北京市高等教育精品教材立项项目

高等学校计算机科学与技术教材

中国大学出版社图书奖首届优秀教材奖一等奖

- 原理与技术的完美结合
- 教学与科研的最新成果
- 语言精炼，实例丰富
- 可操作性强，实用性突出

# 计算机网络安全教程

## （第2版）

□ 石志国　薛为民　尹浩　编著

清华大学出版社　●　北京交通大学出版社

北京市高等教育精品教材立项项目·高等学校计算机科学与技术教材

中国大学出版社图书奖首届优秀教材奖一等奖

# 计算机网络安全教程

## （第2版）

石志国　薛为民　尹　浩　编著

清华大学出版社

北京交通大学出版社

·北京·

## 内 容 简 介

本书在原书修订版基础上，参考很多老师的修改意见，对相关内容做了大量修整，使之更加适合高校教学和自学的需要。本书通过大量的实例来讲解知识点，将安全理论、安全工具与安全编程三方面内容有机地结合到一起，适量增加了理论部分的分量，同时配备了实验指导书。

全书从网络安全体系上分成四部分。第一部分：计算机网络安全基础，介绍网络安全的基本概念、实验环境配置、网络安全协议基础及网络安全编程基础。第二部分：网络安全攻击技术，详细介绍了攻击技术“五部曲”及恶意代码的原理和实现。第三部分：网络安全防御技术，操作系统安全相关原理、加密与解密技术的应用、防火墙、入侵检测技术以及 IP 和 Web 安全相关理论。第四部分：网络安全综合解决方案，从工程的角度介绍了网络安全工程方案的编写。

本书可以作为高校以及各类培训机构相关课程的教材或参考书。本书提供的全书源代码、所有的涉及软件和授课幻灯片等教学支持信息，可以从图书支持网站 http://www.gettop.net 下载，也可以从出版社网站 http://press.bjtu.edu.cn 的下载栏目中下载。



**图书在版编目（CIP）数据**

计算机网络安全教程 / 石志国，薛为民，尹浩编著. —2 版. —北京：清华大学出版社；北京交通大学出版社，2011.2

（高等学校计算机科学与技术教材）

ISBN 978-7-5121-0469-3

Ⅰ. ①计… Ⅱ. ①石… ②薛… ③尹… Ⅲ. ①计算机网络-安全技术-高等学校：技术学校-教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2011）第 010074 号

责任编辑：谭文芳

出版发行：清 华 大 学 出 版 社　邮编：100084　电话：010-62776969　http://www.tup.com.cn

北京交通大学出版社　邮编：100044　电话：010-51686414　http://press.bjtu.edu.cn

印 刷 者：北京瑞达方舟印务有限公司

经　　销：全国新华书店

开　　本：185×260　印张：21.75　字数：554 千字

版　　次：2011 年 2 月第 2 版　2011 年 2 月第 1 次印刷

书　　号：ISBN 978-7-5121-0469-3/TP・632

印　　数：1～10 000 册　定价：31.00 元

# 前　言

本书在原书修订版的基础上，参考了很多老师的意见，对内容做了大量修整和扩充，使之更加适合高校教学和自学的需要。本书通过大量的实例来讲解知识点，将安全理论、安全工具与安全编程三方面内容有机地结合到一起，每章最后都配有大量的习题，用来检查教学和学习的进度。

## 与前两版的比较

2004 年初，《计算机网络安全教程》出版，目的是为了解决网络安全技术教学的迫切需要。书中综合了作者在北京大学计算机研究所的部分研究内容、清华大学计算机系的部分教学内容，以及网络信息安全国际认证考试的部分内容，在写作过程中还得到了当时三院院士王选老师的支持和指导。本书出版以来，受到了广大读者的认可和欢迎，同时，很多读者也提出了很多中肯的批评和改进意见。当前，网络安全是计算机相关领域中的一门重要学科，很多高校和研究机构都设置了网络信息安全本科专业，以及网络信息安全方向的硕士点和博士点。

2007 年初出版了《计算机网络安全教程》修订版，在保证第 1 版整体结构的情况下，对内容进行了全面的扩充和修正，一个主要的特点是理论性的增强，主要有以下 6 方面。

（1）增强了书的理论性并全面阐述了网络安全两个重要的概念：恶意代码和 Web 安全，添加了两章，分别为第 7 章恶意代码和第 11 章 IP 安全与 Web 安全，将全书扩充为 12 章。

（2）修正了部分内容不规范、图表不清楚的问题。

（3）全面扩充了拒绝服务攻击和分布式拒绝服务攻击的分类和原理。

（4）增加了安全操作系统的机制与原理。

（5）增加了数字签名、数字水印和公钥基础设施 PKI 的相关内容。

（6）为了检查教学以及自学的效果，每章都重新设计了选择题、填空题和问答题，并在书后给出选择题和填空题的参考答案。

2010 年，通过网络征集了很多修改意见。针对老师们意见较多的恶意代码一章，进行重写，其他章节同时进行了修改和完善。在没有增加篇幅的前提下，主要做了如下 4 个方面的调整。

（1）重新编写恶意代码一章，重点介绍了常见的 PE 病毒、脚本病毒、U 盘病毒以及网络蠕虫的原理与实现，并用程序展示了各种病毒的传染方法。

（2）修正了部分内容不规范的问题。例如：RSA 算法中，公钥是 e，私钥是 d，这是一个大家都默认的规则，而且在教材中前面是 a，b，后面是 e，d，内容不严谨。

（3）增加了部分原理介绍，如端口扫描、克隆账户及操作系统漏洞，等等。

（4）增加了配套的实验指导，并设计了 10 个实验，同时优化了相关的配套资料。

## 本书结构

因为每一章内容都比较庞杂，所以每一章前面设计了“本章要点”，提示本章重点掌握的内容。每一章后面设计了适量的习题，主要是针对本章重点、难点进行训练。附录提供了选择题和填空题的答案，便于读者对照检查自己的学习效果。

## 本书导读

网络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性科学。全书从三个角度介绍计算机网络安全技术：计算机网络安全理论、网络安全攻防工具和网络安全编程，这三方面内容均来自实际的工程以及课堂的实践，并通过网络安全攻防体系结合在一起。从网络安全攻防体系上，全书分成四部分，共十二章。

### 第 1 部分：网络安全基础

第 1 章 网络安全概述与环境配置：介绍信息安全和网络安全的研究体系、研究网络安全的意义、评价网络安全的标准和实验环境的配置。

第 2 章 网络安全协议基础：介绍 OSI 参考模型和 TCP/IP 协议组，实际分析 IP，TCP，UDP，ICMP 协议的结构，以及工作原理、网络服务和网络命令。

第 3 章 网络安全编程基础：介绍网络安全编程的基础知识、C 和 C++的几种编程模式，以及网络安全编程的常用技术，如 Socket 编程、注册表编程和驻留编程，等等。

### 第 2 部分：网络攻击技术

第 4 章 网络扫描与网络监听：介绍黑客及黑客攻击的基本概念、如何利用工具实现网络踩点、网络扫描和网络监听。

第 5 章 网络入侵：介绍常用的网络入侵技术，如社会工程学攻击、物理攻击、暴力攻击、漏洞攻击和缓冲区溢出攻击等。

第 6 章 网络后门与网络隐身：介绍网络后门和木马的基本概念，并利用四种方法实现网络后门；介绍利用工具实现网络跳板和网络隐身。

第 7 章 恶意代码：介绍恶意代码的发展史，恶意代码长期存在的原因；介绍常见恶意代码的原理，程序实现常见的 PE 病毒、脚本病毒、U 盘病毒，等等。

### 第 3 部分：网络防御技术

第 8 章 操作系统安全基础：介绍 UNIX、Linux 和 Windows 的特点，着重介绍安全操作系统的原理，介绍 Windows 操作系统的安全配置方案。

第 9 章 密码学与信息加密：介绍密码学的基本概念，DES 加密算法的概念及如何利用程序实现，RSA 加密算法的概念及实现算法，PGP 加密的原理及实现。

第 10 章 防火墙与入侵检测：介绍防火墙的基本概念、分类、实现模型，以及如何利用软件实现防火墙的规则集；介绍入侵检测系统的概念、原理，以及如何利用程序实现简单的入侵检测系统。

第 11 章 IP 安全与 Web 安全：介绍 IPSec 的必要性，IPSec 中的 AH 协议和 ESP 协议、密钥交换协议 IKE 及 VPN 的解决方案等。

### 第 4 部分：网络安全综合解决方案

第 12 章 网络安全方案设计：从网络安全工程的角度介绍网络安全方案编写的注意点和评价标准。

## 致谢

本书第 1 版出版以来，很多老师和同学提出了批评和改进意见，很多意见非常中肯和真诚，对此，首先向他们表示感谢，我们也会尽全力通过网页和电子邮件等方式为读者提供更为周到的服务。

其次要感谢的是很多在网上提出了修改意见的读者，他们在提出意见的同时，还真诚勇敢地在网上留下自己的真实联系方式。他们是：武汉科技大学中南分校信息工程学院计算机网络系的赵义老师，山东力明科技职业学院理工学院的仝瑞钦老师，北京市房山区理工大房山分校的张志军老师，福建工业学校邱云芳老师，西安科技大学通信学院院办刘涛老师，湖南科技学院计算机与通信工程系徐钢峰老师，青岛远洋船员学院乔显亮老师，电子科技大学成都学院文炜老师，成都高新西区团结学院路杨道静老师，四川省成都市芳草街的余伟老师，等等，这里不再一一列举。还有很多老师通过电子邮件反馈了修改意见，例如：李学宝等老师通过电子邮件提出了非常详细的修改意见，这里对他们表示最深切的谢意！

在编写过程中，还得到众多老师的指导和帮助。在这里要感谢中科院软件所卿斯汉研究员、贺也平研究员、梁洪亮博士、商青华博士、周启明博士、张宏博士和金洁华工程师；感谢清华大学计算机系林闯主任、尹浩副教授；感谢北京科技大学王志良教授、徐正光教授、张晓彤教授和解仑教授；感谢中央广播电视大学崔林教授，徐孝凯教授、田萧老师和王春凤老师；感谢中国软件行业协会邱钦伦高级工程师。感谢他们为本书提供了大量并且详尽的编程资料，并为本书解决了很多编程方面的问题。

尤其要感谢的是北京交通大学出版社的编辑谭文芳老师，7 年来她稳定的支持是本书能及时更新的关键。

## 图书支持

本书可以作为高校以及各类培训机构相关课程的教材或教学参考书，网络安全自学人员和网络安全开发人员的参考书。本书提供完整的教学幻灯片、书中的所有软件和源代码以及相关学习资源，将在 http://www.gettop.net 或者 http://press.bjtu.edu.cn 下载栏目中发布，欢迎访问和下载。

由于作者水平和时间有限，难免出现错误，对于本书的任何问题请使用 E-mail 发送到作者邮箱：shizhiguo@tom.com。

石志国

2010 年 12 月

# 目　录

## 第 1 部分　网络安全基础

## 第 2 部分 网络攻击技术

## 第 3 部分 网络防御技术

## 第 4 部分 网络安全综合解决方案

# 第 1 部分

# 网络安全基础

1

☑ 第 1 章　网络安全概述与环境配置

☑ 第 2 章　网络安全协议基础

☑ 第 3 章　网络安全编程基础

所谓教育，是忘却了在校学的全部内容之后剩下的本领。

—— 阿尔伯特 · 爱因斯坦（Albert Einstein）

对一切来说，只有热爱才是最好的老师，它远远胜过责任感。

—— 阿尔伯特 · 爱因斯坦（Albert Einstein）

不是所有能计算的都有价值，不是所有有价值的都能被计算。

—— 阿尔伯特 · 爱因斯坦（Albert Einstein）