

<<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

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：<http://www.tushu007.com>

## <<网络安全技术案例教程>>

### 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Internet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。

## 书籍目录

第1章 网络安全概述1.1 网络安全考虑1.1.1 网络的主要安全隐患1.1.2 常见的网络安全认识误区1.1.3 备份与容灾1.2 网络安全设计原则1.3 网络安全的法律和法规1.3.1 国外的相关法律和法规1.3.2 我国的相关法律和法规1.4 习题第2章 病毒、蠕虫和木马的清除与预防2.1 计算机病毒2.1.1 计算机病毒的主要特点2.1.2 广义计算机病毒的分类2.1.3 计算机病毒的发展趋势2.2 计算机病毒防护软件2.3 部署企业网络防病毒系统2.3.1 Symantec NAV 10.1企业版概述2.3.2 Symantec NAV 10.1部署过程2.3.3 设置Symantec控制台2.3.4 Symantec网络防病毒系统应用2.4 蠕虫病毒2.4.1 蠕虫病毒的定义和危害性2.4.2 蠕虫病毒的工作模式2.4.3 蠕虫病毒的基本特征2.4.4 蠕虫病毒的预防措施2.5 狙击波蠕虫病毒防护2.5.1 狙击波蠕虫病毒概述2.5.2 狙击波蠕虫病毒防护步骤2.6 木马2.6.1 木马概述2.6.2 木马的组成2.6.3 木马的攻击原理2.6.4 木马的危害2.6.5 木马的识别和清除2.7 木马的安装及使用2.7.1 B02K概述2.7.2 B02K安装与使用步骤2.8 木马防范工具的使用2.8.1 木马克星2009简介2.8.2 木马克星2009应用2.9 流氓软件2.9.1 流氓软件的主要特征2.9.2 流氓软件分类2.9.3 流氓软件的防范2.10 习题第3章 黑客攻击及其防御3.1 认识黑客及其攻击手段3.1.1 黑客与黑客攻击3.1.2 黑客攻击的手段3.2 黑客攻击的基本步骤3.2.1 收集初始信息3.2.2 查找网络地址范围3.2.3 查找活动机器3.2.4 查找开放端口和人口点3.2.5 查看操作系统类型3.2.6 弄清每个端口运行的服务3.3 拒绝服务攻击与防范3.3.1 使用 Sniffer 软件监视网络的状态3.3.2 防范方法3.4 习题第4章 防火墙4.1 防火墙概述4.1.1 防火墙定义4.1.2 防火墙的主要功能4.1.3 与防火墙有关的主要术语4.2 防火墙的分类4.2.1 按防火墙的软、硬件形式划分4.2.2 按防火墙性能划分4.3 主要防火墙技术4.3.1 包过滤技术4.3.2 应用代理技术4.3.3 状态检测技术4.4 防火墙的体系结构4.4.1 双宿主堡垒主机体系结构4.4.2 被屏蔽主机体系结构4.4.3 被屏蔽子网体系结构4.5 防火墙配置的基本原则4.6 防火墙的选择4.7 Windows 防火墙4.7.1 windows 防火墙的一般设置方法4.7.2 Windows 防火墙的应用4.8 习题第5章 ISA Server 2006 的应用配置5.1 ISA Server 简介5.1.1 ISA Server 2006 的主要功能5.1.2 多网络结构5.1.3 防火墙的设置种类和网络模板5.1.4 ISA Server 与VPN的集成5.1.5 ISA Server 缓存的种类5.1.6 ISA Server 与其他软件防火墙的比较5.2 利用VMware Workstation 建立测试环境5.2.1 VMware Workstation 概述5.2.2 搭建ISA Server 2006 测试环境的步骤5.3 ISA网络配置和网络规则5.3.1 网络和网络集配置5.3.2 应用网络模板5.3.3 网络规则5.4 安装ISA Server 20065.4.1 安装前的准备5.4.2 安装ISA Server 20065.4.3 测试ISA Server 防火墙是否安装成功5.5 ISA防火墙策略5.5.1 ISA防火墙策略工作方式5.5.2 防火墙访问规则5.5.3 ISA防火墙发布规则5.6 ISA Server的网页缓存5.6.1 网页缓存概述5.6.2 搭建网页缓存测试环境5.6.3 缓存设置5.6.4 设置缓存规则5.6.5 缓存区内容的更新5.7 ISA Server 客户端的应用5.7.1 ISA Server 客户端概述5.7.2 搭建ISA Server 客户端测试环境5.7.3 ISA Server 的配置5.7.4 web 代理客户端的配置5.7.5 Secure NAT 客户端的配置5.7.6 防火墙客户端的配置5.8 开放访问Internet5.8.1 访问Internet概述5.8.2 创建访问规则5.8.3 开放FTP写入的功能和开放非标准连接端口5.9 开放或阻挡实时通信软件5.9.1 实时通信软件概述5.9.2 开放或阻挡腾讯QQ测试环境5.9.3 开放腾讯QQ实时通信步骤5.10 习题第6章 IDS与IPS6.1 入侵检测系统概述6.1.1 入侵检测系统的功能6.1.2 入侵检测系统的模型6.1.3 入侵检测技术及其发展趋势6.1.4 入侵检测的流程6.2 入侵检测系统的分类6.2.1 基于主机的入侵检测系统6.2.2 基于网络的入侵检测系统6.2.3 混合型入侵检测系统6.3 典型入侵检测产品介绍6.3.1 金诺网安入侵检测系统KIDS6.3.2 华强IDS.....第7章 网络安全隔离第8章 Windows Server 2003安全配置第10章 系统安全风险评估参考文献

## 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，它的核心是集成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。

<<网络安全技术案例教程>>

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

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:<http://www.tushu007.com>