

<<网络安全技术理论与实践>>

图书基本信息

书名：<<网络安全技术理论与实践>>

13位ISBN编号：9787302281924

10位ISBN编号：7302281920

出版时间：2012-6

出版时间：清华大学出版社

作者：廉龙颖 编

页数：278

字数：446000

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>

## <<网络安全技术理论与实践>>

### 内容概要

《21世纪高等院校计算机网络工程专业规划教材·网络安全技术理论与实践》全面地介绍了计算机网络安全的情况和发展趋势。

全书分为15章，全面讲述网络安全的基础知识（网络安全概述和网络安全编程基础），网络安全攻击技术（黑客与隐藏ip技术，网络扫描与网络监听，网络攻击，网络后门与清除日志，计算机病毒的防治），网络安全防御技术（操作系统安全配置方案，防火墙技术，入侵检测，信息加密与认证技术，无线网络安全）及网络安全工程（网络安全管理，网络安全方案设计）。

《21世纪高等院校计算机网络工程专业规划教材·网络安全技术理论与实践》基本概念清晰，表达深入浅出，内容翔实，重点突出，理论与实践相结合，实用性强，易于教学。

《21世纪高等院校计算机网络工程专业规划教材·网络安全技术理论与实践》可作为信息安全、计算机、网络工程等专业本科生的教科书，也可供从事相关专业教学、科研和工程的人员参考。

# <<网络安全技术理论与实践>>

## 书籍目录

### 第1章 网络安全概述

- 1.1 网络安全的攻防体系研究
- 1.2 研究网络安全的必要性和社会意义
- 1.3 网络安全的法律法规体系
- 1.4 网络安全标准
- 1.5 网络安全的评估标准
- 1.6 实验环境配置

思考与练习

### 第2章 网络安全基础

- 2.1 osi参考模型
- 2.2 tcp / ip协议簇
- 2.3 网际协议ip
- 2.4 网际控制报文协议icmp
- 2.5 地址解析协议arp
- 2.6 传输控制协议tcp
- 2.7 用户数据报协议udp
- 2.8 常用的网络服务
- 2.9 常用的网络命令

思考与练习

### 第3章 网络安全编程基础

- 3.1 网络安全编程概述
- 3.2 asp . net语言编程
- 3.3 网络安全编程实例

思考与练习

### 第4章 黑客与隐藏ip技术

- 4.1 黑客
- 4.2 隐藏ip

思考与练习

### 第5章 网络扫描与网络监听

- 5.1 信息搜集
- 5.2 网络扫描
- 5.3 网络监听

思考与练习

### 第6章 网络攻击

- 6.1 社会工程学攻击
- 6.2 物理攻击
- 6.3 暴力攻击
- 6.4 unicode漏洞攻击
- 6.5 sql注入攻击
- 6.6 缓冲区溢出攻击
- 6.7 基于木马的攻击
- 6.8 拒绝服务攻击

思考与练习

### 第7章 网络后门与清除日志

- 7.1 网络后门

## <<网络安全技术理论与实践>>

### 7.2 清除日志

#### 思考与练习

### 第8章 计算机病毒的防治

#### 8.1 计算机病毒概述

#### 8.2 计算机病毒技术

#### 8.3 计算机病毒实例

#### 8.4 计算机病毒的检测与防范

#### 思考与练习

### 第9章 操作系统安全配置方案

#### 9.1 windows操作系统

#### 9.2 windows nt的系统结构

#### 9.3 windows nt的安全模型

#### 9.4 操作系统常规安全措施

#### 9.5 操作系统中级安全配置措施

#### 9.6 操作系统高级安全配置措施

#### 思考与练习

### 第10章 防火墙技术

#### 10.1 防火墙概述

#### 10.2 防火墙的功能

#### 10.3 防火墙的发展和类型

#### 10.4 防火墙体系结构

#### 10.5 防火墙选择原则

#### 10.6 某企业销售系统中防火墙建立实例

#### 10.7 常用防火墙的配置

#### 10.8 防火墙的发展趋势

#### 思考与练习

### 第11章 入侵检测

#### 11.1 入侵检测概述

#### 11.2 入侵检测原理及主要方法

#### 11.3 入侵检测系统

#### 11.4 入侵检测系统示例

#### 思考与练习

### 第12章 信息加密与认证技术

#### 12.1 密码学基本概念

#### 12.2 加密体制分类

#### 12.3 des对称加密技术

#### 12.4 rsa公钥加密技术

#### 12.5 信息加密技术应用

#### 12.6 认证技术

#### 思考与练习

### 第13章 无线网络安全

#### 13.1 无线局域网(wlan)

#### 13.2 无线个域网(wpan)

#### 13.3 无线城域网(wman)

#### 13.4 无线网络面临的安全威胁

#### 13.5 无线局域网的安全技术

#### 思考与练习

## <<网络安全技术理论与实践>>

### 第14章 网络安全管理

- 14.1 网络安全管理背景
- 14.2 网络安全管理过程
- 14.3 评审整体信息安全策略
- 14.4 评审网络体系结构和应用
- 14.5 识别网络连接类型
- 14.6 识别网络特性和信任关系
- 14.7 识别安全风险
- 14.8 识别控制区域
- 14.9 实施和运行安全控制措施
- 14.10 监视和评审实施

#### 思考与练习

### 第15章 网络安全方案设计

- 15.1 网络安全方案概念
- 15.2 网络安全案例需求
- 15.3 解决方案设计

#### 思考与练习

#### 参考文献

## 章节摘录

版权页：插图：1.5 网络安全的评估标准为实现对网络安全的定性评价，美国国防部所属的国家计算机安全中心（NCSC）在20世纪90年代提供了网络安全性标准（DoD5200.28-STD），即可信任计算机标准评估准则（Trusted Computer Standards Evaluation Criteria, TCSEC），也叫橘黄皮书（Orange Book）。

该标准认为要使系统免受攻击，对应不同的安全级别，硬件、软件和存储的信息应实施不同的安全保护。

安全级别对不同类型的物理安全、用户身份验证、操作系统软件的可信任性和用户应用程序进行了安全描述。

目前，TCSEC已经成为了现行的网络安全标准。

TCSEC将网络安全性等级划分为A、B、C、D4类共7级，其中，A类安全等级最高，D类安全等级最低。

1.D级D级也称为酌情安全保护，是可用的最低安全形式。

该标准说明整个系统都是不可信任的。

对硬件来说，没有任何保护，操作系统容易受到损害，对于用户和他们对存储在计算机上信息的访问权限没有身份认证。

2.C1级C级有两个安全子级别，即C1和C2，也称为自选安全保护系统，它描述了一个UNIX系统上可用的级别。

对硬件来说，存在某种程度的保护，因为它不再那么容易受到损害，尽管这种可能性存在。

用户必须通过用户注册名和口令系统识别自己，用这种方式来确定每个用户对程序和信息拥有什么样的访问权限。

3.C2级除C1级包含的特征外，C2级还包括其他的创建受控访问环境的安全特性，该环境具有进一步限制用户执行某些命令或访问某些文件的能力。

这不仅基于许可权限，而且基于身份验证级别，另外，这种安全级别要求对系统加以审核，审核可用来跟踪记录所有与安全有关的事件，比如哪些是由系统管理员执行的活动。

4.B1级B级也称为被标签的安全性保护，分为三个子级别。

B1级或称为标准安全保护，是支持多级安全的第一个级别，这一级说明了一个处于强制性访问控制之下的对象，不允许文件的拥有者改变其许可权限。

5.B2级B2级也称为结构保护，要求计算机系统中所有对象都加标签，而且给设备分配单个或多个安全级别。

这是提出的较高安全级别的对象与另一个较低安全级别的对象相互通信的第一个级别。

6.B3级B3级也称为安全域级别，使用安装硬件的办法来加强域，例如，内存管理硬件用来保护安全域免遭无授权访问或其他安全域对象的修改。

<<网络安全技术理论与实践>>

编辑推荐

《21世纪高等院校计算机网络工程专业规划教材:网络安全技术理论与实践》由清华大学出版社出版。

<<网络安全技术理论与实践>>

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>