

<<网络安全实验教程>>

图书基本信息

书名：<<网络安全实验教程>>

13位ISBN编号：9787302255307

10位ISBN编号：730225530X

出版时间：2011-7

出版时间：清华大学出版社

作者：孙建国 等编著

页数：171

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>

## <<网络安全实验教程>>

### 内容概要

《网络安全实验教程》基于网络安全体系结构，选择最新的网络安全实用软件和技术，在基本的网络安全实用技术和理论基础上，系统地讲授网络分析、远程控制技术、sslvpn技术、防火墙技术、入侵检测技术和虚拟蜜网技术等网络安全实验内容。

本书不仅介绍网络安全体系结构基本理论和方法，还设计了多个应用工具实例。

通过sniffer分析软件、pcanywhere远程控制程序、snort入侵检测系统以及honeywall蜜网架构等实验用例的训练，学生可以建立网络信息安全的体系概念，了解网络协议、数据包结构、网络安全管理技术等

在计算机系统的重要性。

《网络安全实验教程》取材新颖，采用实例教学的组织形式，内容由浅入深，循序渐进。

书中给出了大量设计实例及扩展方案，不仅可以作为教学内容进行学习，而且部分内容还具有工程实践价值。

本书可作为高等院校计算机类、电子类和自动化类等有关专业的教材和参考书。

# <<网络安全实验教程>>

## 书籍目录

### 第1章 网络安全实验概述

#### 1.1 引论

##### 1.1.1 网络安全现状及发展

##### 1.1.2 黑客及黑客入侵技术

##### 1.1.3 网络安全主要影响因素

#### 1.2 网络安全基本知识

##### 1.2.1 网络安全研究内容

##### 1.2.2 网络安全体系结构

##### 1.2.3 网络安全评价标准

##### 1.2.4 信息安全定义

#### 1.3 网络安全实验基本要求

### 第2章 网络安全研究内容

#### 2.1 密码技术

##### 2.1.1 基本概念

##### 2.1.2 密码算法

##### 2.1.3 网络安全应用

#### 2.2 防火墙技术

##### 2.2.1 防火墙体系结构

##### 2.2.2 包过滤防火墙

##### 2.2.3 代理防火墙

#### 2.3 入侵检测

##### 2.3.1 入侵检测技术分类

##### 2.3.2 入侵检测系统结构

##### 2.3.3 重要入侵检测系统

##### 2.3.4 入侵检测发展方向

#### 2.4 计算机病毒学

##### 2.4.1 计算机病毒定义

##### 2.4.2 计算机病毒分类

##### 2.4.3 病毒危害与防范

##### 2.4.4 防护与检测策略

#### 2.5 网络安全管理规范

##### 2.5.1 信息网络安全策略

##### 2.5.2 信息网络管理机制

### 第3章 网络分析实验

#### 3.1 网络分析原理

##### 3.1.1 tcp / ip原理

##### 3.1.2 交换技术

##### 3.1.3 路由技术

##### 3.1.4 网络嗅探技术

#### 3.2 sniffer网络分析实例

##### 3.2.1 sniffer pro简介

##### 3.2.2 程序安装实验

##### 3.2.3 数据包捕获实验

##### 3.2.4 网络监视实验

#### 3.3 扩展实验

## <<网络安全实验教程>>

- 3.3.1网络协议嗅探
- 3.3.2ftp协议分析
- 3.3.3telnet协议分析
- 3.3.4多协议综合实验

### 第4章 远程控制实验

- 4.1远程控制原理
  - 4.1.1远程控制技术
  - 4.1.2远程控制方式
  - 4.1.3远程控制软件
- 4.2pcanywhere远程控制实例
  - 4.2.1软件的安装与使用
  - 4.2.2配置被控端(hosts)
  - 4.2.3配置主控端(remotes)
- 4.3扩展实验

### 第5章 ssl vpn实验

- 5.1ssl vpn原理
  - 5.1.1基本概念
  - 5.1.2ssl vpn
- 5.2vpn配置实验
- 5.3ssl vpn配置实验

### 第6章 防火墙实验

- 6.1防火墙技术
  - 6.1.1基本概念
  - 6.1.2个人防火墙
- 6.2天网防火墙实验
- 6.3瑞星防火墙实验
- 6.4防火墙评测实验

### 第7章 入侵检测实验

- 7.1入侵检测原理
  - 7.1.1入侵检测步骤
  - 7.1.2检测技术特点
  - 7.1.3snort简介
- 7.2snort入侵检测实例
- 7.3snort扩展实验

### 第8章 虚拟蜜网实验

- 8.1虚拟蜜网系统
  - 8.1.1蜜网技术
  - 8.1.2虚拟蜜网
- 8.2搭建虚拟蜜网
- 8.3漏洞扫描实验
- 8.4渗透攻击实验

### 参考文献

## 章节摘录

版权页：插图：1.2.4 信息安全定义信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，免受破坏、更改和泄露，系统连续可靠正常地运行，信息服务不中断。

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合学科。

随着信息安全技术的发展，经历了从基本安全隔离、主机加固阶段，到后来的网络认证阶段，直到将行为监控和审计也纳入安全的范畴。

这样的演变不仅仅是为了避免恶意攻击，更重要的是为了提高网络的可信度。

信息安全的内涵在不断的延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。

从广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

目前常用的基础性安全技术包括以下内容。

## <<网络安全实验教程>>

### 编辑推荐

《网络安全实验教程》为教育部“高等学校教学质量与教学改革工程”立项项目。

<<网络安全实验教程>>

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>