# <<网络安全技术案例教程>>

## 图书基本信息

书名：<<网络安全技术案例教程>>

13位ISBN编号：9787302218777

10位ISBN编号：7302218773

出版时间：2010-2

出版时间：归奕红、 刘宁 清华大学出版社 (2010-02出版)

作者：归奕红，刘宁 著

页数：375

## 前言

随着计算机技术、现代通信技术和网络技术的发展，尤其是Intemet的广泛应用，计算机网络与人们的工作和生活的联系越来越密切、越来越深入，同时也使网络系统的安全问题日益复杂和突出。
计算机的应用使机密和财富集中于计算机，计算机网络的应用使这些机密和财富随时受到联网用户的攻击威胁。
计算机病毒的肆虐、黑客的非法入侵、重要资料被破坏或丢失，都会造成网络系统的瘫痪。
目前人们已开始重视来自网络内部的安全威胁。
近几年来，有关网络安全的书籍逐渐增多，本书与之相比较，其主要特色有以下三个方面：第一，理论与案例相结合。
本书尽量避免单纯的原理性介绍和复杂的算法介绍等内容，主要从构建一个安全的网络系统的实际需要出发，结合应用型本科和高职高专院校学生的特点，以及广大社会培训机构和个人的实际需要，通过大量的实用案例分析以及详细的实施步骤，培养上述人员分析问题和解决问题的能力，使其具备较强的动手和应用能力，以达到能够胜任网络系统的安全设计与管理工作的目的。
第二，增加了颇具实用价值的内容。
例如，VMware Workstation虚拟环境的搭建及应用，ISA Server 2006的应用配置，snort入侵检测系统的搭建及应用，跨交换机VLAN的设置及应用，申请Thawte公司免费证书实现邮件安全技术，Wowdows Server 2003安全配置及应用等。
通过学习这些知识，读者可以在一台计算机上搭建一个仿真的网络环境，从而进行本书中所有安全技术项目的实践，并掌握很多在其他资料上无法获取的技术方法。
第三，技术资料前沿。
计算机应用技术与网络技术的发展是非常迅速的，为了使本书尽量靠近新知识、新技术的前沿，我们参阅了大量的国内外最新资料，力争反映网络安全技术的最新发展。
本书层次清楚、概念准确、深入浅出、通俗易懂。
本书的编写人员是柳州职业技术学院多年工作在教学第一线的教师，不仅具有丰富的教学经验，还长期对外进行技术服务，具有丰富的社会实践经验。
书稿的实用价值也在授课及实际项目实施过程中得到了验证。
本书第1、第6、第8～10章（除9.4、9.12节外）及第7.2、第7.4～第7.6节由归奕红编写，第2、第4、第5章由刘宁编写，第3章由曾春编写，第7.1、第7.3、第7.7、第7.8节由罗海波编写，第9.4、第9.12节由陆晓希编写，全稿由归奕红和刘宁统编和审阅。
参加本书编写的人员还有黄光明、谭耀坚、聂伟、韦柳凤、姚强等。

# <<网络安全技术案例教程>>

## 内容概要

《网络安全技术案例教程》紧密结合当前网络安全技术的发展，用通俗易懂的语言，概括介绍了网络安全知识；深入浅出地介绍了病毒、木马及恶意软件的防范、黑客攻击及其防御、防火墙、ISA Server 2006的应用配置、IDS与IPS、网络安全隔离、PKI与加密技术、Windows Server 2003安全配置、系统安全风险评估的基础知识与应用技术。

《网络安全技术案例教程》在编写过程中遵循理论与实践相结合的原则，提供了大量的网络安全应用实例，以使读者在掌握计算机网络安全基本原理的同时，能够胜任网络系统的安全设计与管理工作。

《网络安全技术案例教程》每章课后均附有习题，能够帮助读者开阔思路，加深对所学内容的理解和掌握。

《网络安全技术案例教程》适合作为应用型本科计算机类和通信类专业的课程教材，也可作为高职高专计算机类和通信类专业及相近专业的课程教材，还可作为系统管理员、安全技术人员的培训教材或工作参考书。

# <<网络安全技术案例教程>>

## 书籍目录

## 章节摘录

插图：2.安装杀毒软件即可预防所有病毒的入侵任何一款杀毒软件都不能保证能完全查杀所有已知和未知的病毒，何况杀毒软件查杀某一病毒的能力总是滞后于该病毒的出现，所以当病毒库代码还没有来得及更新之前，这些新病毒仍可能成功入侵系统。
3.不上互联网就不会感染病毒病毒主要是通过互联网进行传播，但并不意味着不上互联网就不会感染病毒，病毒还可以通过U盘、移动硬盘和光盘等存储媒介传播。
局域网中只要有一台计算机感染了病毒，则整个局域网都很可能受到感染。
4.文件属性设置为只读就可以拒绝病毒病毒或黑客程序可以修改文件属性，因此，设置只读并不能有效防毒。
为了防止病毒感染，可以采取对文件夹或文件进行数据加密的方法，这样病毒就无法感染其中的文件了。
5.在每台计算机中安装单机版杀毒软件与安装网络版杀毒软件等效有些企业为了节省成本，购买单机版杀毒软件，他们认为在每台计算机上安装这些单机版杀毒软件与安装网络版杀毒软件等效。
这种认识是非常错误的。
网络版杀毒系统不等于在每台机器上安装杀毒软件，它的核心是集中的网络防毒系统管理。
网络版杀毒软件可以在一台服务器上通过安全中心控制整个网络的客户端杀毒软件进行同步病毒查杀、软件系统升级，同时架空整个网络的病毒，使病毒无处藏身。
而单机版杀毒软件只能孤军作战，很难实现整个网络同步进行病毒查杀和软件升级、更新。
此外，网络版杀毒软件可以在一台服务器上进行统一的病毒防护策略部署。
这对于整个网络的管理非常方便，而单机版杀毒软件是不可能做到的。
如果网络规模比较大，要为每台计算机单独进行防护配置几乎是不可能的。
6.安装多个杀毒和防火墙软件可以使系统更安全这种观点并不是完全错误，但很不现实。
不同的杀毒软件和防火墙软件的防毒和防攻击能力不一样，实验证明，使用某个杀毒软件对系统进行全面查杀后，再用另外的杀毒软件还能查出一些病毒、木马和恶意软件。
但是在企业网络中，如果安装多个杀毒和防火墙软件，不仅增加了大量的成本，还会严重影响网络性能，何况大多数杀毒和防火墙软件的绝大部分功能是相同的，如此做法所获得的好处不大。
此外，不同品牌的杀毒软件和防火墙软件还可能存在冲突，甚至根本不能安装或运行。
7.网络安全威胁主要来源于外部网络《信息周刊》研究部2008年的调查显示，60%以上的网络威胁和攻击来自网络内部，如未经授权的雇员对文件或数据的访问、带有公司数据的可移动设备遗失或失窃等。
但是这一点却并没有引起企业足够的重视，许多网络管理员和企业领导还一直认为，只要做好对外部网络攻击的防范就可以保障网络安全了。

## 编辑推荐

《网络安全技术案例教程》：21世纪高职高专规划教材·计算机应用系列

# <<网络安全技术案例教程>>

## 版权说明