

## <<网络安全与维护>>

### 图书基本信息

书名：<<网络安全与维护>>

13位ISBN编号：9787305049484

10位ISBN编号：7305049484

出版时间：2007-3

出版时间：南京大学出版社

作者：刘永华

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>

## <<网络安全与维护>>

### 内容概要

网络安全与维护，ISBN：9787305049484，作者：刘永华 主编

## &lt;&lt;网络安全与维护&gt;&gt;

## 书籍目录

第1章 网络安全概述	1.1 网络安全简介	1.1.1 网络安全的概念	1.1.2 网络安全模型
	1.1.3 计算机安全的分级	1.1.4 网络安全的重要性	1.2 网络安全现状
1.3 网络安全威胁	1.3.1 安全攻击	1.3.2 基本的威胁	1.3.3 主要的可实现的威胁
	1.3.4 病毒	1.4 影响网络安全的因素	1.4.1 计算机系统因素
	1.4.2 操作系统因素	1.4.3 网络协议因素	1.4.4 人为因素
1.5 网络安全技术	1.5.1 数据加密与认证	1.5.2 防火墙	1.5.3 入侵检测
	1.5.4 访问控制	1.5.5 病毒防治	复习思考题第2章 操作系统安全
2.1 操作系统的漏洞	2.1.1 系统漏洞的概念	2.1.2 漏洞的类型	2.1.3 漏洞对网络安全的影响
2.2 Windows Server 2003的安全	2.2.1 windows server 2003安全模型	2.2.2 Windows Server 2003安全隐患	2.2.3 Windows Server 2003安全防范措施
2.3 Linux网络操作系统的安全	2.3.1 Linux网络操作系统的基本安全机制	2.3.2 Linux网络操作系统可能受到的攻击	2.3.3 Linux网络安全防范策略
	2.3.4 加强Linux网络服务器的管理	复习思考题第3章 数字加密与认证	3.1 密码学
	3.1.1 加密的起源	3.1.2 密码学基本概念	3.1.3 传统加密技术
	3.1.4 对称密钥算法	3.1.5 公开密钥算法	3.1.6 加密技术在网络中的应用
	3.1.7 密码分析	3.2 密钥管理	3.2.1 密钥的分类和作用
	3.2.2 密钥长度	3.2.3 密钥产生技术	3.2.4 密钥的组织结构
	3.2.5 密钥分发	3.2.6 密钥的保护	3.3 数字签名与数字证书
	3.3.1 电子签名	3.3.2 认证机构(CA)	3.3.3 数字签名
	3.3.4 公钥基础设施(PKI)	3.3.5 数字证书	3.3.6 数字时间戳技术
	3.4 认证技术	3.4.1 身份认证的重要性	3.4.2 身份认证的方式
	3.4.3 消息认证	3.4.4 认证技术的实际应用	3.5 数字证书应用实例
	3.5.1 获得及安装免费数字证书	3.5.2 在IE中查看数字证书	3.5.3 发送安全邮件
	3.5.4 检查Windows是否为微软正版	复习思考题第4章 防火墙技术	4.1 防火墙的基本概念与分类
	4.1.1 防火墙的基本概念	4.1.2 防火墙的作用	4.1.3 防火墙的优缺点
	4.1.4 防火墙的分类	4.2 防火墙技术	4.2.1 包过滤技术
	4.2.2 应用代理技术	4.2.3 状态检测技术	4.2.4 技术展望
	4.3 防火墙的体系结构	4.3.1 双重宿主主机结构	4.3.2 屏蔽主机结构
	4.3.3 屏蔽子网结构	4.3.4 防火墙的组合格	4.4 选择防火墙的注意事项
	4.4.1 选型防火墙的基本原则	4.4.2 选择防火墙的注意事项	复习思考题第5章 入侵检测系统
	5.1 入侵检测概述	5.1.1 入侵检测概念	5.1.2 入侵检测系统组成
	5.1.3 入侵检测功能	5.2 入侵检测系统分类	5.2.1 根据数据源分类
	5.2.2 根据检测原理分类	5.2.3 根据体系结构分类	5.2.4 根据工作方式分类
	5.2.5 根据系统其他特征分类	5.3 入侵检测技术	5.3.1 误用检测技术
	5.3.2 异常检测技术	5.3.3 高级检测技术	5.3.4 入侵诱骗技术
	5.3.5 入侵响应技术	5.4 入侵检测体系	5.4.1 入侵检测模型
	5.4.2 入侵检测体系结构	5.5 入侵检测系统与协同	5.5.1 数据采集协同
	5.5.2 数据分析协同	5.5.3 响应协同	5.6 入侵检测分析
	5.6.1 入侵检测特点分析	5.6.2 入侵检测与防火墙	5.6.3 入侵检测系统的缺陷
	5.7 入侵检测的发展	5.7.1 入侵检测标准	5.7.2 入侵检测评测
	5.7.3 入侵检测发展	复习思考题第6章 网络病毒的防治技术	6.1 计算机网络病毒的特点及危害
	6.1.1 计算机病毒的概念	6.1.2 计算机病毒的特点	6.1.3 计算机病毒的分类
	6.1.4 计算机网络病毒的概念	6.1.5 计算机网络病毒的特点	6.1.6 计算机网络病毒的分类
	6.1.7 计算机网络病毒的危害	6.2 几种典型病毒的分析	6.2.1 CIH病毒
	6.2.2 宏病毒	6.2.3 蠕虫病毒	6.2.4 木马病毒
	6.3 计算机病毒的症状	6.3.1 病毒发作前的症状	6.3.2 病毒发作时的症状
	6.3.3 病毒发作后的症状	6.4 反病毒技术	6.4.1 预防病毒技术
	6.4.2 检测病毒技术	6.4.3 杀毒技术	6.5 计算机病毒发展的新技术
	6.5.1 抗分析病毒技术	6.5.2 隐蔽性病毒技术	6.5.3 多态性病毒技术
	6.5.4 超级病毒技术	6.5.5 插入性病毒技术	6.5.6 破坏性感染病毒技术
	6.5.7 病毒自动生产技术	6.5.8 Internet病毒技术	6.6 防杀网络病毒
	6.6.1 防毒软件	6.6.2 反病毒软件	6.6.3 瑞星杀毒软件
	6.6.4 金山毒霸	6.6.5 江民杀毒软件	复习思考题第7章 网络维护
	7.1 Windows自带的网络工具	7.1.1	

## <<网络安全与维护>>

Ping命令 7.1.2 Ipconfig / Winipcfg命令 7.1.3 Netstat命令 7.1.4 Tracert命令 7.2 网  
网络连接设备的维护 7.2.1 网卡 7.2.2 集线器和交换机 7.2.3 路由器 7.2.4 网线  
7.2.5 RJ-45接头 7.3 网络性能优化 7.3.1 系统内存优化 7.3.2 CPU的优化 7  
.3.3 硬盘优化 7.3.4 网络接口优化 7.4 网络故障和排除 7.4.1 网络常见故障概述  
7.4.2 网络故障排除的思路 7.4.3 局域网故障与排除 7.4.4 Windows局域网使用过程中  
的常见故障 7.4.5 故障实例及排除方法 复习思考题主要参考文献

## <<网络安全与维护>>

### 编辑推荐

本书涵盖了网络安全和管理的基本概念、原理和技术，主要包括操作系统安全、数字加密与认证、防火墙技术、入侵检测系统、网络病毒的防治技术、网络维护等内容。

本书内容全面、取材新颖，既有网络安全和管理的理论知识，又有实用技术，反映了网络安全和管理技术的最新发展。

本书可作为大学本科及高职高专学校计算机、信息安全、网络工程、信息工程等专业信息安全课程的教材，也可供计算机爱好者、网络管理员及安全软件开发人员阅读和参考。

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>