第一图书网, tushu007.com

<<信息安全工程技术>>

图书基本信息

书名：<<信息安全工程技术>>

13位ISBN编号：9787563526666

10位ISBN编号：7563526668

出版时间：2011-7

出版时间：北京邮电大学出版社

作者：郭乐深

页数：294

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

内容概要

郭乐深、尚晋刚、史乃彪主编的《信息安全工程技术》以具体的信息安全问题具体分析和解决为目的，结合当前流行的信息安全工程常用的软件，由局部到整体的思路全面介绍信息安全工程领域的实用技术。
全书分为两个部分，第1部分首先介绍信息安全形势、Windows系统信息安全技能、网络扫描技术、漏洞扫描技术、局域网侦听技术、自定义数据包生成攻击技术；接下来介绍最新的Metasploit安全测试工具、网络抓包工具等；最后介绍入侵检测和
Snort技术、防火墙和IPTABLES技术、VPN和OpenVPN技术、加解密工具和 OpenSSL技术等。
第2
部分举出一个接近实际的信息安全工程案例，从安全技术基础设施项目的目标、目标的信息安全所存在问题、目标的信息安全需求分析、目标的安全功能要素分析和方案、目标的安全服务体系、目标的安全教育培训服务、目标的项目管理、目标的质量保证体系等完整过程来阐述一个完整的信息安全工程，来帮助读者从全方位建立对信息安全工程技术整体架构的认识。

《信息安全工程技术》既适合作为信息安全及其相关专业本科生及研究生的专业教材，同时由于包含了极其丰富的信息安全实用技术，也适合于企、事业单位的网络管理人员、安全维护人员、系统管理人员和其他相关技术人员阅读参考。

书籍目录

第1部分
第1章 绪论
1.1 了解信息安全形势
1.2 认识信息安全环境
1.3 养成良好的行为习惯
本章小结
思考题
第2章 Windows系统信息安全技能
2.1 网络安全
2.2 操作系统安全
2.3 病毒防护
2.4 应用软件和互联网安全
2.5 数据安全
本章小结
思考题
第3章 网络扫描
3.1 网络扫描的工作方式
3.2 主机发现
3.3 Nmap端口扫描参数
3.4 端口扫描
3.5 服务和版本探测
3.6 时间和性能
3.7 操作系统检测
3.8 Nmap输出
3.9 防火墙／IDS躲避
本章小结
思考题
第4章 漏洞扫描
4.1 Nessus
4.2 Nikto
本章小结
思考题
第5章 局域网侦听
5.1 局域网寻址
5.2 交换环境中使用ettercap和arpspoof
5.3 静态ARP绑定
5.4 获取局域网信息
5.5 操作数据包数据
本章小结
思考题
第6章 自定义数据包生成
6.1 创建自定义数据包的意义
6.2 hping数据包构建工具
6.3 Scapy工具
6.4 使用Scapy构建数据包

本章小结
思考题
第7章 Metasploit安全测试工具
7.1 Metasploit界面
7.2 选择漏洞
7.3 选择有效载荷（Payload）
7.4 设定选项
7.5 隐藏选项
本章小结
思考题
第8章 网络抓包
8.1 tcpdump抓包工具
8.2 Ethereal／Wireshark工具
本章小结
思考题
第9章 入侵检测技术和Snort
9.1 入侵检测（Intrusion Detection）的概念
9.2 入侵检测系统的分类
9.3 入侵检测系统模型
9.4 入侵检测的技术途径
9.5 入侵检测系统的挑战及发展趋势
9.6 Snort简介
9.7 Snort规则
9.8 Snort与tcpdump的比较
9.9 Snort的体系结构
9.10 安装使用Snort
9.11 入侵检测系统的发展趋势
本章小结
思考题
第10章 防火墙和LPTABLES
10.1 技术现状
10.2 防火墙的定义和描述
10.3 防火墙的任务
10.4 防火墙术语
10.5 包过滤
10.6 代理服务器
10.7 Web代理
10.8 电路级网关
10.9 应用级网关
10.10 防火墙的一些高级特性
10.11 使用IPTABLES构建Linux下的防火墙
本章小结
思考题
第11章 虚拟专用网（VPN）和OpenVPN
11.1 VPN简介
11.2 VPN的特点
11.3 VPN安全技术

11.4 VPN的种类及其实现方式
11.5 目前VPN的实现举例
11.6 OpenVPN
本章小结
思考题
第12章 加解密工具和OpenSSL
12.1 OpenSSL背景
12.2 OpenSSL结构
12.3 OpenSSL功能
12.4 OpenSSL应用
本章小结
思考题
第2部分
第13章 信息安全工程案例
13.1 ××IT安全技术基础设施项目的目标
13.2 项目范围
13.3 安全宗旨
13.4 信息安全“三元论”
13.5 安全标准和规范
思考题
第14章 信息安全所存在的问题
14.1 信息安全表述模型——P2DR模型
14.2 信息安全实现原则和方法学
14.3 安全完整解决方案结构
14.4 多角度的安全需求分析和设计
思考题
第15章 信息安全需求分析
15.1 ××部门网络安全策略和管理体系需求分析
15.2 ××部门网络业务安全需求分析
15.3 分布式安全需求分析和设计
15.4 层次性安全需求分析和设计
15.5 ××部门网络安全集成需求分析
思考题
第16章 安全功能要素详细分析和方案
16.1 网络拓扑结构
16.2 边界安全问题
16.3 主机安全
16.4 安全风险评估
16.5 入侵监控和防御
16.6 访问控制
16.7 日志和审计
16.8 身份认证
16.9 信息加密
16.10 灾难恢复
16.11 安全管理工具
16.12 安全测评
思考题

第17章 安全服务体系
17.1 专业安全服务体系
17.2 安全方案服务体系
17.3 企业信息安全策略顾问服务
17.4 安全评估顾问服务
17.5 安全管理维护方案
17.6 安全紧急响应服务
17.7 安全测评服务
17.8 教育培训服务
思考题
第18章 安全集成方案
18.1 方案一：强健型方案
18.2 方案二：经济型方案
18.3 安全建设规划和规划型方案
18.4 安全系统自身安全说明
18.5 集成性说明
思考题
第19章 项目管理
19.1 项目运作方式
19.2 项目实施组人员组织结构
19.3 项目实施管理
思考题
第20章 质量保证体系
20.1 项目执行人员的质量职责
20.2 项目质量控制措施
本章小结
思考题
附录　学习参考资料
参考文献

编辑推荐

信息安全工程技术是一门涉及计算机科学、网络技术、通信技术等多种学科的综合性科学。
从总体上，网络安全可以分成网络攻击技术和网络防御技术两大方面，只有全面把握两方面的内容，才能真正掌握计算机网络安全技术。
郭乐深、尚晋刚、史乃彪主编的《信息安全工程技术》可以帮助读者了解信息安全工程技术的整体框架，并熟悉如何建立一套比较完善的信息安全工程。
它着重阐述了应用信息安全技术所需要注意的问题，还涉及了信息安全的不同领域，探讨了很多不同方向的信息安全策略，并在第2部分以8章的篇幅提供了一套接近实际的信息安全工程案例供读者参考。
　编写本书的目的是为那些需要信息安全技术的人提供一些参考资料，使他们能真正了解并掌握信息安全工程技术。
对于初识信息安全的非技术人员来说，本书可以作为认识、了解信息安全的大纲，供他们快速了解信息安全的基础知识并认识到信息安全的必要性。
对于了解信息安全的技术人员来说，本书可以帮助他们更加深入地领略信息安全的精髓。

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