

<<网络安全技术>>

图书基本信息

书名：<<网络安全技术>>

13位ISBN编号：9787111379256

10位ISBN编号：711137925X

出版时间：2012-6

出版时间：机械工业出版社

作者：陈卓 编

页数：211

字数：339000

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>>

### 内容概要

本书在第1版的基础上进行了修改和完善，全面介绍了网络安全的基本概念、原理以及应用，主要内容包括密码算法基础、身份认证技术、黑客攻击与防范、计算机病毒的原理与防御、防火墙技术及应用、入侵检测技术、操作系统安全、数据的备份与恢复，最后介绍了网络安全系统的规划与设计。

本书根据高职高专计算机网络技术专业的要求编写，并考虑了计算机相关专业的要求，内容丰富，文字浅显易懂，可作为高职高专计算机网络以及计算机应用等专业的教材，也可作为计算机爱好者的自学参考书。

为方便教学，本书配备电子课件等教学资源。

凡选用本书作为教材的教师均可登录机械工业出版社教材服务网

本书根据高职高专计算机网络技术专业的要求编写，并考虑了计算机相关专业的要求，内容丰富，文字浅显易懂，可作为高职高专计算机网络以及计算机应用等专业的教材，也可作为计算机爱好者的自学参考书。

# <<网络安全技术>>

## 书籍目录

前言

第1章 计算机网络安全概述

1.1引言

1.2主要的网络安全技术

1.3我国计算机网络安全现状

1.4计算机网络安全的级别分类

1.5网络安全法律法规

本章小结

复习思考题

第2章 密码算法基础

2.1密码学简介

2.2如何保证机密性

2.3防止消息被篡改

2.4数字签名

2.5密码算法应用实例

本章小结

复习思考题

实践与训练

第3章 身份认证技术

3.1口令机制

3.2采用数字证书进行身份认证

3.3采用IC卡与指纹认证身份

本章小结

复习思考题

实践与训练

第4章 黑客攻击与防范

4.1概述

4.2信息踩点

4.3网络扫描

4.4网络监听

4.5DoS/DDoS攻击与防范

本章小结

复习思考题

实践与训练

第5章 计算机病毒的原理与防御

5.1计算机病毒简介

5.2几种典型病毒的特征与防范

5.3“流氓”软件与网络钓鱼

5.4常用杀毒软件

本章小结

复习思考题

实践与训练

第6章 防火墙技术及应用

6.1防火墙简介

6.2防火墙的技术类型

## <<网络安全技术>>

- 6.3 防火墙的分类
- 6.4 防火墙的体系结构
- 6.5 防火墙的功能与缺陷
- 6.6 硬件防火墙
- 6.7 防火墙应用实例

本章小结

复习思考题

实践与训练

### 第7章 入侵检测系统

- 7.1 入侵检测系统简介
- 7.2 入侵检测系统的分类
- 7.3 商业入侵检测系统介绍
- 7.4 入侵检测系统的部署
- 7.5 入侵检测系统应用实例

本章小结

复习思考题

实践与训练

### 第8章 操作系统安全

- 8.1 操作系统概述
- 8.2 Windows安全
- 8.3 Windows系统下Web、FTP服务器安全配置

本章小结

复习思考题

实践与训练

### 第9章 数据的备份与恢复

- 9.1 数据备份
- 9.2 数据备份工具
- 9.3 常用的数据恢复工具

本章小结

复习思考题

实践与训练

### 第10章 网络安全系统的规划与设计

- 10.1 网络安全系统规划设计概述
- 10.2 网络安全系统规划设计的基本方法
- 10.3 网络安全系统规划设计案例

本章小结

复习思考题

实践与训练

参考文献

## 章节摘录

版权页：插图：2.C级安全 C级有两个安全子级别，即C1级和C2级。

(1) C1级安全 C1级安全又称自由选择性安全保护 ( Discretionary Security Protection ) 级别，它描述了一种典型的在UNIX系统上的安全级别。

这种级别的系统对硬件提供了某种程度的保护，用户拥有注册账号和口令系统，通过账号和口令来识别用户是否合法，并决定用户对程序和数据有什么样的访问权，但其硬件受到损害的可能性仍然存在。

用户拥有的访问权是指对文件的访问权。

文件的拥有者和超级用户 ( Root ) 可以改动文件中的访问属性，从而对不同的用户给予不同的访问权。

例如，让文件拥有者具有读/写和执行的权力，而给其他用户只分配读的权力。

(2) C2级安全 C2级以C1级标准为基础，除了具有C1级包含的特性外，C2级系统还具有访问控制环境 ( Controlled—Access Environment ) 的权力。

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权限，而且还加入了身份认证级别。

另外，系统对发生的事件加以审计 ( Audit )，并写入日志当中，如什么时候开机，哪个用户在什么时候从哪里登录等，这样通过查看日志，就可以发现入侵的痕迹，如多次登录失败，也可以大致推测出可能有人想强行闯入系统。

审计除了可以记录下系统管理员执行的活动以外，还加入了身份认证级别，这样就可以知道谁在执行这些命令。

能够达到C2级的常见操作系统有：UNIX、XENIX、Netware 3.0、Windows NT等。

3.B级安全 B级安全也称为强制性安全保护，包括三个子级别，即B1级、B2级和B3级。

(1) B1级安全 B1级即标志安全保护 ( Labeled Security Protection )，是支持多级安全 ( 如秘密和绝密 ) 的第一个级别，这个级别说明一个处于强制性访问控制之下的对象 ( 如磁盘或文件服务器目录 )，系统不允许文件的使用者修改其许可权限，这种用户标志和加密标志的双重保护，加强了系统信息的安全性。

B1级的计算机安全措施，视操作系统而定，政府机关和安全承包商们是B1级计算机系统的主要拥有者。



#### 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>