第一图书网, tushu007.com

<<防火墙与VPN>>

图书基本信息

书名：<<防火墙与VPN>>

13位ISBN编号：9787302186519

10位ISBN编号：7302186510

出版时间：2008-12

出版时间：迪波斯 (Richard Tibbs)、奥克斯 (Edward Oakes)、李展、 刑博特 清华大学出版社 (2008-12出版)

作者：（美）迪波斯，（美）奥克斯 著

页数：350

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

本书采用教科书形式、以理论基础与实际应用结合的方法，全面介绍了与网络安全相关的各种内容，覆盖了防御对策、攻击形式以及与计算机安全相关的策略，填补了其他一些安全图书某些内容缺失的空白。
本书以平易近人的语言详细阐述了防火墙、入侵检测系统、加密基础、操作系统加固、抵御病毒／木马／间谍软件攻击以及安全策略和安全标准的实际应用。
为了巩固学习的知识，在本书每一章的末尾，都给出了多项选择题、练习题、项目题和一个案例研究，为学生提供了动手实践和深入理解本章内容的机会。
本书适合于作为学习网络安全的教材，也是网络管理员、安全专业人员以及安全审计专业人员日常工作的手边手册。
参加本书翻译工作的人员包括：张长富、蔡建章、李匀、张建安、邓铁洪、徐君、杨莹、李强、李勇、蒋恩骏、杨文保、苏辛、周成兴、魏敬安、朱建波、徐志平、赵杰辉、傅祎、郭碧莲、郭洵、洪晓煜、黄宣达、江松波、柯渝、赖曲芳、廖阳、刘文红、贺军等，张福林先生对本书中的一些关键段落和疑难之处作出了详细的解释和指导，在此深表感谢。
限于译者水平，错误和遗漏之处，敬请读者批评指导。

第一图书网, tushu007.com

内容概要

本书以一个对基本网络与计算机安全概念的复习单元开始，着重介绍网络和数据链路层以及TCP和UDP传输协议，防火墙安装和配置实践，特定的防火墙技术、工具和技巧，虚拟专用网技术，日常防火墙的维护等。

书中的实例、练习以及工程题均使用了低成本，易获得的硬件来创建小型网络，帮助读者理解和学习防火墙和虚拟专用网。

本书适用于高等院校计算机及相关专业的本科生和教师，从事信息安全方面工作的人员。

作者简介

作者：(美国)迪波斯 (Richard Tibbs) (美国)奥克斯 (Edward Oakes) 译者：李展 刑博特Richard W.Tibbs博士获得了美国乔治梅森大学系统与信息技术工程学院的哲学博士学位.专门从事运营管理研究。
他还在科罗拉多大学波尔得分校获得了计算机科学硕士学位以及应用数学学士学位。
他主要研究网络安全、网络和计算机、网络和计算机容量规划、队列理论和仿真、流量监控和分析以及远程通信网络中的自适应路由。
他是ACM、IEEE和INFORMS的成员。
Tibbs博士曾在工业部门、政府机关和学术研究单位工作20多年，后来在瑞德福大学任全职教师。
他的行业背景包括宇航、电信和软件开发。
他在政府机关工作的单位是美国地质调查局和MITRE公司.他还在美国联邦基金研究和开发中心的运输工程部工作过。
Edwarld B.OakesEdward B.Oakes在瑞德福大学获得了计算机科学学士学位，现正在理工大学攻读硕士学位。
2004年，他由于教学开发的贡献获得了安娜李斯图尔特奖。
他现在是瑞德福大学理论计算方面的学术带头人.在网络和安全方面有超过14年的实践经验。
除了其他角色之外.他还担任瑞德福大学信息安全主管有5年的时间。
他喜欢的领域包括网络安全、无线计算，以及在教室中理论联系实际的授课。

书籍目录

第1部分 网络概念与TCP／IP族第1章 网络与数据链路层协议概述1.1 概述1.2 安全的简明定义1.2.1 协议1.2.2 安全体系结构与策略1.2.3 应用1.2.4 加密技术1.2.5 相关的技术1.2.6 检测、分析与事故响应1.3 TCP／IP协议族1.4 数据链路层帧接收模式与寻址1.4.1 以太网媒体访问控制（MAC）1.4.2 单播地址与广播地址1.4.3 多播地址1.4.4 混杂模式——在什么时机是适当的1.5 Internet协议（IP）概述1.5.1 IP首部内容1.5.2 过滤参数1.5.3 典型的过滤应用程序1.6 本章小结1.7 技能测试1.7.1 多项选择题1.7.2 练习题1.7.3 项目题1.7.4 案例研究第2章 传输控制协议与用户数据报协议详解2.1 概述2.2 TCP状态机2.2.1 TCP会话2.2.2 TCP标志及首部内容2.2.3 TCP端口2.2.4 三次握手（建立连接）2.2.5 已连接模式2.2.6 连接拆除2.2.7 半开放TCP扫描2.2.8 重要的TCP应用程序2.3 用户数据报协议2.3.1 UDP首部内容2.3.2 UDP端口2.3.3 重要的UDP应用程序2.4 Internet控制消息协议2.4.1 ICMPPing2.4.2 ICMPTraceRoute2.5 本章小结2.6 技能测试2.6.1 多项选择题2.6.2 练习题2.6.3 项目题2.6.4 案例研究第2部分 防火墙基础第3章 软件防火墙、小型办公室防火墙和企业防火墙3.1 概述3.2 硬件和软件防火墙3.2.1 防火墙作为路由器3.2.2 独立代理或者应用程序防火墙3.2.3 企业防火墙3.2.4 SOHO防火墙3.3 个人防火墙：基于主机的软件防火墙3.3.1 WindowsXPFirewall3.3.2 ZoneAlarm3.3.3 BlackICF3.3.4 Mac OS X防火墙3.4 内部防火墙：ACL及iptables3.5 防火墙测试3.5.1 在线扫描器3.5.2 开源扫描器3.6 本章小结3.7 技能测试3.7.1 多项选择题3.7.2 练习题3.7.3 项目题3.7.4 案例研究第4章 威胁、数据包过滤和状态防火墙4.1 概述4.2 安全威胁的种类4.2.1 IP地址欺骗4.2.2 IP路由表4.2.3 关于单播RPF和DNS反向查找的更多信息4.2.4 拒绝服务攻击4.2.5 TCP缺陷：SYN泛洪攻击及连接劫持4.2.6 中间人攻击4.2.7 重放攻击4.3 主要的防火墙类型：非状态、状态、代理和内容识别防火墙4.3.1 非状态与状态防火墙4.3.2 深入状态防火墙4.3.3 代理或应用防火墙4.3.4 内容识别数据包过滤防火墙4.4 关于使用Nessus的更多信息4.4.1 启动Nesstus4.5 本章小结4.6 技能测试4.6.1 多项选择题4.6.2 练习题4.6.3 项目题4.6.4 案例研究第5章 初步防火墙安装练习5.1 概述5.2 实验室概述5.2.1 防火墙PC的要求5.2.2 内部网络中服务的实现问题5.3 在防火墙计算机上安装LEAF5.3.1 初始安装5.3.2 定位NIC模块5.3.3 安装不同的NIC模块5.3.4 安装升级5.4 在外部计算机上安装Linux5.4.1 外部计算机的服务和工具5.5 黑帽／白帽方案：使用工具评估防火墙的能力5.6 防火墙连接至Internet或校园网5.6.1 配置环境5.7 本章小结5.8 技能测试5.8.1 多项选择题5.8.2 练习题5.8.3 项目题5.8.4 案例研究第6章 确定防火墙需求6.1 概述6.2 防火墙策略6.2.1 管理支持6.2.2 深入说明防火墙策略6.2.3 用户教育6.3 网络设计6.4 防火墙规则语法6.4.1 Shorewall规则6.4.2 Cisco访问列表项6.4.3 数据流的流动（输入和输出）6.5 为外部世界提供的服务6.5.1 域名服务6.5.2 简单邮件传输协议第7章 防火墙高级概念和术语第3部分 VPN和日志

章节摘录

插图：

编辑推荐

《防火墙与VPN原理与实践》适用于高等院校计算机及相关专业的本科生和教师，从事信息安全方面工作的人员。

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