第一图书网, tushu007.com

<<计算机网络安全与应用技术>>

图书基本信息

书名：<<计算机网络安全与应用技术>>

13位ISBN编号：9787111302285

10位ISBN编号：7111302281

出版时间：2010-5

出版时间：机械工业出版社

作者：张兆信　等编著

页数：258

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

前言

本书按高职高专实施素质教育的实际需求进行编写。
作者均为多年从事网络安全教学和网络安全设计及实践，并有丰富高职高专教学经验的教师。
本书内容以计算机网络安全为重点，兼顾基础理论，以通俗的语言、丰富的实例和“理论+工具+分析实施”的形式，由浅入深地对计算机网络安全相关理论、应用技术、工具及实施方法进行了系统介绍。
使读者快速掌握书中内容。
在本书的编写过程中，注重内容的取舍，能力求反映最新技术。
对于所用的一些软件，为了使读者便于查找，都给出了相关网址。
本课程建议授课学时为40学时，其中理论为20学时，实践为20学时。
本书第1章介绍计算机网络安全概述；第2章介绍计算机网络系统的硬件防护技术；第3章介绍加密技术；第4章介绍备份技术；第5章介绍防火墙技术；第6章介绍计算机操作系统的安全与配置；第7章介绍计算机病毒；第8章介绍黑客的攻击与防范；第9章介绍网络入侵与入侵检测。
每章后附有与内容紧密结合的习题或实训。
本书由张兆信、赵永葆、赵尔丹等编著，其中第1、2、3、9章由张兆信、张丽坤编写，第4、5、8章由赵永葆编写，第6、7章由赵尔丹、张照枫编写，全书由张兆信统稿。
由于作者水平有限，书中出现的错误和不妥之处，敬请读者批评指正。
本书还配有电子教案，读者可在机械工业出版社网站上下载。

内容概要

本书围绕计算机网络安全，对网络安全相关的理论、工具及实施方法进行了系统介绍，内容包括计算机网络安全概述、计算机网络系统的硬件防护技术、加密技术、备份技术、防火墙技术、计算机操作系统的安全与配置，以及计算机病毒、黑客的攻击与防范和网络入侵与入侵检测。

本书本着“理论知识以够用为度，重在实践应用”的原则，以“理论+工具+分析实施”为主要形式编写。
主要章节都配合内容提供了应用工具及分析实施的相关实例，每章都配有习题或实训。

本书适合作为高职高专计算机专业、网络专业及相近专业的教材，也可供有关工程技术人员和自学者使用。

书籍目录

出版说明
前言
第1章 计算机网络安全概述
1. 1 计算机网络安全事件
1. 2 计算机网络安全的含义及安全等级
1. 3 计算机网络系统的脆弱性及安全威胁
1. 4 计算机网络安全的体系结构
1. 5 计算机网络安全设计
1. 6 网络安全意识与教育
1. 7 网络安全的管理策略
1. 8 习题
第2章 计算机网络系统的硬件防护技术
2. 1 影响实体安全的主要因素
2. 2 计算机的安全维护
2. 3 计算机机房建设与安全防护
2. 4 实训
2. 5 习题
第3章 加密技术
3. 1 加密概述
3. 2 传统加密方法(对称密码)
3. 2. 1 数据加密标准
3. 2. 2 其他对称分组密码
3. 3 公钥加密(非对称密码)
3. 3. 1 RSA公钥加密
3. 3. 2 DH公钥加密
3. 4 公钥基础设施
3. 4. 1 数字签名
3. 4. 2 认证及身份验证
3. 5 Kerberos身份认证系统
3. 6 PGF加密系统
3. 7 加密技术的应用
3. 7. 1 Word文件加密解密
3. 7. 2 Foxmail加密解密
3. 7. 3 winRAR加密解密技术
3. 8 使用加密工具加密
3. 8. 1 ABI—CODER的应用
3. 8. 2 电子邮件加密工具A—lock的应用
3. 9 计算机网络加密技术
3. 9. 1 链路加密
3. 9. 2 节点加密
3. 9. 3 端一端加密
3. 10 实训
3. 11 习题
第4章 备份技术
4. 1 备份技术概述

4. 1. 1 备份的概念
4. 1. 2 备份数据的类型
4. 1. 3 备份的方式
4. 1. 4 常用备份存储设备
4. 1. 5 网络备份
4. 2 备份的层次与备份方法
4. 2. 1 备份的层次
4. 2. 2 备份技术
4. 3 Windows XP中的备份与恢复
4. 3. 1 Windows XP中备份的作用
4. 3. 2 Windows XP的备份方法
4. 3. 3 Windows XF中文件(夹)的备份
4. 3. 4 Windows XF中其他重要数据的备份
4. 4 克隆利器——Ghost
4. 4. 1 Ghost介绍
4. 4. 2 用Ghost备份硬盘上的数据
4. 4. 3 Ghost使用注意事项
4. 5 winRAR的使用
4. 5. 1 winRAR介绍
4. 5. 2 winRAR压缩文件
4. 5. 3 winRAR解压文件
4. 6 网络备份方案的设计
4. 6. 1 备份软件
4. 6. 2 日常备份制度
4. 6. 3 灾难恢复措施
4. 7 实训
4. 8 习题
第5章 防火墙技术
5. 1 防火墙概述
5. 1. 1 防火墙概念
5. 1. 2 防火墙的功能
5. 1. 3 防火墙的局限性
5. 2 防火墙的分类
5. 2. 1 网络层防火墙
5. 2. 2 应用层网关
5. 2. 3 复合型防火墙
5. 3 防火墙的选择和使用
5. 3. 1 防火墙的选择原则
5. 3. 2 防火墙的使用误区
5. 4 防火墙的发展趋势
5. 5 防火墙产品实例
5. 5. 1 联想网御2000
5. 5. 2 天网防火墙
5. 6 实训
5. 7 习题
第6章 计算机操作系统的安全与配置
6. 1 Windows XP操作系统的安全性

6．1．1 Windows XP的登录机制
6．1．2 Windows XP的屏幕保护机制
6．1．3 Windows XP的文件保护机制
6．1．4 利用注册表提高Windows XP系统的安全
6．2 Windows 2003的安全基础
6．2．1 Windows 2003的安全基础概念
6．2．2 用户账号的管理
6．2．3 组的管理
6．2．4 Windows 2003的安全模型
6．2．5 Windows 2003的安全机制
6．2．6 Windows 2003的安全性
6．2．7 Windows 2003安全访问控制
6．2．8 在Windows 2003系统中监视和优化性能
6．2．9 Windows 2003的安全措施
6．3 Windows 2008操作系统的安全性
6．3．1 Windows安全
6．3．2 安全配置向导
6．3．3 可信平台模块管理
6．3．4 BitIocker驱动器加密
6．4 UNIX系统的安全性
6．4．1 UNIX操作系统简介
6．4．2 UNIX系统的安全性
6．5 Linux系统的安全性
6．5．1 Linux操作系统简介
6．5．2 Linux系统的常用命令
6．5．3 Linux系统的网络安全
6．6 实训
6．6．1 实训1 Windows XP的密码设置
6．6．2 实训2 Windows 2003／2008用户账户的管理
6．7 习题
第7章 计算机病毒
7．1 计算机病毒概述
7．1．1 计算机病毒的定义
7．1．2 计算机病毒的发展历史
7．1．3 计算机病毒的危害
7．1．4 计算机病毒的特征
7．2 计算机病毒的分类
7．3 计算机病毒的工作原理
7．3．1计算机病毒的结构
7．3．2引导型病毒的工作原理
7．3．3 文件型病毒的工作原理
7．4 反病毒技术
7．4．1 反病毒技术的发展
7．4．2 病毒防治常用方法
7．4．3 Windows病毒防范技术
7．5 知名计算机病毒介绍
7．5．1 CIH病毒

7．5．2 Word宏病毒
7．5．3 冲击波病毒
7．5．4 振荡波病毒
7．5．5 熊猫烧香病毒
7．5．6 其他类型病毒
7．6 常用杀毒软件
7．6．1 瑞星杀毒软件
7．6．2 江民杀毒软件
7．6．3 卡巴斯基反病毒软件
7．7 实训
7．8 习题
第8章 黑客的攻击与防范
8．1 关于黑客
8．2 黑客攻击的步骤与防范
8．2．1 黑客攻击的步骤
8．2．2 防范黑客原则
8．3 端口扫描与安全防范
8．3．1 端口的概念
8．3．2 端口的分类
8．3．3 端口扫描
8．3．4 端口扫描的安全防范
8．4 拒绝服务攻击与防范
8．4．1 拒绝服务攻击的概念
8．4．2 分布式拒绝服务攻击
8．4．3 拒绝服务攻击的防范
8．5 网络监听与防范
8．5．1 网络监听的工作原理
8．5．2 网络监听的检测和防范
8．6 木马与安全防范
8．6．1 木马的概念
8．6．2 木马的种类
8．6．3 木马工具——冰河
8．6．4 木马的防范
8．6．5 木马的清除
8．7 邮件炸弹
8．7．1 邮件炸弹的概念
8．7．2 预防邮件炸弹
8．8 实训
8．9 习题
第9章 网络入侵与入侵检测
9．1 网络入侵
9．1．1 入侵目的及行为分类
9．1．2 入侵步骤
9．2 入侵检测
9．2．1 入侵检测系统定义
9．2．2 入侵检测的必要性
9．2．3 入侵检测系统分类

9．2．4 入侵检测系统发展的一些方向
9．3 常用入侵检测系统
9．3．1 IDS的硬件主要产品
9．3．2 IDS的主要软件产品
9．3．3 Snort应用
9．4 入侵检测系统与防火墙联动技术
9．5 实训
9．6 习题
参考文献

章节摘录

插图：随着计算机网络技术的发展和普及，全球信息化已成为人类发展的大趋势。
计算机网络的快速发展使得网上资源越来越丰富，电子商务、电子政务、电子税务、电子海关、网上银行、网络防伪等诸多新兴业务也迅速兴起，又由于Internet的国际化、社会化、开放化、个人化4个特点，使得网络安全问题变得越来越重要，计算机网络犯罪所造成的经济损失令人吃惊，而且在许多时候网络侵入所造成的后果远远不能用经济损失来衡量。
下面是来自公开媒体的一些典型安全事件。
Pakistan病毒：巴锡特（Basit）和阿姆杰德（Amjad）两兄弟是巴基斯坦的拉合尔（La.hore）人，经营着一家IBM-PC及其兼容机的小商店。
1996年初，他们编写了Pakistan病毒，即c-Brain病毒。
一般而言，业界都公认这是真正具备完整特征的电脑病毒始祖。
他们的目的主要是为了防止自己的软件被任意盗拷，只要有人盗拷他们的软件，C.Brain就会发作，将盗拷者的硬盘剩余空间给吃掉。
1988年美国典型计算机病毒入侵计算机网络的事件：1988年11月2日，美国有6000多台计算机被病毒感染，造成Internet不能正常运行。
这次非常典型的计算机病毒入侵计算机网络的事件，迫使美国政府立即作出反应，国防部也成立了计算机应急行动小组。
这次事件中遭受攻击的有5个计算机中心和12个地区节点，它们连接着政府、大学、研究所和拥有政府合同的25万台计算机。
这次病毒事件给计算机系统造成的直接经济损失就达9600万美元。
这个病毒程序的设计者是罗伯特·莫里斯（RobertT.Morris），当年23岁，在康乃尔（Comell）大学攻读研究生学位。
黑客侵入美国军方及美国航空航天局网络典型事件：1996年12月，黑客侵入美国空军的全球网网址并将其主页肆意改动，迫使美国国防部一度关闭了其他80多个军方网址。
2002年11月12日，美国联邦政府对一名英国计算机管理员提起诉讼，指控他非法侵入了美军和美国航空航天局的92处计算机网络，其中在侵入新泽西州一处海军设施的网络时导致该设施系统陷入崩溃。
考生答卷被删事件：2002年江苏省普通高中信息技术等级考试，由于“黑客”入侵，有近万名考生的答卷被删，造成了非常恶劣的后果。
之后，“黑客”以破坏网上考试被判刑6个月。
17岁黑客害了11万台计算机：17岁的犯罪嫌疑人池勇是黑龙江省七台河市一所高级中学的在校生，他自己经营了一个“混客帝国”网站，从事病毒攻击、盗取数据、非法交易等危害网络安全的行为。

编辑推荐

《计算机网络安全与应用技术》是普通高等教育“十一五”国家级规划教材,全国高等职业教育规划教材

第一图书网, tushu007.com

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