

<<网络安全完全手册>>

图书基本信息

书名：<<网络安全完全手册>>

13位ISBN编号：9787121017674

10位ISBN编号：7121017679

出版时间：2005-1

出版时间：电子工业出版社

作者：[美] Roberta Bragg ,

页数：614

字数：1005000

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>

## <<网络安全完全手册>>

### 内容概要

本书由美国计算机网络安全专家集体编写，为读者描绘了有关网络安全领域的总体框架。全书共分6个部分30章，详细介绍了30种不同的网络安全领域的解决方案，主要包括授权与认证控制、网络设备安全、防火墙、VPN、无线网络、入侵检测、Linux/UNIX安全、Windows安全、Novell安全、J2EE安全、.NET安全、数据库安全、灾难恢复及事件响应、法律问题等。本书在内容上注重全面性，几乎涉及了与网络安全相关的所有主题，是一本完整的网络安全参考手册。

本书适合从事网络安全工作的技术人员及开发人员使用，也适合作为计算机应用专业高年级本科生和研究生的教材。

<<网络安全完全手册>>

作者简介

布拉格，是Microsoft Certified Professional杂志的安全顾问兼专栏作家，她也是SearchWin2000.com的安全专家。

Roberta发起并参与了2002年的首届Windows安全峰会。

## &lt;&lt;网络安全完全手册&gt;&gt;

## 书籍目录

第一部分 网络安全基础 第1章 网络安全概述 1.1 好的安全实践方案的益处 1.2 安全方法学 1.3 小结 1.4 参考文献 第2章 风险分析与防御模型 2.1 威胁定义和风险分析 2.2 防御模型 2.3 小结 2.4 参考文献 第3章 安全策略开发 3.1 安全策略的开发 3.2 安全策略主题举例 3.3 安全策略的实施 3.4 小结 3.5 参考文献 第4章 安全机构 4.1 角色和责任 4.2 职责的分离 4.3 安全运作管理 4.4 安全生命期管理 4.5 安全感知 4.6 强制实施 4.7 信息的分类 4.8 文档化 4.9 安全审计 4.10 受管理的安全服务 4.11 小结 4.12 参考文献 第二部分 访问控制 第5章 物理安全 5.1 资产的分类 5.2 物理脆弱性评估 5.3 选择安全的站点位置 5.4 对资产进行保护:锁和入口控制 5.5 物理入侵检测 5.6 小结 5.7 参考文献 第6章 认证与授权控制 6.1 认证 6.2 授权 6.3 小结 第7章 数据安全架构 7.1 数据安全架构的原理 7.2 数据安全架构的应用程序 7.3 小结 第8章 安全管理架构 8.1 可操作的强制实施 8.2 管理安全 8.3 可记账性控制 8.4 活动监控和审计 8.5 小结 第三部分 网络体系结构 第9章 网络设计要素 9.1 网络安全设计简介 9.2 性能 9.3 可用性 9.4 安全 9.5 小结 9.6 参考文献 第10章 网络设备安全 10.1 交换机和路由器基础 10.2 网络硬化 10.3 小结 第11章 防火墙 11.1 防火墙概述 11.2 防火墙的其他功能 11.3 小结 11.4 参考文献 第12章 虚拟专用网络安全 12.1 VPN的工作原理 12.2 VPN协议 12.3 客户机/服务器远程访问的脆弱性和威胁 12.4 站点 对站点网络的脆弱性和威胁 12.5 小结 第13章 无线网络安全 13.1 无线频率安全基础 13.2 数据链路 层无线安全特性、缺陷和威胁 13.3 无线网络硬化实践和建议 13.4 小结 第14章 入侵检测系统 14.1 IDS概念 14.2 IDS类型和检测模型 14.3 IDS特点 14.4 IDS开发考虑 14.5 小结 第15章 完整性 与可用性结构 15.1 版本控制和变更控制 15.2 安装补丁 15.3 备份 15.4 系统和网络冗余 15.5 小 结 第16章 基于网络角色的安全 16.1 E?mail 16.2 代理服务器 16.3 DNS服务器 16.4 源代码库访 问 16.5 Web服务器 16.6 IP电话和流媒体 16.7 信用卡安全 16.8 打印机和传真机 16.9 特殊系统 16.10 SCADA 16.11 PBX 16.12 小结 第四部分 操作系统安全 第17章 操作系统安全模型 17.1 操 作系统模块 17.2 传统安全模型 17.3 可信计算技术 17.4 小结 17.5 参考文献 第18章 常见UNIX 脆弱点 18.1 从新安装的系统开始 18.2 删除不需要的守护程序 18.3 安装OpenSSL 18.4 使 用OpenSSH替换脆弱的守护程序 18.5 不为守护程序使用根 18.6 使用chroot隔离过程 18.7 使 用TCP Wrapper 18.8 审计应用程序 18.9 审计计时程序工作 18.10 扫描SUID和SGID文件 18.11 了 解哪个端口打开 18.12 运行CIS扫描 18.13 保持补丁更新 18.14 使用集中化日志服务器 18.15 考 虑替换sendmail 18.16 预定安全列表 18.17 小结 第19章 Linux安全 19.1 从新安装的系统开始 19.2 安装文件扫描应用程序 19.3 确定服务器的角色 19.4 查看常见扫描端口 19.5 IP约束 19.6 查看日 志文件 19.7 监控脆弱点 19.8 小结 第20章 Windows安全 20.1 在Windows中应用6项安全基础 20.2 Windows系统的威胁分析 20.3 缓解安全威胁 20.4 安全检查表 20.5 小结 第21章 Novell安全 21.1 NetWare综述 21.2 Novell目录服务 21.3 NDS安全 21.4 保证NetWare安全的技巧和最佳实践 21.5 小结 21.6 参考文献 第五部分 应用系统安全 第22章 应用系统安全原则 22.1 Web应用系统安全 22.2 常规应用系统安全 22.3 嵌入式应用系统安全 22.4 远程管理安全 22.5 小结 第23章 编写安 全软件 23.1 金牌原则——不要轻易相信任何人 23.2 金牌安全原则 23.3 小结 第24章 J2EE安全 24.1 Java和J2EE 24.2 J2EE体系结构 24.3 认证和授权 24.4 协议 24.5 小结 第25章 Windows.NET 安全 25.1 .NET的核心安全特性 25.2 .NET中的应用级安全 25.3 小结 第26章 数据库安全 26.1 一 般数据库安全概念 26.2 理解数据库服务器的安全层次 26.3 理解数据库层安全 26.4 使用应用层安 全 26.5 数据库备份和恢复 26.6 及时升级服务器 26.7 数据库审计与监控 26.8 小结 第六部分 响 应 第27章 灾难恢复与业务持续 27.1 灾难恢复 27.2 业务持续 27.3 小结 第28章 攻击与对策 28.1 攻击 28.2 防范对策 28.3 小结 28.4 参考文献 第29章 事件响应与取证分析 29.1 事件响应计划 29.2 取证分析 29.3 小结 29.4 参考文献 第30章 有关信息安全的法律 30.1 网络规则:定义计算机犯 罪 30.2 信息安全规定:保护的责任 30.3 指导事件响应检查所依从的法律 30.4 小结 安全词汇

<<网络安全完全手册>>

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>