

<<网络安全与防护基础教程>>

图书基本信息

书名：<<网络安全与防护基础教程>>

13位ISBN编号：9787301088500

10位ISBN编号：7301088507

出版时间：2005-7

出版时间：北京大学出版社

作者：雷承达

页数：283

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>

## <<网络安全与防护基础教程>>

### 内容概要

《面向21世纪全国高职高专信息技术类规划教材：网络安全与防护基础教程》紧紧围绕计算机网络安全发展前沿的热点问题，比较全面和系统地介绍了网络与信息安全的基本理论和应用实践的 latest 成果。

全书共分十章，包括绪论、密码学基础、系统攻击与防护、入侵检测系统、防火墙技术、虚拟专用网、恶意代码与计算机病毒、数据安全、网络安全和评估、网络安全的发展方向等内容。

全书材料丰富，内容翔实，覆盖面广，可读性强，可作为从事国家安全和保密工作的人员在高新技术条件下做好工作、提高业务水平必备的实用工具书，也可作为国内网络安全、计算机安全和信息安全领域相关人员的技术培训教材。

《面向21世纪全国高职高专信息技术类规划教材：网络安全与防护基础教程》还可作为通信与电子系统、信号与信息处理、密码学等专业的本科生和大专生相关课程的教学参考书。

## 书籍目录

第1章绪论1.1网络安全概述1.1.1网络安全的基本概念1.1.2网络安全的目标1.1.3网络安全的分类1.1.4安全服务1.1.5安全机制1.2网络安全威胁1.2.1存在原因1.2.2威胁类别1.2.3防护措施1.3网络安全现状及对策1.3.1网络安全现状1.3.2主要的网络安全问题1.3.3网络安全策略1.4网络安全体系1.4.1物理安全1.4.2网络安全1.4.3系统、信息和应用安全1.4.4安全管理1.5思考题第2章密码学基础2.1数据加密技术2.1.1数据加密的基本概念2.1.2加密体制的分类2.1.3对称密码体制2.1.4公钥密码体制2.1.5混合密码体制2.2数字签名技术2.2.1散列算法2.2.2数字签名的基本概念2.2.3数字签名的特点2.2.4数字签名的实现过程2.3公钥基础设施2.3.1PKI的基本组成2.3.2PKI的主要功能2.3.3认证中心2.3.4数字证书2.4密钥管理2.4.1密钥管理的基本概念2.4.2密钥管理的实现方法2.4.3密钥的生成2.4.4密钥的分配2.4.5密钥的备份与恢复2.4.6密钥的更新和销毁2.5思考题第3章系统攻击与防护3.1系统攻击概述3.1.1黑客与入侵者3.1.2系统攻击的三个阶段3.1.3网络入侵的对象3.2口令攻击3.2.1口令认证的过程3.2.2破解口令的方法3.2.3创建安全口令3.3IP欺骗3.3.1IP欺骗的原理3.3.2IP欺骗的基本形式3.3.3IP欺骗攻击的防护3.4端口扫描3.4.1端口扫描的基本概念3.4.2端口扫描技术3.4.3端口扫描的防御技术3.5网络监听3.5.1网络监听的原理3.5.2网络监听的检测技术3.5.3网络监听的防御技术3.6电子邮件攻击3.6.1电子邮件的工作原理3.6.2电子邮件面临的主要威胁3.6.3电子邮件攻击方法3.6.4电子邮件防护措施3.7思考题第4章入侵检测系统4.1入侵检测4.1.1入侵检测概述4.1.2入侵检测的主要任务和作用4.1.3入侵检测系统的基本结构4.1.4入侵检测系统的工作原理4.1.5入侵检测系统的分类4.1.6入侵检测系统的局限性4.2入侵检测系统的分析方式4.2.1异常检测技术4.2.2误用检测技术4.2.3异常检测技术和误用检测技术的4.2.4其他入侵检测技术的研究4.3入侵检测系统的结构4.3.1基于网络的入侵检测系统4.3.2基于主机的入侵检测系统4.3.3基于分布式系统的入侵检测技术4.4思考题第5章防火墙技术5.1防火墙概述5.1.1防火墙的定义和相关概念5.1.2防火墙的功能5.1.3防火墙的安全策略5.1.4防火墙的局限性5.2防火墙的种类5.2.1包过滤防火墙5.2.2应用代理过滤防火墙5.2.3状态检测防火墙5.3防火墙的体系结构5.3.1筛选路由器5.3.2双宿主主机结构5.3.3屏蔽主机结构5.3.4屏蔽子网结构5.4思考题第6章虚拟专用网6.1虚拟专用网概述6.1.1虚拟专用网的概念6.1.2虚拟专用网的功能6.1.3虚拟专用网的类型6.1.4虚拟专用网的优点6.1.5虚拟专用网的原理6.2虚拟专用网技术6.2.1隧道技术6.2.2密码技术6.2.3身份认证技术6.2.4密钥管理技术6.3隧道协议6.3.1隧道协议的基本概念6.3.2第二层隧道协议6.3.3第三层隧道协议6.4思考题第7章恶意代码与计算机病毒7.1恶意代码7.1.1恶意代码的基本概念7.1.2恶意代码的特点和分类7.1.3恶意代码的清除7.2计算机病毒7.2.1计算机病毒的概念7.2.2计算机病毒的特征7.2.3计算机病毒的分类7.2.4计算机病毒的结构7.4思考题第8章数据安全8.1数据完整性8.1.1数据完整性8.1.2提高数据完整性的办法8.2网络备份技术8.2.1网络备份的种类8.2.2备份恢复的种类8.2.3网络备份系统的组成8.2.4备份和恢复的设备与介质8.2.5提高备份性能的技术8.3归档8.3.1归档的基本概念8.3.2归档的方法8.3.3归档中的介质与冗余8.4分级存储管理8.4.1分级存储管理的功能组件8.4.2分级存储管理的工作过程8.5容错与网络冗余8.5.1容错技术的分类8.5.2容错系统实现方法8.5.3网络冗余8.6灾难恢复技术8.6.1灾难恢复前的准备8.6.2灾难恢复过程8.7思考题第9章网络安全管理和评估9.1网络安全管理9.1.1网络安全管理的概念9.1.2网络安全管理面临的风险9.1.3网络安全管理的目标9.1.4网络安全管理系统的构成9.1.5网络安全管理的措施9.2信息安全管理策略9.2.1制定信息安全管理策略的原则9.2.2信息安全管理策略的基本内容9.3信息安全管理标准9.3.1IS017799标准简介9.3.2IS017799标准控制措施9.3.3IS017799标准的应用9.4安全评估9.4.1安全评估的过程9.4.2安全评估的主要内容9.4.3安全评估的基本技术9.5安全评估准则9.5.1可信计算机系统评估准则9.5.2计算机信息系统安全保护等级划分准则9.5.3通用安全评估准则9.6思考题第10章网络安全的发展方向10.1密码技术的发展方向10.1.1密码专用芯片集成技术10.1.2椭圆曲线加密技术10.1.3量子加密技术10.1.4混沌加密技术10.1.5生物特征加密技术10.2入侵检测系统的发展方向10.2.1分布式入侵检测技术10.2.2智能化入侵检测10.2.3入侵预防技术10.2.4全面的安全防御技术10.3防火墙技术的发展方向10.3.1性能方面的发展趋势10.3.2体系结构的发展趋势10.3.3系统管理的发展趋势10.4虚拟专用网的发展趋势10.4.1IPSecVPN10.4.2MPLSVPN10.5思考题附录英文缩略词参考文献

<<网络安全与防护基础教程>>

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>