

<<无线网络安全防护>>

图书基本信息

书名：<<无线网络安全防护>>

13位ISBN编号：9787111111108

10位ISBN编号：7111111109

出版时间：2003-1

出版时间：机械工业出版社

作者：（美）Christian Barnes 等著，林生，龚克 等译

页数：278

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>

<<无线网络安全防护>>

内容概要

本书介绍无线网络所面临的挑战及无线网络的广播特性，涉及监听、截取和窃听技术，以及黑客攻击的工具和设备，入侵检测策略。

书中还介绍了如何建立信息分级过程，如何设计和部署安全网络，如何设计和规划成功的审计，如何开发无线网络安全检查表。

本书适合网络安全技术人员参考。

<<无线网络安全防护>>

书籍目录

第1章 无线通信网络的挑战 1.1 概述 1.2 无线通信网络技术概述 1.3 了解无线通信网络的发展前景
1.4 了解无线通信网络的优点 1.5 面对现在无线通信网络的实际情况 1.6 分析无线通信网络的标准 1.7
总结 1.8 解决方案简要概括 1.9 常见问题解答第2章 安全入门 2.1 概述 2.2 理解安全基础知识和安全
保护原理 2.3 评价安全策略的作用 2.4 认识一些普遍接受的安全与保密标准 2.5 解决普通风险和威胁
2.6 总结 2.7 解决方案简要概括 2.8 常见问题解答第3章 无线网络构架与设计 3.1 概述 3.2 固定无线技术
3.3 依照802.11框架来开发WLAN 3.4 遵循802.15构架来开发WPAN 3.5 移动无线技术 3.6 光学无线
技术 3.7 探索设计过程 3.8 创建设计方法 3.9 从设计角度理解无线网络的属性 3.10 总结 3.11 解决方
案简要概括 3.12 常见问题解答第4章 常见攻击和弱点 4.1 概述 4.2 WEP中存在的弱点 4.4 窃听、截取
和监听 4.5 欺骗与非授权访问 4.6 网络接管与篡改 4.7 拒绝服务和泛洪攻击 4.8 恶意软件介绍 4.9 偷
窃用户设备 4.10 总结 4.11 解决方案简要概括 4.12 常见问题解答第5章 无线安全对策 5.1 概述 5.2 再
次访问策略 5.3 分析威胁 5.4 设计和部署安全网络 5.5 实现WEP 5.6 过滤MAC 5.7 过滤协议 5.8 使用
封闭系统和网络 5.9 分配IP 5.10 使用VPN 5.11 保护用户 5.12 总结 5.13 解决方案简要概括 5.14 常
见问题解答第6章 绕过安全措施 6.1 概述 6.2 计划和准备 6.3 利用WEP 6.4 “战争驾驶” 6.5 盗窃用户
设备 6.6 MAC过滤 6.7 绕过高级安全机制 6.8 利用内部人员 6.9 安装欺诈基站 6.10 利用VPN 6.11 总
结 6.12 解决方案简要概括 6.13 常见问题解答第7章 监控和入侵检测 7.1 概述 7.2 设计探测方案 7.3
防御性监控事项 7.4 入侵检测策略 7.5 进行弱点评估 7.6 事故响应和处理 7.7 进行站点调查, 查找欺
诈基站 7.8 总结 7.9 解决方案简要概括 7.10 常见问题解答第8章 审计 8.1 概述 8.2 设计和计划成功的
审计 8.3 定认标准 8.4 进行审计 8.5 分析审计数据 8.6 生成审计报告 8.7 总结 8.8 解决方案简要概括
8.9 常见问题解答第9章 案例说明 9.1 概述 9.2 实现不安全的无线网络 9.3 实现极度安全的无线LAN
9.4 进行“战争驾驶” 9.5 检查周围的环境 9.6 建立无线安全检查列表 9.7 总结 9.8 解决方案简要概括
9.9 常见问题解答

<<无线网络安全防护>>

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>