

<<计算机安全实验教程>>

图书基本信息

书名：<<计算机安全实验教程>>

13位ISBN编号：9787111258377

10位ISBN编号：7111258371

出版时间：2009-2

出版时间：陈波、于冷 机械工业出版社 (2009-02出版)

作者：陈波，于冷 编

页数：308

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>

<<计算机系统安全实验教程>>

前言

“信息安全”是一个直接面向工程、面向应用的专业领域。

信息安全课程的教学需要重视理论的讲授，使学生掌握解决问题的基本技术，更要强调实践教学，培养学生解决安全问题的操作能力，培养学生的整体安全意识和综合应用能力。

我们遵循信息安全PDRR模型的核心思想，以及“信息安全类专业指导性专业规范”项目组提出的“信息安全类专业知识体系”，并结合教材《计算机系统安全原理与技术》，编写了本书。

编写中我们力求做到：1) 内容系统、体系完整。

与《计算机系统安全原理与技术》(第2版)一书相对应，从以下几个层次研究信息安全问题：计算机硬件与环境安全、操作系统安全、计算机网络安全、数据库系统安全、应用系统安全以及安全管理。

设置的“信息安全”实验课程的内容包含9大类近40个模块。

第1类：密码学基础与密码技术应用，包括对称、非对称密码系统、公钥密码系统、消息摘要、数字签名、信息隐藏与数字水印等实验模块。

第2类：系统硬件安全，包括常用硬件设备的性能检测、将U盘改造成系统加密狗等实验模块。

第3类：操作系统安全，使用微软基准安全分析器分析系统漏洞、Windows系统账户口令强度测试、Windows系统安全配置、微软安全小工具的使用等实验模块。

第4类：数据库安全，包括SQLServer2000的安全管理等实验模块。

<<计算机系统安全实验教程>>

内容概要

《计算机系统安全实验教程》涉及了计算机系统各层次的安全问题和普遍采用的安全机制，包括密码基础知识、计算机硬件、操作系统、计算机网络、数据库系统、程序和应用系统、应急响应与灾难恢复、计算机系统安全风险评估等近40个安全实验。

实验教程既可与教材《计算机系统安全原理与技术》（第2版）配套使用，也可单独作为信息安全实验指导书，便于自学。

《计算机系统安全实验教程》设计的实验（包括网络环境下的安全实验）仅需在PC上实现，无需增加额外的软、硬件设备投资。

实验内容新颖，每个实验均给出了详细的操作步骤及相关代码，并给出了丰富的参考资料。

《计算机系统安全实验教程》可作为信息安全专业、信息对抗专业、计算机专业、信息工程专业或相近专业的本科或研究生教材，也可作为网络信息安全领域科技人员的参考书。

<<计算机系统安全实验教程>>

书籍目录

出版说明前言第1章 计算机系统安全虚拟实验环境搭建1.1 虚拟机软件VMware的使用1.2 基于VMware的虚拟安全实验平台第2章 密码学基础实验2.1 密码算法基础2.1.1 Windows系统中常用文档的保护与破解2.1.2 凯撒密码及其破解的编程实现2.1.3 DES算法编程实现2.1.4 RSA算法工具的使用2.1.5 RSA算法编程实现2.2 SHA—1算法编程实现2.3 DsA算法工具的使用2.4 信息隐藏与数字水印2.4.1 LSB信息隐藏算法编程实现2.4.2 数字水印常见工具的使用第3章 计算机系统硬件安全实验3.1 常见硬件检测工具的使用3.2 将U盘改造成系统加密狗3.3 U盘文件的盗取程序实现第4章 操作系统安全实验4.1 Windows操作系统安全防护4.1.1 Windows系统账户口令强度测试4.1.2 使用微软基准安全分析器MBSA分析系统漏洞4.1.3 Windows系统安全设置4.2 微软安全小工具的使用第5章 网络安全实验5.1 网络攻击与防范5.1.1 ARP欺骗攻击与防范5.1.2 网络扫描的编程实现5.1.3 网络嗅探的编程实现5.2 网络攻击防范5.2.1 网络防火墙的使用5.2.2 Windows下Snort入侵检测系统的使用5.3 网络应用安全5.3.1 SSH工具的使用5.3.2 利用OpenSSL的C / S安全通信程序设计第6章 数据库安全实验6.1 SQLServer 2000数据库的安全管理6.2 SQLServer 2000数据库的备份与恢复第7章 应用系统安全实验7.1 恶意代码的分析与检测7.1.1 使用系统行为监控软件SSM防范恶意代码7.1.2 使用超级巡警查杀恶意代码7.1.3 u盘病毒及其免疫程序的实现7.2 代码静态检测工具PC-Lint的使用7.3 软件保护常用技术编程实现7.4 使用WebScarab进行Web安全测试第8章 应急响应与灾难恢复实验8.1 数据恢复软件Easy Recovery的使用8.2 计算机取证软件EnCase的使用第9章 计算机系统安全风险评估9.1 安全漏洞扫描工具Nessus的使用9.2 信息安全风险评估工具的使用第10章 综合实验10.1 PGP的使用10.2 .NET框架下密码算法编程实

<<计算机系统安全实验教程>>

章节摘录

第1章 计算机系统安全虚拟实验环境搭建1.1 虚拟机软件VMware的使用【实验目的】信息安全课程中要进行相关的安全实验，有的实验需要至少两台主机及其独立的操作系统，且主机间可以通过以太网进行通信。

有的实验对系统本身以及对网络中其他主机有潜在的破坏性。

为此，利用虚拟机软件VMware在一台主机中再虚拟出一台PC并安装一套操作系统，以便完成后续的安全实验。

【实验类型】软件的安装、配置与使用。

【实验原理】1. 虚拟机的概念虚拟机的概念主要有两种，一种是像Java那样提供介于硬件和编译程序之间的软件；另一种是指利用软件"虚拟"出来一台计算机。

本实验中的虚拟机是指后者。

"虚拟机"是一个由软件提供的、具有模拟真实的特定硬件环境的计算机，虚拟机提供的"计算机"和真正的计算机一样，也包括CPU、内存、硬盘、光驱、软驱、显卡、声卡、SCSI卡、USB接口、PCI接口、BIOS等。

在虚拟机中可以 and 真正的计算机一样安装操作系统、应用程序和软件，也可以对外提供服务。

X86平台的虚拟化技术可分为3类，全硬件仿真虚拟化技术（Hardware Emulation）、半虚拟化技术（Para-Virtualization）和操作系统级虚拟化技术（OS-Level Virtualization）。

<<计算机安全实验教程>>

编辑推荐

《计算机安全实验教程》由机械工业出版社出版。

<<计算机系统安全实验教程>>

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>