

全国信息技术人才培养工程指定培训教材  
网络信息安全工程师高级职业教育系列教程

# 计算机网络信息安全 理论与实践教程

信息产业部电子教育与考试中心 组编  
蒋建春 文伟平 杨凡 郑生琳 编著



北京邮电大学出版社  
[www.buptpress.com](http://www.buptpress.com)

TP393.08/262

2008

全国信息技术人才培养工程指定培训教材  
网络信息安全工程师高级职业教育系列教程

# 计算机网络信息安全 理论与实践教程

信息产业部电子教育与考试中心 组编  
蒋建春 文伟平 杨凡 郑生琳 编著

ISBN 978-7-5623-1289-9

编 著：蒋建春 文伟平 杨凡 郑生琳  
责任编辑：陈 颖  
出版发行：北京邮电大学出版社  
地 址：北京市海淀区学院路10号(100876)  
发 行 部：电话：010-62282182 传真：010-62282178  
E-mail: publisher@bupt.edu.cn  
经 销：各地新华书店  
印 刷：北京忠信印刷厂  
开 本：787 mm×1 092 mm 1/16  
印 张：23.25  
字 数：726千字  
印 数：1-2 000册  
版 次：2008年5月第1版

元 00.82, 01 5

北京邮电大学出版社

·北京·

## 内 容 简 介

本书是“网络信息安全工程师高级职业教育”项目的培训教程。本书参考和借鉴了广大网络信息安全人员的最新研究成果,结合了网络信息安全实践经验,系统归纳总结了网络信息安全职业人员所需知识和技能,并给出典型案例和信息安全实践指导。本书主要内容包括:网络信息安全概况、互联网协议安全、网络攻击原理与常用方法、Windows 系统安全、Unix/Linux 操作系统安全、恶意代码分析技术与防护、防火墙原理和应用、网站安全、邮件服务器安全、电子邮箱安全、FTP 服务器安全、数据库安全、浏览器安全、安全工具软件应用等。

本书还包括练习题以及相应的网络信息安全实验部分。读者通过该书,能够快速地掌握职业所需要的知识和技能。本书也可以作为从事网络信息安全的广大技术人员和大专院校师生的参考用书。

### 图书在版编目(CIP)数据

计算机网络信息安全理论与实践教程/蒋建春等编著. —北京:北京邮电大学出版社,2008  
ISBN 978-7-5635-1589-9

I. 计… II. 蒋… III. 计算机网络—安全技术—水平考试—教材 IV. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 060499 号

---

书 名: 计算机网络信息安全理论与实践教程

编 著: 蒋建春 文伟平 杨 凡 郑生琳

责任编辑: 陈 瑶

出版发行: 北京邮电大学出版社

社 址: 北京市海淀区西土城路 10 号(100876)

发 行 部: 电话:010-62282185 传真:010-62283578

E-mail: publish@bupt.edu.cn

经 销: 各地新华书店

印 刷: 北京忠信诚胶印厂

开 本: 787 mm×1 092 mm 1/16

印 张: 29.25

字 数: 726 千字

印 数: 1—5 000 册

版 次: 2008 年 5 月第 1 版 2008 年 5 月第 1 次印刷

---

ISBN 978-7-5635-1589-9

定 价: 58.00 元

· 如有印装质量问题,请与北京邮电大学出版社发行部联系 ·

## 序

随着信息技术在经济社会各领域不断深化的应用,信息技术对生产力以至于人类文明发展的巨大作用越来越明显。党的“十七大”提出要“全面认识工业化、信息化、城镇化、市场化、国际化深入发展的新形势新任务”,“发展现代产业体系,大力推进信息化与工业化融合”,明确了信息化的发展趋势,首次鲜明地提出了信息化与工业化融合发展的崭新命题,赋予了我国信息化全新的历史使命。近年来,日新月异的信息技术呈现出新的发展趋势,信息技术与其他技术的结合更加紧密,信息技术应用的深度、广度和专业化程度不断提高。信息技术人才在综合国力竞争中越来越占有重要地位。

为了抓住机遇,迎接挑战,实施人才强国战略,信息产业部启动了“全国信息技术人才培养工程”。该项工程旨在通过政府政策引导,充分发挥全行业和社会教育培训资源的作用,建立规范的信息技术教育培训体系、科学的培训课程体系、严谨的信息技术人才评测服务体系,培养造就大批行业急需的、结构合理的高素质信息技术应用型人才,以促进信息产业持续快速协调健康发展。

全国信息技术水平考试是根据信息产业部有关规定组织并委托信息产业部全国电子信息应用教育中心负责具体实施的全国统一考试,是全国信息技术人才培养工程的重要组成部分,该考试坚持客观公正、中立权威、走国际化道路,以严格的认证质量赢得社会认可。

为了配合全国信息技术水平考试,由各方专家依据信息产业对技术人才素质与能力的需求,在充分吸取国内外先进信息技术培训课程优点的基础上,信息产业部全国电子信息应用教育中心精心组织编写了全国信息技术水平考试用书。这些教材注重提升信息技术人才分析问题和解决问题的能力,对各层次信息技术人才的培养工作具有现实的指导意义。

信息产业部全国电子信息应用教育中心

## 前 言

随着互联网的发展和信息技术的普及,网络和信息技术已经渗入到日常生活和工作当中,社会信息化和信息网络化,突破了应用信息在时间和空间上的障碍,使信息的价值不断提高。但是与此同时,网页篡改、计算机病毒、系统非法入侵、数据泄密、网站欺骗、服务瘫痪、漏洞非法利用等信息安全事件时有发生。目前,许多企事业单位的业务依赖于信息系统安全运行,信息安全重要性日益凸显。信息安全已成为影响国家安全、经济发展、社会稳定、公民利益的重要问题。

面对国家和社会的需求,信息产业部电子教育与考试中心推出了“网络信息安全工程师高级职业教育项目。其目标就是培养“德才兼备、攻防兼备”的信息安全工程师,能够在各级行政、企事业单位、网络公司、信息中心、互联网接入单位中从事信息安全服务、运维、管理工作。

全书共分二十一章及实验篇,主要内容包括:网络信息安全概况、互联网协议安全、网络攻击原理与常用方法、Windows 系统安全、Unix/Linux 操作系统安全、恶意代码原理、计算机病毒技术分析与安全防护、特洛伊木马技术分析与安全防护、网络蠕虫技术分析与安全防护、防火墙原理和应用、iptables 防火墙、Apache 服务安全、IIS 安全、邮件服务器安全、电子邮箱安全、FTP 服务器安全、数据库安全、浏览器安全、Ghost 软件、安全通信工具软件、网络安全监测分析工具。

本书是作者在网络信息安全职业教育领域工作中的尝试,编写时力求突出职业教育特点。由于作者水平有限,书中如果有不当之处,希望广大读者不吝赐教。

作者

2008 年 3 月

# 目 录

9	1.0	网络安全现状与问题	3
9	1.0.1	网络安全现状	3
10	1.0.2	典型安全问题	4
11	1.0.3	网络信息安全目标	5
13	1.1	网络信息安全基本功能	5
14	1.1.1	网络安全防御	6
14	1.1.2	网络安全监测	6
14	1.1.3	网络安全应急	6
14	1.1.4	网络安全恢复	6
15	1.2	网络信息安全基本技术	6
15	1.2.1	网络物理安全	6
15	1.2.2	网络认证	6
15	1.2.3	网络访问控制	6
15	1.2.4	网络安全保密	7
15	1.2.5	网络安全监测	7
15	1.2.6	网络漏洞评估	7
15	1.2.7	恶意代码防护	7
15	1.2.8	应急响应	7
15	1.2.9	网络安全体系	8
15	1.3	网络信息安全威胁分析	8
15	1.3.1	网络信息安全威胁来源	8
15	1.3.2	网络信息安全威胁对象	8

## 第一篇 网络信息安全基础篇

### 第1章 绪论

18	1.1	网络安全现状与问题	3
19	1.1.1	网络安全现状	3
19	1.1.2	典型安全问题	4
20	1.2	网络信息安全目标	5
20	1.2.1	机密性	5
21	1.2.2	完整性	5
21	1.2.3	可用性	5
22	1.2.4	抗抵赖性	5
23	1.2.5	可控性	5
24	1.3	网络信息安全基本功能	5
24	1.3.1	网络安全防御	6
25	1.3.2	网络安全监测	6
26	1.3.3	网络安全应急	6
26	1.3.4	网络安全恢复	6
26	1.4	网络信息安全基本技术	6
26	1.4.1	网络物理安全	6
28	1.4.2	网络认证	6
28	1.4.3	网络访问控制	6
28	1.4.4	网络安全保密	7
28	1.4.5	网络安全监测	7
29	1.4.6	网络漏洞评估	7
30	1.4.7	恶意代码防护	7
31	1.4.8	应急响应	7
31	1.4.9	网络安全体系	8
32	1.5	网络信息安全威胁分析	8
32	1.5.1	网络信息安全威胁来源	8
32	1.5.2	网络信息安全威胁对象	8

1.6	网络安全管理概念、方法与流程	9
1.6.1	网络安全管理定义	9
1.6.2	网络安全管理基本方法	10
1.6.3	网络安全管理基本流程	11
1.7	网络信息安全漏洞网站	12
	本章小结	14
	本章练习	14
<b>第2章 互联网协议安全</b>		
2.1	引言	15
2.2	TCP/IP 协议	15
2.2.1	TCP/IP 协议结构	15
2.2.2	IP 协议	17
2.2.3	TCP 协议	18
2.2.4	UDP 协议	19
2.2.5	ICMP 协议	19
2.3	TCP/IP 协议安全分析	20
2.3.1	以太网协议安全	20
2.3.2	ARP 协议安全	21
2.3.3	IP 协议安全	21
2.3.4	ICMP 协议	22
2.3.5	IP 分组、重组算法安全	23
2.3.6	RIP 协议安全	24
2.3.7	TCP 协议安全	24
2.3.8	SYN Flood 攻击	25
2.3.9	UDP 安全	26
2.3.10	应用层安全	26
	本章小结	26
	本章练习	26
<b>第3章 网络攻击原理与常用方法</b>		
3.1	网络攻击概述	28
3.1.1	网络攻击概念	28
3.1.2	网络攻击技术发展演变	29
3.2	网络攻击一般过程	30
3.2.1	隐藏攻击源	31
3.2.2	收集攻击目标信息	31
3.2.3	挖掘漏洞信息	32
3.2.4	获取目标访问权限	32
3.2.5	隐蔽攻击行为	33

3.2.6	实施攻击	33
3.2.7	开辟后门	33
3.2.8	清除攻击痕迹	34
3.3	网络攻击常见技术方法	34
3.3.1	端口扫描	34
3.3.2	口令破解	35
3.3.3	缓冲区溢出	36
3.3.4	网络蠕虫	37
3.3.5	网站假冒	37
3.3.6	拒绝服务	37
3.3.7	网络嗅探	38
3.3.8	SQL 注入攻击	39
3.3.9	社交工程方法(Social Engineering)	40
3.3.10	电子监听技术	40
3.3.11	会话劫持	40
3.3.12	漏洞扫描	40
3.3.13	代理技术	40
3.3.14	数据加密技术	41
3.4	黑客常用软件	41
3.4.1	扫描类软件	41
3.4.2	远程监控类软件	41
3.4.3	系统攻击和密码破解	42
3.4.4	监听类软件	43
3.5	网络攻击案例	43
3.5.1	Nmap 扫描	43
3.5.2	DDoS 攻击	46
3.5.3	W33.Blaster.Worm	46
3.5.4	网络嗅探攻击	47
	本章小结	49
	本章练习	49

## 第二篇 Windows 及 Unix 系统安全篇

### 第 4 章 Windows 系统安全

4.1	Windows 系统安全概况	53
4.1.1	Windows 系统架构	53
4.1.2	Windows 安全模型	54
4.1.3	Windows 安全机制	55
4.2	Windows 系统安全分析	56



4.3	Windows 系统安全增强技术方法与流程	57
4.3.1	Windows 系统安全增强方法概述	57
4.3.2	Windows 系统安全增强基本流程	57
4.4	Windows 2000 系统安全最佳实践	59
4.4.1	系统启动安全增强	59
4.4.2	账号与口令管理安全增强	59
4.4.3	安装最新系统补丁	61
4.4.4	网络安全增强	61
4.4.5	增强 TCP/IP 协议栈抗拒绝服务能力	63
4.4.6	安装第三方防护软件	63
4.5	Windows 系统常见漏洞与解决方法	64
4.5.1	Unicode 漏洞	64
4.5.2	ISAPI 缓冲区扩展溢出	64
4.5.3	IIS RDS(Remote Data Services)	65
4.5.4	NetBIOS	65
4.5.5	空对话连接造成的信息泄露	65
4.5.6	SAM 中的弱散列(LAN Manager hash)	66
4.5.7	RPC 漏洞	67
	本章小结	67
	本章练习	68
<b>第 5 章 Unix/Linux 操作系统安全</b>		
5.1	Unix/Linux 系统安全概况	69
5.1.1	Unix/Linux 系统架构	69
5.1.2	Unix/Linux 安全机制	70
5.2	Unix/Linux 系统安全隐患	71
5.3	Unix/Linux 系统安全增强方法和流程	73
5.3.1	Unix/Linux 系统安全增强方法	73
5.3.2	Unix/Linux 系统安全增强基本流程	73
5.4	Unix/Linux 系统安全增强技术	74
5.4.1	安装系统补丁软件包	74
5.4.2	最小化系统网络服务	74
5.4.3	设置系统开机保护口令	75
5.4.4	弱口令检查	75
5.4.5	禁用默认账号	76
5.4.6	用 SSH 增强网络服务安全	77
5.4.7	利用 tcp_wrapper 增强访问控制	77
5.4.8	构筑 Unix/Linux 主机防火墙	77
5.4.9	使用 Tripwire 或 md5sum 完整性检测工具	77
5.4.10	检测 LKM 后门	77

5.4.11	系统安全监测	78
5.5	Linux 安全增强实例	78
5.5.1	禁止访问重要文件	78
5.5.2	禁止不必要的 SUID 程序	78
5.5.3	为 LILO 增加开机口令	78
5.5.4	设置口令最小长度和最短使用时间	79
5.5.5	限制远程访问	79
5.5.6	用户超时注销	79
5.5.7	注销时删除命令记录	80
5.6	Unix/Linux 系统常见漏洞与解决方法	80
5.6.1	空口令或弱口令的账号	80
5.6.2	R 命令	80
5.6.3	RPC 服务缓冲区溢出	81
5.6.4	缺省 SNMP 字符串	81
5.6.5	Sendmail	82
5.6.6	LPD(Remote Print Protocol Daemon)	82
5.6.7	Sadmind and Moundd	83
	本章小结	83
	本章练习	84

### 第三篇 恶意代码防护篇

#### 第 6 章 恶意代码原理

6.1	恶意代码概述	87
6.1.1	恶意代码定义	87
6.1.2	恶意代码分类	88
6.2	计算机病毒	89
6.2.1	计算机病毒概念	89
6.2.2	计算机病毒特性	89
6.2.3	计算机病毒运行机制	90
6.3	特洛伊木马	91
6.3.1	特洛伊木马概念	91
6.3.2	特洛伊木马分类	91
6.3.3	特洛伊木马运行机制	91
6.4	网络蠕虫	92
6.4.1	网络蠕虫概念与特性	92
6.4.2	网络蠕虫运行机制	92
6.5	其他恶意代码	94
6.6	恶意代码防范总体框架	95

87	· 本章小结 .....	96
87	· 本章练习 .....	96
<b>第7章 计算机病毒技术与安全防护</b>		
87	7.1 计算机病毒技术分析 .....	97
87	7.1.1 引导型病毒 .....	97
87	7.1.2 宏病毒 .....	97
87	7.1.3 多态病毒 .....	98
87	7.1.4 隐蔽病毒 .....	99
80	7.2 计算机病毒防范技术与防病毒产品 .....	99
80	7.2.1 计算机病毒检测 .....	99
80	7.2.2 计算机病毒安全管理 .....	99
81	7.2.3 计算机病毒应急响应 .....	100
81	7.2.4 防病毒产品典型技术 .....	100
83	7.2.5 防病毒技术发展趋势 .....	101
83	7.3 计算机病毒防护典型模式 .....	103
83	7.3.1 基于单机病毒防护 .....	103
83	7.3.2 基于网络病毒防护 .....	103
84	7.3.3 基于网络分级病毒防护 .....	103
84	7.3.4 基于邮件网关病毒防护 .....	104
84	7.3.5 基于网关级防护 .....	104
84	7.4 企业防毒典型需求与选购标准 .....	105
84	7.4.1 企业网中病毒传播分析 .....	105
84	7.4.2 企业网中防毒典型需求 .....	106
84	7.4.3 企业网中防毒系统部署特点 .....	108
84	7.4.4 企业网中防毒系统考虑因素 .....	108
84	7.4.5 防毒产品选购标准 .....	109
84	7.5 主流防毒产品选介 .....	111
84	7.5.1 江民 .....	111
84	7.5.2 瑞星 .....	112
84	7.5.3 金山毒霸 .....	114
84	7.5.4 北信源 .....	114
84	7.5.5 其他 .....	116
84	· 本章小结 .....	116
84	· 本章练习 .....	116
<b>第8章 特洛伊木马技术与安全防护</b>		
84	8.1 特洛伊木马技术分析 .....	118
84	8.1.1 特洛伊木马植入技术 .....	118
84	8.1.2 特洛伊木马隐藏技术 .....	119

137	8.1.3	特洛伊木马存活性技术	120
137	8.1.4	特洛伊木马自启动技术	120
137	8.2	特洛伊木马防护策略与防护模式	120
138	8.2.1	特洛伊木马防护策略	120
138	8.2.2	特洛伊木马防护模式	122
138	8.3	特洛伊木马安全防护主要技术	122
138	8.3.1	网络端口检查	122
138	8.3.2	可疑系统文件检查	122
138	8.3.3	系统注册表检查	122
140	8.3.4	隐蔽型木马检测	123
140	8.3.5	网络流量监控	124
140	8.3.6	防止木马植入	124
141	8.3.7	木马通信拦截	124
142	8.3.8	木马清除	124
143	8.4	特洛伊木马查杀典型安全工具	125
143	8.5	典型特洛伊木马	126
143	8.5.1	冰河	126
	8.5.2	广外女生	126
	8.5.3	网络精灵	127
	8.5.4	SubSeven	127
	8.5.5	黑洞 2001	128
143	8.5.6	火凤凰	129
143	8.5.7	Sweet Heart	129
143	8.5.8	网络神偷	129
143	8.5.9	网络公牛	130
143	8.5.10	聪明基因	131
143		本章小结	132
143		本章练习	132
	<b>第9章</b>	<b>网络蠕虫技术分析与安全防护</b>	
156	9.1	网络蠕虫常用技术分析	133
156	9.1.1	网络蠕虫扫描	133
157	9.1.2	网络蠕虫漏洞挖掘	134
158	9.2	网络蠕虫防护策略与防护模式	135
158	9.2.1	网络蠕虫防护策略	135
158	9.2.2	网络蠕虫防护模式	135
158	9.3	网络蠕虫防范技术	136
159	9.3.1	网络蠕虫监测与预警	136
159	9.3.2	网络蠕虫传播抑制	136
159	9.3.3	模仿生物疾病防范网络蠕虫	137

9.3.4	网络系统漏洞检测与系统加固	137
9.3.5	网络蠕虫免疫	137
9.3.6	网络蠕虫阻断与隔离	137
9.3.7	网络蠕虫清除	138
9.4	网络蠕虫典型安全产品或工具	138
9.4.1	网络流量监测	138
9.4.2	补丁管理系统	139
9.4.3	安全网关	139
9.4.4	入侵检测	139
9.4.5	网络蠕虫专杀工具	140
9.5	典型网络蠕虫	140
9.5.1	红色代码	140
9.5.2	MSBlast. Remove. Worm/W32	141
9.5.3	SQL Slammer	142
9.5.4	MSN 肉鸡	143
	本章小结	145
	本章练习	145

## 第四篇 防火墙篇

### 第 10 章 防火墙原理和应用

10.1	防火墙工作机制与用途	149
10.1.1	防火墙概念	149
10.1.2	防火墙原理	150
10.2	防火墙核心技术与分类	151
10.2.1	包过滤	151
10.2.2	服务代理	153
10.2.3	网络地址转换	155
10.3	防火墙防御体系结构类型	156
10.3.1	基于双宿主主机防火墙结构	156
10.3.2	基于代理型防火墙结构	156
10.3.3	基于屏蔽子网的防火墙结构	157
10.4	防火墙主要技术参数	158
10.4.1	防火墙功能指标	158
10.4.2	防火墙性能指标	158
10.4.3	防火墙安全指标	158
10.5	防火墙产品类型、局限性与发展	159
10.5.1	防火墙产品分类	159
10.5.2	防火墙商业产品	159

10.5.3	开源代码防火墙	160
10.5.4	防火墙的局限性	160
10.5.5	防火墙产品发展趋势	160
10.6	防火墙部署过程与典型应用模式	161
10.6.1	防火墙部署基本方法与步骤	161
10.6.2	防火墙典型部署模式	161
	本章小结	163
	本章练习	163
<b>第 11 章 Linux 防火墙</b>		
11.1	iptables 概述	164
11.1.1	iptables 的发展	164
11.1.2	iptables 工作原理	164
11.2	iptables 语法与典型用法	166
11.3	iptables 典型配置案例	169
11.3.1	基本配置初始模板	169
11.3.2	网络服务安全保护配置	169
11.3.3	常见攻击阻断配置	169
11.4	iptables 综合应用实例	170
11.4.1	实例网络环境说明	170
11.4.2	iptables 配置实现过程	170
11.4.3	iptables 配置文件	172
	本章小结	172
	本章练习	173
<b>第五篇 网站服务安全篇</b>		
<b>第 12 章 Apache 服务安全</b>		
12.1	Apache 概述	177
12.1.1	Apache 基本安装	177
12.1.2	Apache 基本配置	179
12.1.3	Apache 安全分析	180
12.2	Apache 安全机制与配置	181
12.2.1	本地文件安全	181
12.2.2	Apache 模块管理机制	181
12.2.3	Apache 认证机制	181
12.2.4	连接耗尽应对机制	182
12.2.5	多线程下载保护机制	183
12.2.6	Apache 自带的访问机制	183
12.2.7	Apache 审计和日志	183

12.2.8	CGI 和 SSI 风险缓解机制	183
12.2.9	Apache 服务器防范 DoS	184
12.3	Apache 安全最佳实践	184
12.3.1	及时安装 Apache Web 补丁	184
12.3.2	Apache 服务器密码保护	185
12.3.3	为 Apache 使用专门的用户和组	185
12.3.4	隐藏 Apache 的版本号	185
12.3.5	Apache Web 目录访问策略	186
12.3.6	Apache 文件目录保护	186
12.3.7	删除 Apache 默认目录或不必要的文件	187
12.4	Apache 安全增强软件与工具	187
12.4.1	Apache 服务器“安全沙箱”	187
12.4.2	使用 SSL 增强 Apache 安全通信	187
12.4.3	其他	187
12.5	Apache 已知漏洞以及修补方法	188
	本章练习	190

## 第 13 章 IIS 安全

13.1	IIS 安全概述	191
13.1.1	IIS 安全威胁分析	191
13.1.2	网站攻击级别	191
13.2	IIS 安全机制	192
13.2.1	IIS 文件保护	192
13.2.2	IIS 匿名访问机制	193
13.2.3	IIS 认证机制	194
13.2.4	IP 地址和域名访问控制	195
13.2.5	IIS 访问控制综合机制	196
13.2.6	IIS 日志	197
13.2.7	IIS 性能优化调整	198
13.3	IIS 安全工具	199
13.3.1	IIS 权限管理工具	199
13.3.2	IIS Lockdown	202
13.3.3	URLScan	207
	本章小结	209
	本章练习	210

## 第六篇 邮件安全篇

### 第 14 章 邮件服务器安全

14.1	概述	213
14.1.1	电子邮件概念	213

14.1.2	电子邮件系统组成	213
14.1.3	电子邮件协议	215
14.1.4	典型邮件系统	215
14.2	电子邮件安全	216
14.2.1	邮件典型安全需求	216
14.2.2	邮件服务 QoS 指标	217
14.2.3	邮件安全隐患	217
14.2.4	邮件安全威胁	218
14.3	电子邮件服务安全机制	219
14.3.1	邮件服务认证机制	219
14.3.2	邮件服务访问控制机制	219
14.3.3	邮件服务日志审计机制	219
14.3.4	邮件过滤机制	219
14.3.5	垃圾邮件行为识别机制	220
14.3.6	其他	221
14.4	电子邮件服务安全最佳实践	221
14.4.1	SMTP 用户认证	221
14.4.2	关闭 Open Relay	221
14.4.3	实时黑名单过滤	221
14.4.4	关闭 SMTP 的“EXPN”和“VRFY”功能	222
14.4.5	安装补丁软件包	222
14.4.6	邮件服务器的反向域名解析功能	222
14.5	电子邮件服务安全工具和典型产品	222
14.5.1	邮件服务安全工具	222
14.5.2	典型邮件安全产品	223
	本章小结	225
	本章练习	225
<b>第 15 章 电子邮箱安全</b>		
15.1	电子邮箱概述	226
15.1.1	电子邮箱概念	226
15.1.2	常用电子邮箱类型	226
15.2	电子邮件安全分析	227
15.2.1	邮箱口令被窃取	227
15.2.2	邮件内容被截获	227
15.2.3	邮件附件病毒	227
15.2.4	邮箱炸弹攻击	227
15.2.5	邮箱口令破解	228
15.2.6	邮件软件缺陷	228
15.3	电子邮件安全防护	229



15.3.1	邮件客户端软件应用限制	229
15.3.2	邮箱密码安全	229
15.3.3	电子邮件加密	229
15.3.4	邮件病毒防护	237
15.3.5	邮箱炸弹防护	239
15.4	垃圾邮件过滤	239
15.4.1	邮件客户端过滤机制	239
15.4.2	基于内容垃圾邮件过滤	239
15.4.3	基于安全列表的垃圾邮件过滤	240
15.5	电子邮件备份	241
15.5.1	邮件备份	241
15.5.2	Foxmail	241
15.5.3	Outlook Express	243
	本章小结	246
	本章练习	246
<b>第七篇 文件服务安全篇</b>		
<b>第 16 章 FTP 服务器安全</b>		
16.1	FTP 概述	249
16.1.1	FTP 工作机制	249
16.1.2	FTP 安全脆弱性分析	250
16.2	FTP 服务器典型安全机制分析	251
16.2.1	FTP 服务文件安全	251
16.2.2	FTP 服务认证机制	251
16.2.3	FTP 服务访问控制机制	251
16.2.4	FTP 服务日志审计机制	251
16.3	wu-ftpd 服务器安全配置	251
16.3.1	wu-ftpd 服务器简况	251
16.3.2	最佳安全配置实践	252
16.4	Proftpd 服务器安全配置	256
16.4.1	Proftpd 服务器简况	256
16.4.2	最佳安全配置实践	256
16.5	Vsftpd 服务器安全配置	257
16.5.1	Vsftpd 服务器简况	257
16.5.2	最佳安全配置实践	258
16.6	FTP Serv-U 安全配置	259
16.6.1	FTP Serv-U 服务器简况	259
16.6.2	最佳安全配置实践	259