

<<网络安全基础教程与实训>>

图书基本信息

书名：<<网络安全基础教程与实训>>

13位ISBN编号：9787301168776

10位ISBN编号：7301168772

出版时间：2010-2

出版时间：尹少平 北京大学出版社 (2010-02出版)

作者：尹少平 编

页数：288

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>

<<网络安全基础教程与实训>>

前言

第2版在第1版基础上做了较大修整，扩充了应用案例和实训项目，删除了较为陈旧的示例，增加了网络安全新技术内容，内容更加全面和系统，表述更为规范和准确，基本能够涵盖高职高专学生对于网络安全技术应当掌握和了解的知识和方法。

针对第1版的改动如下。

第1章对网络安全内涵的阐述前后重复的部分做了删减；第2章标题做了修改，原内容做了精简，增加了应用案例；第3章为本书的重点，内容做了较大扩充，增加了成熟的密码学应用案例PGP和SET的讲述，并增加了PGP的实训项目，另外还修改了DSA算法描述中的错误；第4章修改了标题，增加了最新操作系统Windows Server 2008和常用操作系统Linux的安全性阐述；第5章删减了原书中的病毒示例，增加了比较新的梅勒斯病毒分析，增加了2009年最新杀毒病毒软件的新技术应用案例，修改和补充了实训项目；第9章删减了较陈旧的内容，如木马示例，增加了Web安全一节；增加了第11章综合实训；第6章、第7章、第8章和第10章内容做了适当的改动，在此不一一赘述。

学完本书，学生将具备网络协议分析、操作系统安全配置、密码技术应用、防病毒软件的应用、防火墙的安装与使用、入侵检测系统和VPN系统的配置等方面的能力，能胜任初中级的网络安全管理和安全系统集成的工作。

<<网络安全基础教程与实训>>

内容概要

《网络安全基础教程与实训(第2版)》是《网络安全基础教程与实训》的第2版,各章都进行了修整,扩充了应用案例和实训项目,删除了较为陈旧的示例,增加了网络安全新技术内容,更加全面和系统,基本能够涵盖高职高专学生对于网络安全技术应当掌握和了解的知识和方法。

《网络安全基础教程与实训(第2版)》共分11章,主要包括:网络安全概论、网络监听与TCP/IP协议分析、密码技术、操作系统安全、病毒分析与防御、Internet应用服务安全、防火墙、入侵检测系统、网络攻击与防范、VPN技术、和综合实训。

《网络安全基础教程与实训(第2版)》注重实践技能的培养,以实训为依托,深入浅出地讲解理论知识,因此既可作为高职高专院校计算机及相关专业的学生教材,也可作为计算机网络安全类的技术参考书或培训教材。

书籍目录

第1章 网络安全概论1.1 网络安全简介1.2 网络安全所产生的威胁1.2.1 网络中存在的威胁1.2.2 主机网络安全1.2.3 主机网络安全系统体系结构1.3 协议安全分析1.4 网络安全标准1.4.1 网络安全主要国际标准1.4.2 IS07498.2 安全标准1.4.3 BS7799(ISO17799 : 2000)标准1.5 网络安全组件1.6 安全策略的制定与实施1.7 本章小结1.8 本章习题第2章 网络监听与TCP / IP协议分析2.1 网络监听与数据分析2.1.1 网络监听的基本原理2.1.2 网络监听工具2.2 网络层协议报头结构2.2.1 IP数据报结构2.2.2 ARP2.2.3 ICMP2.2.4 IGMP2.3 传输层协议报头结构2.3.1 TCP2.3.2 LJP2.4 TCP会话安全2.5 TCP / IP报文捕获与分析2.6 本章小结2.7 本章实训2.8 本章习题第3章 密码技术3.1 对称密码体制3.1.1 对称加密体制的概念3.1.2 DES算法3.1.3 DES算法实现3.2 公钥密码体制3.2.1 公钥密码体制的概念3.2.2 RSA算法3.2.3 RSA算法实现3.3 数字签名技术3.3.1 数字签名技术的概念3.3.2 数字签名的实现方法3.3.3 数字签名的其他问题3.4 密钥管理3.4.1 私钥分配3.4.2 公钥分配3.4.3 用公钥加密分配私钥密码体制的密钥3.5 认证3.5.1 身份认证3.5.2 主机之间的认证3.5.3 Kerberos认证3.5.4 基于PKI的身份认证3.6 本章小结3.7 本章实训3.8 本章习题第4章 操作系统安全4.1 操作系统安全基础4.1.1 操作系统安全管理目标4.1.2 操作系统安全管理措施4.2 WindowsServer2003账户安全4.2.1 账户种类4.2.2 账户与密码约定4.2.3 账户和密码安全设置4.3 WindowsServer2003文件系统安全4.3.1 NTFS权限及使用原则4.3.2 NTFS权限的继承性4.3.3 共享文件夹权限管理4.3.4 文件的加密与解密4.4 WindowsServer2003主机安全4.5 WindowsServer2008安全创新特.凹4.5.1 安全配置向导4.5.2 网络访问保护4.5.3 高级安全Windows防火墙4.6 Linux操作系统安全基础4.6.1 Linux自身的安全机制4.6.2 Linux用户账户与密码安全4.6.3 Linux的文件访问控制4.7 本章小结4.8 本章实训4.9 本章习题第5章 病毒分析与防御5.1 计算机病毒概述5.1.1 计算机病毒的定义5.1.2 设计病毒的动机5.1.3 计算机病毒的特性5.1.4 计算机病毒的分类5.1.5 计算机病毒感染的表现5.2 病毒机制与组成结构5.2.1 计算机病毒的组成结构5.2.2 计算机病毒的传染5.2.3 计算机病毒的触发机制5.2.4 计算机病毒的生存周期5.3 病毒实例剖析5.3.1 Nimda蠕虫病毒剖析5.3.2 CIH病毒剖析5.3.3 梅勒斯病毒剖析5.4 病毒的防范与清除5.4.1 防范病毒5.4.2 检测病毒5.4.3 清除病毒5.5 病毒和反病毒的发展趋势5.5.1 病毒的发展趋势5.5.2 病毒清除技术的发展趋势5.5.3 防病毒系统的要求5.6 本章小结5.7 本章实训5.8 本章习题第6章 Internet应用服务安全6.1 Internet应用服务概述6.1.1 客户机朋艮务器模型6.1.2 应用服务的划分6.1.3 Internet的安全6.2 Web服务的安全6.2.1 IIS-Web安全设置6.2.2 浏览器的安全性6.3 FTP服务的安全6.4 电子邮件服务的安全6.4.1 E-mail工作原理及安全漏洞6.4.2 安全风险6.4.3 安全措施6.4.4 IIS-SMTP服务安全6.5 SQLServer2000安全6.5.1 身份认证模式6.5.2 安全配置6.6 本章小结6.7 本章实训6.8 本章习题第7章 防火墙7.1 防火墙概述7.1.1 防火墙的发展7.1.2 防火墙的功能7.2 防火墙技术7.2.1 防火墙的包过滤技术7.2.2 防火墙的应用代理技术7.2.3 防火墙的状态检测技术7.2.4 防火墙系统体系结构7.2.5 防火墙的主要技术指标7.3 防火墙的缺陷7.4 防火墙产品介绍7.4.1 Cisco防火墙简介7.4.2 紫荆盾NetST防火墙简介7.5 本章小结7.6 本章实训7.7 本章习题第8章 入侵检测系统8.1 入侵检测系统概述8.1.1 入侵检测定义8.1.2 入侵检测系统的主要功能8.2 入侵检测系统的组成8.3 入侵检测系统的分类8.3.1 按数据来源和系统结构分类8.3.2 按工作原理分类8.3.3 按时效性分类8.3.4 按模块运行分布方式分类8.4 入侵检测系统的工作原理8.4.1 入侵检测系统的检测流程8.4.2 基于异常的入侵检测方法8.4.3 基于误用的入侵检测方法8.5 入侵检测系统的抗攻击技术8.6 入侵检测技术的发展方向8.7 入侵检测工具与产品介绍8.8 本章小结8.9 本章实训8.10 本章习题第9章 网络攻击与防范9.1 网络攻防概述9.1.1 网络攻击的一般目标9.1.2 网络攻击的步骤及过程分析9.1.3 网络攻击的防范对略9.2 端口扫描9.2.1 端口扫描的原理9.2.2 端口扫描的防范对策9.3 网络嗅探原理9.3.1 嗅探器的概念9.3.2 嗅探器攻击的检测9.3.3 嗅探器的危害9.3.4 网络嗅探的防范对策9.4 密码攻防9.4.1 密码攻击常用手段9.4.2 密码攻防对策9.5 特洛伊木马攻防9.5.1 特洛伊木马攻击原理9.5.2 特洛伊木马程序的防范对策9.6 缓冲区溢出攻防9.6.1 缓冲区溢出的原理9.6.2 缓冲区溢出攻击的防范对策9.7 拒绝服务攻击与防范9.7.1 拒绝服务攻防概述9.7.2 拒绝服务模式分类9.7.3 分布式拒绝服务攻击9.8 Web攻击与防范9.9 本章小结9.10 本章实训9.11 本章习题第10章 VPN技术10.1 VPN的基本概念10.2 VPN的系统特性10.3 VPN的原理与协议10.3.1 实现VPN的隧道技术10.3.2 PPTP协议10.3.3 L2F协议10.3.4 L2TP协议10.3.5 IPsec协议10.3.6 SSLVPN10.3.7 Windows2000的VPN技术10.4 构建VPN的解决方案与相关设备10.5 本章小结10.6 本章实训10.7 本章习题第11章 综合实训参考文献

章节摘录

插图：(1) 应用层：是网络访问的网络特性和操作系统特性的最佳结合点。

通过对主机所提供服务的协议的分析，可以知道网络访问的行为，并根据用户设置的策略判断在当前环境下是否允许该行为；另外，还要附加更严格的身份论证。

(2) 传输层：是实现加密传输的首选层。

对于使用了相同安全系统的主机之间的通信，可以实现透明的加密传输，而对于没有加密措施的通用客户软件之间的通信，仍可以使用不加密方式，并且加密与否对于用户来说是透明的。

(3) 网络层：是实现访问控制的首选层。

通过对IP地址、协议、端口号的识别，能方便地实现包过滤功能。

当然，更复杂的设计可以在更多的层实现更多的安全功能，下面就前面的设想提出一个可行的主机网络安全系统的结构模型，如图1.1所示。

在图1.1所示的结构模型中，安全检查承担了防火墙的任务，它对进出的数据包按照系统设置的安全规则进行过滤，另外，在该模块中还可以实现加密/解密。

对用户的访问进行细粒度控制是主机网络安全系统最为重要的特点，它包括两个方面：内部资源访问控制和外部资源访问控制。

<<网络安全基础教程与实训>>

编辑推荐

《网络安全基础教程与实训(第2版)》：扩充了应用案例和实训项目增加了网络安全新技术内容

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>