主要介绍了网络安全的基本概念、网络安全体系结构、网络协议的安全性以及网络系统平台安全。
作为实例，介绍了Windows系列操作系统的安全配置与操作。
第2部分由第5章和第6章组成，主要讨论网络攻击与防护技术。
首先详细介绍了网络攻击技术“五部曲”（信息收集、获得系统或管理员权限、攻击、种植后门、在网络中隐身）。
然后就网络侦察、拒绝服务攻击、缓冲区溢出、欺骗攻击、服务端口管理等内容进行了比较全面的讲解。
关于网络防护，主要讨论了防火墙技术、入侵检测技术、恶意代码防范与应急响应等内容。
最后，简单介绍了网络攻击取证与安全审计等网络安全监控技术。
第3部分为第7章和第8章，这两章以网络的安全应用为主题，讲解了数据加密与解密技术在网络安全中的应用、认证技术及公开密钥基础设施（PKI），并就作者在信息隐藏方面的研究成果做了简单介绍。
然后讨论了IP安全、虚拟专用网（VPN）、安全电子邮件和Web安全技术等内容。

<<网络安全技术>>

内容概要

《网络安全技术》内容共9章，包含网络安全理论基础、网络攻击与防护、网络安全应用及网络安全实验4个部分。
网络安全理论基础部分讲解了网络安全的基础知识、网络安全体系结构、网络协议的安全性以及网络系统平台安全，、使读者初步了解网络安全并掌握网络安全技术的架构。
网络攻击与防护部分从攻与防两个角度讲解网络安全技术，包括网络攻击原理及技术、网络安全防护技术。
网络安全应用部分讲解了密码技术在网络安全中的应用、网络安全应用。
网络安全实验部分从搭建网络安全实验环境开始，分11个项目比较全面地讲解了攻与防等实验：使课程理论与实践紧密地结合起来。
《网络安全技术》内容丰富，技术性强，实现了网络安全理论与应用完美的结合，给读者以实用和最新的网络安全技术。
《网络安全技术》适用范围广，既可以作为高等院校网络安全课程的教材和教学参考书，又可作为网络安全培训教材或自学参考书；对于具有一定网络管理、网络安全基础，并希望进一步提高网络安全技术水平的读者，也是一本理想的技术参考书。

作者简介

刘化君（1954-），山东临沂人，南京工程学院通信工程学院院长、教授，长期从事“计算机网络与通信”的教学与科研工作。
在清华大学学报等学术刊物上发表《高速路由器中一种实现QoS保证的分组转发方案》（EI收录）学术论文60余篇；编著出版《计算机网络与通信》、《网络编程与计算机技术》和《综合布线系统》等著作（普通高等教育“十一五”国家级规划教材）13部，其中获山东省教育厅科技进步奖著作二等奖1项；主持完成《网络处理器路由队列管理与分组调度》等江苏省高校自然科学计划基金项目3项，以及多项省市重点计算机网络工程及应用软件开发研究项目；“电气与电子信息类应用型人才培养体系创新与实践”教学改革研究项目获高等教育国家级教学成果二等奖。

<<网络安全技术>>

书籍目录

章节摘录

插图：信息网络的迅速发展普及应用，在给人们的工作、生活带来巨大便利的同时，也带来了许多安全隐患，出于政治、经济、文化等利益的需要或者好奇心的驱动，网络攻击事件层出不穷、屡见不鲜，且有愈演愈烈之势，轻者给个人或机构带来信息损害、经济利益损失，重者将会影响国家的政治、经济和文化安全。
因此，信息网络安全问题已成为国内外重大的研究课题之一。
信息网络安全是一个非常复杂的综合性问题，涉及到诸多因素，包括技术、产品和管理。
网络安全主要研究信息网络的安全理论、安全应用和安全管理技术，确保网络免受各种威胁和攻击，以便能够正常工作。
本章主要介绍网络安全的基本概念、网络安全风险及其评估、网络安全策略；然后讨论信息网络安全研究的主要内容、关键技术以及发展趋势。
1.1 何谓网络安全互联网技术的普及应用，使得信息突破了时间和空间上的障碍，信息的价值在不断提高。
，然而，计算机技术、网络技术及信息技术也与其他科学技术一样是一把双刃剑。
当大部分人使用信息技术提高工作效率，为社会创造更多财富的同时，也有一些人在利用信息技术做着相反的事情。
他们非法侵入他人的计算机系统窃取机密信息、篡改和破坏数据，给社会造成难以估量的巨大损失。
网络安全越来越成为关系国计民生的大事，已经引起了全社会的高度重视。
网络安全涉及到网络和通信，并不像初次接触这个领域的人想象的那样简单。
网络安全所涉及的内容很多，先介绍一些有关信息安全、网络安全的基本概念。
1.1.1 安全的历史回顾“ 安全 ”一词在字典中被定义为“ 远离危险的状态或特性 ”和“ 为防范间谍活动或蓄意破坏、犯罪、攻击或逃跑而采取的措施 ”。
这是在广泛意义上对安全的表述。
对信息技术而言，纵观其快速发展与广泛的应用，信息安全的含义也有一个不断丰富和发展的过程。
根据社会对信息安全的需求，它经历了三个重要的发展阶段。
第一个阶段是通信安全阶段，这一历史时期比较长。
在远古时代，就有了信息安全的概念。
早期，所有的资产都是物理的，重要的信息也是物理的，保护这种信息，也是采取一些物理性的手段，如深藏密宫、护卫把守等，可将之称为物理安全。
这时信息传递通常也只能用信使完成，飞鸽传书也算是一种信息传递方式。
物理安全存在许多安全缺陷，如果报文在传递过程中被截获，则报文的信息就会被敌人知悉。
因此产生了通信安全问题。
早在公元前600年Julius Caesar发明了凯撒密码（Caesar Cipher），报文即使被截获也无法读懂。
此后，加密报文这个概念得到了迅速发展与应用，一直到目前的量子密码。

编辑推荐

《网络安全技术》：普通高等教育“十一五”计算机类规划教材。

版权说明