



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

- ① 原理与技术的完美结合
- ② 教学与科研的最新成果
- ③ 语言精炼，实例丰富
- ④ 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。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13501256678 13801310933

### 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

---

本书如有质量问题, 请向北京交通大学出版社质监组反映。对您的意见和批评, 我们表示欢迎和感谢。

投诉电话: 010-51686043, 51686008; 传真: 010-62225406; E-mail: [press@bjtu.edu.cn](mailto:press@bjtu.edu.cn)。

# 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 and 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全瑞钦老师，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、田萧老师和王春风老师；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](mailto:shizhiguo@tom.com)。

# 目 录

## 第 1 部分 网络安全基础

第 1 章 网络安全概述与环境配置 .....	3
1.1 信息安全概述 .....	3
1.1.1 信息安全研究层次 .....	3
1.1.2 信息安全的基本要求 .....	4
1.1.3 信息安全的发展 .....	4
1.1.4 可信计算概述 .....	5
1.2 网络安全概述 .....	5
1.2.1 网络安全的攻防体系 .....	5
1.2.2 网络安全的层次体系 .....	7
1.3 研究网络安全的必要性 .....	8
1.3.1 物理威胁 .....	8
1.3.2 系统漏洞威胁 .....	8
1.3.3 身份鉴别威胁 .....	8
1.3.4 线缆连接威胁 .....	9
1.3.5 有害程序威胁 .....	9
1.4 研究网络安全的社会意义 .....	10
1.4.1 网络安全与政治 .....	10
1.4.2 网络安全与经济 .....	10
1.4.3 网络安全与社会稳定 .....	10
1.4.4 网络安全与军事 .....	11
1.4.5 网络安全与青少年成长 .....	11
1.5 网络安全的相关法规 .....	12
1.5.1 我国立法情况 .....	12
1.5.2 国际立法情况 .....	12
1.6 网络安全的评价标准 .....	13
1.6.1 我国评价标准 .....	13
1.6.2 国际评价标准 .....	13
1.7 环境配置 .....	15
1.7.1 配置 VMware 虚拟机 .....	16
1.7.2 网络抓包软件 Sniffer Pro .....	22
小结 .....	25

课后习题 .....	26
<b>第 2 章 网络安全协议基础 .....</b>	<b>27</b>
2.1 OSI 参考模型 .....	27
2.2 TCP/IP 协议族 .....	29
2.2.1 TCP/IP 协议族模型 .....	29
2.2.2 解剖 TCP/IP 模型 .....	29
2.2.3 TCP/IP 协议族与 OSI 参考模型对应关系 .....	30
2.3 网际协议 IP .....	31
2.3.1 IP 协议的头结构 .....	31
2.3.2 IPv4 的 IP 地址分类 .....	33
2.3.3 子网掩码 .....	34
2.4 传输控制协议 TCP .....	35
2.4.1 TCP 协议的头结构 .....	35
2.4.2 TCP 协议的工作原理 .....	38
2.4.3 TCP 协议的“三次握手” .....	38
2.4.4 TCP 协议的“四次挥手” .....	40
2.5 用户数据报协议 UDP .....	42
2.5.1 UDP 协议和 TCP 协议的区别 .....	42
2.5.2 UDP 协议的头结构 .....	43
2.5.3 UDP 数据报分析 .....	43
2.6 ICMP 协议 .....	44
2.6.1 ICMP 协议的头结构 .....	45
2.6.2 ICMP 数据报分析 .....	45
2.7 常用的网络服务 .....	45
2.7.1 FTP 服务 .....	45
2.7.2 Telnet 服务 .....	46
2.7.3 E-mail 服务 .....	48
2.7.4 Web 服务 .....	49
2.7.5 常用的网络服务端口 .....	49
2.8 常用的网络命令 .....	49
2.8.1 ping 指令 .....	50
2.8.2 ipconfig 指令 .....	50
2.8.3 netstat 指令 .....	51
2.8.4 net 指令 .....	52
2.8.5 at 指令 .....	54
2.8.6 tracert 命令 .....	55
小结 .....	55
课后习题 .....	56
<b>第 3 章 网络安全编程基础 .....</b>	<b>57</b>



3.1	网络安全编程概述 .....	57
3.1.1	Windows 内部机制 .....	57
3.1.2	学习 Windows 下编程 .....	58
3.1.3	选择编程工具 .....	59
3.2	C 和 C++的几种编程模式 .....	62
3.2.1	面向过程的 C 语言 .....	62
3.2.2	面向对象的 C++语言 .....	64
3.2.3	SDK 编程 .....	67
3.2.4	MFC 编程 .....	73
3.3	网络安全编程 .....	78
3.3.1	Socket 编程 .....	78
3.3.2	注册表编程 .....	80
3.3.3	文件系统编程 .....	86
3.3.4	定时器编程 .....	88
3.3.5	驻留程序编程 .....	90
3.3.6	多线程编程 .....	96
	小结 .....	99
	课后习题 .....	99

## 第 2 部分 网络攻击技术

第 4 章	网络扫描与网络监听 .....	103
4.1	黑客概述 .....	103
4.1.1	黑客分类 .....	103
4.1.2	黑客精神 .....	104
4.1.3	黑客守则 .....	104
4.1.4	攻击五部曲 .....	105
4.1.5	攻击和安全的关系 .....	105
4.2	网络踩点 .....	106
4.3	网络扫描 .....	106
4.3.1	网络扫描概述 .....	106
4.3.2	被动式策略扫描 .....	107
4.3.3	主动式策略扫描 .....	113
4.4	网络监听 .....	115
	小结 .....	117
	课后习题 .....	118
第 5 章	网络入侵 .....	119
5.1	社会工程学攻击 .....	119
5.2	物理攻击与防范 .....	119
5.2.1	获取管理员密码 .....	120

5.2.2	权限提升 .....	121
5.3	暴力攻击 .....	122
5.3.1	字典文件 .....	122
5.3.2	暴力破解操作系统密码 .....	123
5.3.3	暴力破解邮箱密码 .....	123
5.3.4	暴力破解软件密码 .....	124
5.4	Unicode 漏洞专题 .....	126
5.4.1	Unicode 漏洞的检测方法 .....	126
5.4.2	使用 Unicode 漏洞进行攻击 .....	129
5.5	其他漏洞攻击 .....	132
5.5.1	利用打印漏洞 .....	132
5.5.2	SMB 致命攻击 .....	133
5.6	缓冲区溢出攻击 .....	134
5.6.1	RPC 漏洞溢出 .....	135
5.6.2	利用 IIS 溢出进行攻击 .....	136
5.6.3	利用 WebDav 远程溢出 .....	139
5.7	拒绝服务攻击 .....	143
5.7.1	SYN 风暴 (SYN flooding) .....	143
5.7.2	Smurf 攻击 .....	144
5.7.3	利用处理程序错误进行攻击 .....	145
5.8	分布式拒绝服务攻击 .....	146
5.8.1	DDos 的特点 .....	146
5.8.2	攻击手段 .....	147
5.8.3	DDos 的著名攻击工具 .....	147
	小结 .....	148
	课后习题 .....	148
<b>第 6 章</b>	<b>网络后门与网络隐身 .....</b>	<b>150</b>
6.1	网络后门 .....	150
6.1.1	留后门的艺术 .....	150
6.1.2	常见后门工具的使用 .....	150
6.1.3	连接终端服务的软件 .....	159
6.1.4	命令行安装开启对方的终端服务 .....	162
6.2	木马 .....	163
6.2.1	木马和后门的区别 .....	163
6.2.2	常见木马的使用 .....	163
6.3	网络代理跳板 .....	166
6.3.1	网络代理跳板的作用 .....	166
6.3.2	网络代理跳板工具的使用 .....	167
6.4	清除日志 .....	170

6.4.1	清除 IIS 日志 .....	171
6.4.2	清除主机日志 .....	172
	小结 .....	181
	课后习题 .....	181
<b>第 7 章</b>	<b>恶意代码 .....</b>	<b>182</b>
7.1	恶意代码概述 .....	182
7.1.1	研究恶意代码的必要性 .....	182
7.1.2	恶意代码的发展史 .....	182
7.1.3	恶意代码长期存在的原因 .....	184
7.2	恶意代码实现机理 .....	185
7.2.1	恶意代码的定义 .....	185
7.2.2	恶意代码攻击机制 .....	185
7.3	常见的恶意代码 .....	186
7.3.1	PE 病毒 .....	187
7.3.2	脚本病毒 .....	193
7.3.3	宏病毒 .....	195
7.3.4	浏览器恶意代码 .....	195
7.3.5	U 盘病毒 .....	197
7.3.6	网络蠕虫 .....	203
	小结 .....	205
	课后习题 .....	206

### 第 3 部分 网络防御技术

<b>第 8 章</b>	<b>操作系统安全基础 .....</b>	<b>211</b>
8.1	常用操作系统概述 .....	211
8.1.1	UNIX 操作系统 .....	211
8.1.2	Linux 操作系统 .....	212
8.1.3	Windows 操作系统 .....	213
8.2	安全操作系统的研究发展 .....	214
8.2.1	国外安全操作系统的发展 .....	214
8.2.2	国内安全操作系统的发展 .....	217
8.3	安全操作系统的基本概念 .....	218
8.3.1	主体和客体 .....	218
8.3.2	安全策略和安全模型 .....	218
8.3.3	访问监控器和安全内核 .....	218
8.3.4	可信计算基 .....	220
8.4	安全操作系统的机制 .....	220
8.4.1	硬件安全机制 .....	220
8.4.2	标识与鉴别 .....	221

8.4.3	访问控制 .....	221
8.4.4	最小特权管理 .....	222
8.4.5	可信通路 .....	222
8.4.6	安全审计 .....	223
8.5	代表性的安全模型 .....	223
8.5.1	安全模型的特点 .....	223
8.5.2	主要安全模型介绍 .....	223
8.6	操作系统安全体系结构 .....	225
8.6.1	安全体系结构的内容 .....	225
8.6.2	安全体系结构的类型 .....	226
8.6.3	Flask 安全体系结构 .....	226
8.6.4	权能体系结构 .....	227
8.7	操作系统安全配置方案 .....	227
8.7.1	安全配置方案初级篇 .....	227
8.7.2	安全配置方案中级篇 .....	230
8.7.3	安全配置方案高级篇 .....	235
	小结 .....	243
	课后习题 .....	243
<b>第 9 章</b>	<b>密码学与信息加密 .....</b>	<b>245</b>
9.1	密码学概述 .....	245
9.1.1	密码学的发展 .....	245
9.1.1	密码技术简介 .....	246
9.1.2	消息和加密 .....	246
9.1.3	鉴别、完整性和抗抵赖性 .....	247
9.1.4	算法和密钥 .....	247
9.1.5	对称算法 .....	248
9.1.6	公开密钥算法 .....	248
9.2	DES 对称加密技术 .....	248
9.2.1	DES 算法的历史 .....	249
9.2.2	DES 算法的安全性 .....	249
9.2.3	DES 算法的原理 .....	250
9.2.4	DES 算法的实现步骤 .....	250
9.2.5	DES 算法的程序实现 .....	254
9.3	RSA 公钥加密技术 .....	259
9.3.1	RSA 算法的原理 .....	259
9.3.2	RSA 算法的安全性 .....	260
9.3.3	RSA 算法的速度 .....	260
9.3.4	RSA 算法的程序实现 .....	260
9.4	PGP 加密技术 .....	264

9.4.1	PGP 简介 .....	264
9.4.2	PGP 加密软件 .....	264
9.5	数字信封和数字签名 .....	267
9.5.1	数字签名的原理 .....	267
9.5.2	数字签名的应用例子 .....	268
9.6	数字水印 .....	269
9.6.1	数字水印产生背景 .....	269
9.6.2	数字水印的嵌入方法 .....	270
9.7	公钥基础设施 PKI .....	271
9.7.1	PKI 的组成 .....	271
9.7.2	PKI 证书与密钥管理 .....	271
9.7.3	PKI 的信任模型 .....	272
	小结 .....	273
	课后习题 .....	273
<b>第 10 章</b>	<b>防火墙与入侵检测 .....</b>	<b>275</b>
10.1	防火墙的概念 .....	275
10.1.1	防火墙的功能 .....	276
10.1.2	防火墙的局限性 .....	276
10.2	防火墙的分类 .....	276
10.2.1	分组过滤防火墙 .....	277
10.2.2	应用代理防火墙 .....	283
10.3	常见防火墙系统模型 .....	284
10.3.1	筛选路由器模型 .....	284
10.3.2	单宿主堡垒主机模型 .....	284
10.3.3	双宿主堡垒主机模型 .....	285
10.3.4	屏蔽子网模型 .....	285
10.4	创建防火墙的步骤 .....	286
10.4.1	制定安全策略 .....	286
10.4.2	搭建安全体系结构 .....	286
10.4.3	制定规则次序 .....	287
10.4.4	落实规则集 .....	287
10.4.5	更换控制 .....	287
10.4.6	审计工作 .....	288
10.5	入侵检测系统的概念 .....	288
10.5.1	入侵检测系统面临的挑战 .....	288
10.5.2	入侵检测系统的类型和性能比较 .....	289
10.6	入侵检测的方法 .....	290
10.6.1	静态配置分析 .....	290
10.6.2	异常性检测方法 .....	290

10.6.3 基于行为的检测方法 .....	290
10.7 入侵检测的步骤 .....	295
10.7.1 信息收集 .....	295
10.7.2 数据分析 .....	295
10.7.3 响应 .....	296
小结 .....	300
课后习题 .....	300
<b>第 11 章 IP 安全与 Web 安全 .....</b>	<b>302</b>
11.1 IP 安全概述 .....	302
11.1.1 IP 安全的必要性 .....	302
11.1.2 IPSec 的实现方式 .....	303
11.1.3 IPSec 的实施 .....	304
11.1.4 验证头 AH .....	304
11.1.5 封装安全有效载荷 ESP .....	304
11.2 密钥交换协议 IKE .....	305
11.2.1 IKE 协议的组成 .....	305
11.2.2 ISAKMP 协议 .....	305
11.2.3 IKE 的两个阶段 .....	306
11.3 VPN 技术 .....	307
11.3.1 VPN 的功能 .....	307
11.3.2 VPN 的解决方案 .....	307
11.4 Web 安全概述 .....	308
11.4.1 网络层安全性 .....	308
11.4.2 传输层安全性 .....	308
11.4.3 应用层安全性 .....	309
11.5 SSL/TLS 技术 .....	309
11.5.1 SSL/TLS 的发展过程 .....	309
11.5.2 SSL 体系结构 .....	310
11.5.3 SSL 的会话与连接 .....	310
11.5.4 OpenSSL 概述 .....	311
11.6 安全电子交易 SET 简介 .....	311
小结 .....	311
课后习题 .....	311

## 第 4 部分 网络安全综合解决方案

<b>第 12 章 网络安全方案设计 .....</b>	<b>315</b>
12.1 网络安全方案概念 .....	315
12.1.1 网络安全方案设计的注意点 .....	315
12.1.2 评价网络安全方案的质量 .....	316



12.2	网络安全方案的框架 .....	316
12.3	网络安全案例需求 .....	318
12.3.1	项目要求 .....	319
12.3.2	工作任务 .....	319
12.4	解决方案设计 .....	320
12.4.1	公司背景简介 .....	320
12.4.2	安全风险分析 .....	321
12.4.3	解决方案 .....	321
12.4.4	实施方案 .....	322
12.4.5	技术支持 .....	322
12.4.6	产品报价 .....	323
12.4.7	产品介绍 .....	323
12.4.8	第三方检测报告 .....	323
12.4.9	安全技术培训 .....	323
小结	.....	325
课后习题	.....	325
附录 A	部分习题参考答案 .....	326
参考文献	.....	330

# 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）

