

<<网络安全>>

图书基本信息

书名：<<网络安全>>

13位ISBN编号：9787115113504

10位ISBN编号：7115113505

出版时间：2003-7-1

出版时间：人民邮电出版社

作者：吕慧勤,熊华,郭世泽

页数：238

字数：373

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>>

### 内容概要

本书主要介绍4种网络安全新技术，即入侵检测技术、蜜罐技术、取证技术和物理隔离技术，重点介绍了与之相关的概念、基本思想、产品使用方法和发展趋势等内容，力求使读者在短的时间内对这些网络安全新技术有比较清晰的认识，为读者进一步使用和研究它们起到引路和铺垫作用。全书共分为5章，介绍了加密认证、防火墙和VPN、入侵检测技术、蜜罐技术、取证技术和物理隔离技术。

本书内容丰富、层次分明，可以作为从事网络安全工作的工程技术人员的实用工具书；也可作为通信与电子系统、信号和信息处理、密码学和网络安全等专业的大学本科生和研究生相关课程的教学参考书；还可作为国内网络安全、信息安全和计算机安全领域相关人员培训班的教材。

## 书籍目录

第1章 安全技术基础 11.1 密码学的基本概念 11.1.1 基本概念 21.1.2 古典密码拾零 41.1.3 密码攻击概述 71.1.4 网络加密方式 81.2 著名密码算法 91.2.1 分组密码算法 91.2.2 公钥密码算法 121.2.3 哈希函数 131.2.4 密码协议 141.3 密码应用与新进展 161.3.1 认证系统 161.3.2 数字签名 171.3.3 电子商务 181.3.4 信息伪装与信息隐藏 201.3.5 数字水印 211.4 网络安全面临的威胁 261.4.1 恶意攻击 271.4.2 安全缺陷 291.4.3 软件漏洞 311.4.4 结构隐患 361.5 网络安全体系结构 411.5.1 OSI安全服务 411.5.2 OSI安全机制 421.6 网络安全产品 431.6.1 防火墙 431.6.2 虚拟专用网 (VPN) 461.7 小结 49

第2章 入侵检测技术 512.1 入侵检测系统概述 512.1.1 入侵检测系统简介 522.1.2 入侵检测系统的历史 552.1.3 入侵检测系统的分类 562.1.4 入侵检测系统的功能 582.1.5 入侵检测系统的基本构成 582.1.6 入侵检测系统的评价标准 592.1.7 入侵检测系统的标准化 602.2 攻击者入侵的主要方法和手段 622.2.1 主要漏洞 622.2.2 侵入系统的主要途径 632.2.3 主要的攻击方法 632.3 入侵检测系统的信息源 652.3.1 基于主机的信息源 652.3.2 基于网络的数据源 672.3.3 应用程序的日志文件 682.3.4 其他入侵检测系统报警信息 692.4 入侵检测系统的关键技术 692.4.1 入侵检测技术 692.4.2 入侵检测系统描述语言 722.4.3 入侵检测系统的体系结构 742.4.4 代理和移动代理技术 762.4.5 安全部件互动协议和接口标准 792.5 入侵检测产品介绍 822.5.1 国外主要产品介绍 822.5.2 国内产品的现状 862.5.3 入侵检测系统的测试与评估 892.5.4 入侵检测系统在网络中的部署 922.5.5 入侵检测产品的选择 932.6 入侵检测系统的发展趋势和研究方向 94

第3章 蜜罐技术 973.1 蜜罐概述 973.1.1 蜜罐技术的发展背景 973.1.2 蜜罐的概念 983.1.3 蜜罐的安全价值 993.1.4 蜜罐面临的法律问题 1023.2 蜜罐的基本配置 1033.2.1 诱骗服务 1033.2.2 弱化系统 1043.2.3 强化系统 1043.2.4 用户模式服务器 1053.2.5 一个配置蜜罐的实例 1063.2.6 小结 1083.3 蜜罐的分类 1083.3.1 根据产品设计目的分类 1093.3.2 根据交互的程度分类 1093.3.3 蜜罐基本分类 1123.3.4 小结 1133.4 蜜罐产品 1143.4.1 DTK 1143.4.2 空系统 1143.4.3 BOF 1153.4.4 Specter 1163.4.5 Home-made蜜罐 1173.4.6 Honeyd 1173.4.7 SmokeDetector 1193.4.8 Bigeye 1193.4.9 LaBrea tarpit 1193.4.10 NetFacade 1203.4.11 KFSensor 1203.4.12 Tiny蜜罐 1213.4.13 Mantrap 1213.4.14 Honeynet 1223.4.15 小结 1223.5 Honeynet 1233.5.1 Honeynet的概念 1233.5.2 Honeynet与蜜罐的不同之处 1233.5.3 Honeynet的研究价值 1243.5.4 Honeynet的功能 1243.5.5 小结 1273.6 蜜罐信息的收集和分析技术 1283.6.1 蜜罐的信息收集 1293.6.2 信息收集和分析实例 1303.6.3 小结 1333.7 蜜罐的特点及发展趋势 1343.7.1 蜜罐的优缺点 1343.7.2 蜜罐的发展趋势 136

第4章 计算机取证技术 1374.1 计算机取证的基本概念 1374.1.1 计算机取证的定义 1374.1.2 电子证据的概念 1384.1.3 电子证据的特点 1394.1.4 常见电子设备中潜在的电子证据 1404.2 计算机取证的一般步骤 1414.2.1 计算机取证的基本原则 1424.2.2 计算机取证的一般步骤 1454.2.3 网络攻击和取证模型 1464.2.4 利用IDS取证 1474.2.5 利用蜜罐取证 1514.3 计算机取证的安全策略 1604.3.1 保留信息 1604.3.2 计划响应 1614.3.3 开展培训 1624.3.4 加速调查 1634.3.5 防止匿名 1644.3.6 保护证据 1654.3.7 结论 1654.4 计算机取证的常见工具 1664.4.1 Encase 1664.4.2 SafeBack 1684.4.3 NetMonitor 1694.4.4 其他常见工具 1714.5 计算机取证的法律问题 1724.5.1 电子证据的真实性 1724.5.2 电子证据的证明力 1754.5.3 取证工具的法律效力 1764.5.4 其他困难和挑战 1794.6 小结 180

第5章 物理隔离技术 1815.1 物理隔离概述 1815.1.1 物理隔离的概念 1815.1.2 物理隔离的作用 1835.1.3 物理隔离的误区 1895.2 物理隔离的原理、分类和发展趋势 1905.2.1 物理隔离的技术原理 1905.2.2 物理隔离的分类 1925.2.3 物理隔离的发展趋势 1995.3 物理隔离产品 1995.3.1 中网物理隔离网闸 (X-gap) 2005.3.2 伟思集团 2015.3.3 上海上科联合网络科技有限公司 2015.3.4 中国长城计算机深圳股份有限公司 2025.3.5 天行网安 2025.4 物理隔离的部署 2045.4.1 客户端的物理隔离 2045.4.2 集线器级的物理隔离 2045.4.3 服务器端的物理隔离 2045.4.4 物理隔离的典型实例 2045.4.5 物理隔离方案的选择 2075.5 物理隔离的不足之处 2085.5.1 物理隔离的安全特性 2085.5.2 物理隔离与其他安全措施的配合 209

附录1 国内入侵检测产品简介 211  
附录2 公安部通过的物理隔离安全产品 235  
附录3 参考资料 237



#### 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>