

<<网络安全与管理>>

图书基本信息

书名：<<网络安全与管理>>

13位ISBN编号：9787302299493

10位ISBN编号：7302299498

出版时间：2012-10

出版时间：张素娟、吴涛、朱俊东 清华大学出版社 (2012-10出版)

作者：张素娟，吴涛，朱俊东 著

页数：401

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>

## <<网络安全与管理>>

### 内容概要

《高等院校计算机教育系列教材：网络安全与管理》结合作者多年从事网络管理的经验，由浅入深地介绍了网络安全和网络管理的相关内容。

从基础理论知识，到实际应用，再到具体配置，结合例证和最新技术发展及趋势，全面介绍了如何加强网络的安全性和可管理性。

本内容理论充足，覆盖范围广泛、层次分明。

全书共分为11章，各章的主要内容说明如下：第1、2章介绍了网络安全的基本概念、基本要求、安全体系和安全协议等基础理论知识；第3章介绍了加密及加密算法的相关理论；第4~6章分别从操作系统、Web站点和邮件系统出发介绍了相关的安全知识；第7章介绍了如何使用防火墙加强内网的安全性；第8章介绍了病毒的危害、种类及如何预防；第9章介绍了网络攻击及防护的相关知识；第10、11章介绍了网络管理的基本理论和技术，以及相关的网管软件。

综观全书，既有理论讲解，也有实际应用；既介绍了主流技术，也介绍了新技术的发展动向。

《高等院校计算机教育系列教材：网络安全与管理》既可以作为大学本科计算机及信息相关专业的教材，也为网络管理人员提供了很好的参考。

## 书籍目录

第1章 网络安全概述 1.1 网络安全现状及趋势 1.1.1 网络安全的主要威胁 1.1.2 网络系统的脆弱性 1.1.3 网络安全现状 1.1.4 网络安全的发展趋势 1.2 网络安全概述 1.2.1 网络安全的含义及技术特征 1.2.2 网络安全的研究目标和研究的内容 1.2.3 网络安全防护技术 1.3 实体安全概述 1.3.1 实体安全的概念 1.3.2 机房基础设施安全 1.3.3 机房环境安全 1.3.4 设备的安全保护 1.4 网络安全评估 1.4.1 安全风险评估 1.4.2 国外安全评估标准 1.4.3 国内安全评估标准 1.5 本章小结 1.6 课后习题 第2章 网络安全基础 2.1 网络安全体系结构 2.1.1 开放系统互连参考模型 2.1.2 Internet网络体系层次结构 2.1.3 网络安全层次特征体系 2.1.4 IPv6的安全性 2.2 网络协议安全分析 2.2.1 物理层安全 2.2.2 网络层安全 2.2.3 传输层安全 2.2.4 应用层及网络应用安全 2.2.5 安全协议的最新发展 2.3 安全服务与安全机制 2.3.1 安全服务 2.3.2 安全机制 2.3.3 安全机制与安全服务之间的关系 2.4 网络操作命令 2.4.1 ipconfig 2.4.2 ping 2.4.3 arp 2.4.4 nbtstat 2.4.5 netstat 2.4.6 tracert 2.4.7 net 2.4.8 nslookup 2.5 本章小结 2.6 课后习题 第3章 密码和加密技术 3.1 密码技术概述 3.1.1 密码技术的相关概念 3.1.2 密码体制 3.1.3 数据加密方式 3.2 加密解密算法 3.2.1 对称密码算法 3.2.2 非对称密码算法 3.3 常用加密解密技术 3.3.1 对称加密技术 3.3.2 非对称加密及单向加密 3.4 密钥管理和数字证书 3.4.1 密钥管理 3.4.2 公钥基础设施 (PKI) 3.4.3 数字签名 3.4.4 数字证书 3.5 本章小结 3.6 课后练习 第4章 操作系统安全 4.1 操作系统安全基础 4.1.1 安全操作系统的概念 4.1.2 网络操作系统的安全性要求 4.1.3 操作系统的安全机制和安全模型 4.2 Windows 7操作系统的安 4.2.1 Windows 7的操作系统的安 4.2.2 用户账户和用户账户控制 4.2.3 Action Center的安全配置 4.2.4 防火墙设置 4.2.5 Windows Defender实时保护 4.2.6 Windows 7的其他安全功能 4.3 Unix/Linux操作系统的安 4.3.1 Unix/Linux操作系统的安 4.3.2 Unix/Linux系统安全配置 4.4 灾难备份和恢复 4.4.1 灾难备份 4.4.2 灾难恢复 4.5 本章小结 4.6 课后习题 第5章 Web安全 5.1 Web安全基础 5.1.1 Web应用的基础概念 5.1.2 Web应用的架构 5.2 Web的入侵方法 5.2.10Day ( Zero Day Attack ) 5.2.2 ASP上传漏洞 5.2.3 注入漏洞 5.2.4 Cookies欺骗 5.2.5 旁侵 ( 旁注 ) 5.3 Web欺骗与防护机制 5.3.1 Web欺骗 5.3.2 Web欺骗的预防 5.4 Web服务器安全机制 5.4.1 对于单独服务器安全配置 5.4.2 服务器群安全 5.5 Web客户安全机制 5.5.1 安全措施 5.5.2 安全注意事项 5.6 本章小结 5.7 课后习题 第6章 电子邮件安全 6.1 电子邮件系统概述 6.1.1 电子邮件系统原理 6.1.2 邮件系统安全性要求 6.2 电子邮件安全协议 6.2.1 SMTP协议 6.2.2 POP3协议 6.2.3 IMAP4协议 6.2.4 PEM协议 6.2.5 PGP 6.2.6 S/MIME 6.3 邮件服务器安全机制 6.3.1 防垃圾邮件 6.3.2 防邮件欺骗 6.3.3 邮件炸弹 6.4 客户端安全措施 6.4.1 信任中心 6.4.2 拒收垃圾邮件 6.5 本章小结 6.6 课后习题 第7章 防火墙应用技术 7.1 防火墙概述 7.1.1 防火墙的定义和安全要素 7.1.2 防火墙技术的发展历程和未来趋势 7.1.3 影响防火墙性能的关键指标 7.1.4 分布式防火墙 7.2 防火墙部署类型 7.3 防火墙的主要应用 7.3.1 应用包过滤技术实现访问控制规则 7.3.2 应用状态检测技术实现动态包过滤 7.3.3 应用层代理网关技术 7.3.4 防火墙安全操作系统 7.4 典型防火墙的配置 7.5 本章小结 7.6 课后习题 第8章 计算机病毒与反病毒技术 8.1 计算机病毒概述 8.1.1 计算机病毒的定义 8.1.2 计算机病毒的基本特征及发展特点 8.1.3 计算机病毒的分类 8.1.4 计算机病毒的发展概述 8.2 计算机病毒惯用技术 8.2.1 引导型病毒的技术特点 8.2.2 文件型病毒的技术特点 8.2.3 宏病毒的技术特点 8.2.4 网络蠕虫病毒的技术特点 8.2.5 计算机病毒的其他关键技术 8.3 病毒的检测和查杀 8.3.1 计算机反病毒技术的4个发展阶段 8.3.2 常见的病毒检测和查杀方法 8.3.3 杀毒软件的基本工作原理 8.4 恶意软件的防护和查杀 8.4.1 恶意软件的特征和分类 8.4.2 恶意软件的传输机制 8.4.3 恶意软件防御技术 8.5 本章小结 8.6 课后习题 第9章 网络攻防和入侵检测 9.1 网络攻击概述 9.1.1 网络攻击的概念 9.1.2 网络攻击的类型 9.1.3 网络攻击的手段 9.1.4 网络攻击在我国的发展过程 9.2 探测技术 9.2.1 踩点 9.2.2 扫描 9.2.3 查点 9.3 攻击技术 9.3.1 窃听技术 9.3.2 欺骗技术 9.3.3 拒绝服务攻击 9.3.4 数据驱动攻击 9.4 隐藏技术 9.5 网络攻击的防御技术 9.5.1 有效预防端口扫描 9.5.2 口令攻击的防范 9.5.3 恶意代码攻击的防范 9.5.4 预防IP欺骗的方法 9.5.5 预防ARP欺骗攻击 9.5.6 RIP路由欺骗的防范 9.5.7 防范DNS欺骗 9.5.8 缓冲区溢出的攻击防范 9.5.9 对拒绝服务攻击的防范 9.6 入侵检测 9.6.1 入侵检测的基本概念 9.6.2 常用的检测技术介绍 9.6.3 入侵检测系统主流产品 9.6.4 入侵检测技术发展趋势 9.7 本章小结 9.8 课后习题 第10章 网络管理原理 10.1 网络管理概述 10.1.1 网络管理的目标和任务 10.1.2 网络管理的基本范畴 10.1.3 网络管理协议的发展历史 10.2 网络管理系统模型 10.2.1 网络管理系统模型设计的目标 10.2.2 网络管理相关概念和基本模型 10.2.3 网络管理功能和参考模型 10.2.4 网络管理的通信模式 10.3 网络管理相关协议 10.3.1 SNMP协议

和CMIP协议概述 10.3.2 SNMP协议基础知识 10.3.3 SNMP协议基本原理 10.4 网络性能管理 10.5 网络故障管理 10.6 本章小结 10.7 课后习题 第11章 网络管理系统 11.1 网络管理系统概述 11.1.1 网络管理系统的功能和分类 11.1.2 网络管理系统的发展概述 11.1.3 网络管理系统的基本架构 11.1.4 网络管理系统实现数据采集的典型示例 11.2 实用网络管理系统 11.2.1 当前主流网络管理系统的介绍 11.2.2 网络管理系统的测评方法 11.2.3 网络管理系统功能应用演示 11.2.4 SNMP简单配置示例 11.3 本章小结 11.4 课后习题 习题答案

## 章节摘录

版权页：插图：在实际的CA认证环境中不可能只有一个CA中心，多个CA中心之间必然存在一个信任关系模型。

信任关系模型建立的目的是确保一个认证机构颁发的证书，能够被其他认证机构的用户所信任。

信任关系模型有：严格层次信任模型、分布式信任模型、以用户为中心的信任模型和交叉认证模型等。

CA认证中心的功能有以下几个方面。

(1) 证书的颁发 认证中心负责接收、验证用户（包括下级认证中心和最终用户）的数字证书申请，同时将申请的内容进行备案，并根据申请的内容确定是否受理该数字证书申请。

如果认证中心接受该数字证书申请，则进一步确定给用户颁发何种类型的证书。

新证书用认证中心的私钥签名以后，发送到目录服务器供用户下载和查询。

为了保证消息的完整性，返回给用户的所有应答信息都要使用认证中心的签名。

(2) 证书的更新 认证中心可以定期更新所有用户的证书，或者根据用户的请求来更新用户的证书。

(3) 证书的查询 证书的查询功能分为两类，一类是证书申请的查询，认证中心根据用户的查询请求返回当前用户证书申请的处理过程；另一类是用户证书的查询，这类查询由目录服务器来完成，目录服务器根据用户的请求返回适当的证书。

(4) 证书的作废 当用户的私钥由于泄密等原因造成用户证书需要申请作废时，用户需要向认证中心提出证书作废的请求，认证中心根据用户的请求确定是否将该证书作废。

另外一种证书作废的情况是证书已经过了有效期，认证中心将自动把证书作废。

证书的作废功能由认证中心通过维护证书作废列表（CRL，Certificate Revocation List）来完成。

(5) 证书的归档 证书都具有一定的有效期，证书过了有效期之后就应该作废。

因为有时可能需要验证以前的某个交易过程中产生的数字签名，因此作废的证书不能简单地丢弃。

基于此类考虑，认证中心还应当具备作废证书和作废私钥的管理功能。

## <<网络安全与管理>>

### 编辑推荐

《高等院校计算机教育系列教材:网络安全与管理》在编写时联系当前技术的发展,加入了大量新的技术和新的应用内容,既充分体现了时代特色,又实实在在地让读者领略到新技术所带来的实惠。

《高等院校计算机教育系列教材:网络安全与管理》既可以作为大学本科计算机及信息相关专业的教材,也为网络管理人员提供了很好的参考。

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>