21世纪复旦大学研究生教学用书

Network Security Principle and Application

网络安全原理与应用

张世永　主编

科学出版社
www.sciencep.com

21世纪复旦大学研究生教学用书

网络安全原理与应用

张世永　主编

科学出版社

北京

内 容 简 介

本书为复旦大学研究生教学用书，书中全面介绍网络信息安全的基本原理和实践技术。在第一部分“网络安全概述”中先简介 TCP/IP 协议，然后分析目前常见的各种安全威胁，指出问题根源，提出网络安全的任务；第二部分“安全框架与评估标准”介绍一些经典的网络安全体系结构，并介绍了国际和国内对网络安全的评估标准和有关法规；第三部分“密码学理论”着重介绍密码学，从传统密码技术到对称密码体制、公钥密码体制以及密钥分配与管理、数字签名、数据隐写与电子水印等；第四部分为“安全技术和产品”，全面介绍身份认证、授权与访问控制、PKI/PMI、IP 安全、E-mail 安全、Web 与电子商务安全、防火墙、VPN、安全扫描、入侵检测与安全审计、网络病毒防范、系统增强、安全应急响应、网络信息过滤、网络安全管理等技术，内容基本涵盖目前主要的安全技术。在每章后面给出了习题作为巩固知识之用，还给出了大量的参考文献。

本书可作为高等院校计算机、通信、信息等专业研究生和高年级本科生的教材，也可作为计算机、通信、信息等领域研究人员和专业技术人员的参考书。

图书在版编目(CIP)数据

网络安全原理与应用/张世永主编. —北京：科学出版社，2003
(21 世纪复旦大学研究生教学用书)
ISBN 7-03-011450-7

Ⅰ. 网… Ⅱ. 张… Ⅲ. 计算机网络-安全技术-研究生-教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2003)第 033039 号

策划编辑：鞠丽娜 /责任编辑：韩 洁
责任印制：吕春珉 /封面设计：王 浩

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2003 年 5 月第 一 版 开本：787×1092 1/16
2003 年 5 月第一次印刷 印张：27 1/2
印数：1—4 000 字数：620 000
定价：42.00 元
(如有印装质量问题，我社负责调换〈双青〉)

序　言

信息化和网络化是当今世界经济和社会发展的大趋势，也是推进我国国民经济和社会现代化的关键环节。计算机技术和网络技术已深入到社会的各个领域，人类社会各种活动对计算机网络的依赖程度已经越来越大。与此同时，由于计算机网络所具有的开放性和共享性，其安全性也成为人们日益关切的问题。在世界范围内，对计算机网络的攻击手段层出不穷，网络犯罪日趋严重，给各行各业带来了巨大的经济和其他方面损失。我国信息化、网络化建设在技术与装备上对别国的极大依赖性，使网络安全问题尤为突出。因此，增强全社会安全意识，普及计算机网络安全教育，提高计算机网络安全技术水平，促进计算机网络安全的自主研发创新，改善计算机网络的安全现状，成为当务之急。

张世永教授主编的《网络安全原理与应用》一书，正是顺应了这样的要求，它具有科学、严谨的体系结构，全面而系统地阐述了计算机网络安全领域的有关概念、原理、框架、技术，特别是花了足够的篇幅来介绍目前网络安全的各种实际应用技术问题。本书从网络安全概论、网络安全体系结构、国内外网络安全评估标准、密码学知识到各种实用网络安全技术和产品，做了全面深入的讨论，基本涵盖了目前主要的安全技术，所涉及到的内容反映了网络安全领域的最新研究成果和新趋势，并融进了作者近年来在该领域的实践经验与科研成果。

总之，这是一本理论与技术相结合，涉及广泛，新颖而全面，内容深入浅出且引人入胜的好书。它对于有关计算机、通信、信息等专业领域的广大研究生及高年级大学生均为一本值得推荐的教材和参考书。同时对于网络安全领域的研究工作者，对于网络工程师，通信工程师，计算机软、硬件工程师等，也是一本有价值的参考书。

前　言

随着信息化的普及和发展，互联网络已覆盖了社会政治、经济、文化、生产的各个领域，网络安全也越来越成为全社会关注的焦点，并成为网络发展的重要课题。提高全社会网络安全意识，是保障我国信息化建设健康稳定发展的长期重点工作之一。

从20世纪90年代以来，我们在网络信息安全领域开展了广泛而卓有成效的科研工作，取得了一定的成果，荣获了数十项重大成果，包括国家科技进步二等奖、三等奖各1项，部委科技进步一等奖、二等奖各2项，上海市科技进步二等奖4项、三等奖8项，国家计委重大科技成果奖3项，机电部重大科的实践经验与科研成果的一点总结。我们的目标是为网络信息安全领域提供一本既可作教科书，又可作专业人员全面参考的手册书籍。

本书为21世纪复旦大学研究生教学用书，属于上海市学位委员会研究生学位课程教材建设项目，在本书的写作过程中，除了介绍了作者自身的大量研究内容及成果之外，还参考了众多国内外论文、书籍以及其他一些在互联网上公布的相关资料，我们尽量在每章后面都列出，但由于网上资料数量众多且杂乱，可能无法把所有文献都一一注明出处。这些资料来源于众多的大学、研究机构、安全团体、安全网站、商业公司以及一些研究计算机及网络安全问题的个人，对于他们在推动安全事业发展的过程中所做的工作和努力，再次表示衷心的感谢。写作过程中所参考的这些书籍资料，其原文版权属于原作者，特此声明。

本书具有科学严谨的体系结构，内容深入浅出，新颖而全面，涉及广泛，全书在结构上分为网络安全概述、安全框架与评估标准、密码学理论、安全技术和产品四大部分，全面介绍网络信息安全的基本原理和应用实践技术，基本遍及了网络信息安全的各个方面，侧重于基本原理和实践技术，特别是较为系统全面的给出了目前网络信息安全的各种技术，反映了网络信息安全领域的最新研究成果和新趋势，并融进作者近年来在该领域的实践经验与科研成果。此外从教材使用的角度考虑，在每章后面给了习题作为巩固知识之用，书中还给出了大量的参考文献。作为“21世纪复旦大学研究生教学用书”之一，本教材是本为提高研究生的培养质量，把创新能力和创新精神的培养放到突出位置上并适应新的教学和科研要求的有复旦特色的教材。

全书由复旦大学网络与信息工程中心、复旦光华信息科技股份有限公司合作组织编写，第1、15、16、17章由李晓明编写，第2、3、11、13、23、25章由顾国飞编写，第4章由傅维明编写，第5、6、7、章由杨明、候亚飞编写，第8、9、10章由王国平编写，第12、14章由李松年编写，第18、19章由钟亦萍编写，第20、21、26章由吴承荣、顾国飞编写，第22章由廖志成编写，第24章由刘松鹏编写；全书由张世永教授统稿，顾国飞协助。刘鹏、钟洪涛、吴胜浩、王五平、周建华、迟瑞峥等研究生参与了部分资料的收集、整理、录入和校订工作。此外，本书得到了中国工程院院士何德全教授德的大力支持和指导，并为本书欣然作序；上海计算机软件技术开发中心主任朱三元教授在百忙之中审阅全稿，提出了宝贵的意见，在

此一并表示衷心的感谢。

网络与信息安全是一门内容广泛、发展迅速的学科，本书是在此领域内的一次努力尝试，囿于作者的学识和水平，尽管尽了最大努力，但仍难免存在不足之处，诚望读者不吝赐教斧正，以利再版修订。

作　者

2003 年 4 月

目　录

第一部分　网络安全概述

第 1 章　TCP /IP 概述 …… 3
1.1　Internet 起源、现状及未来 …… 3
1.1.1　Internet 的起源和现状 …… 3
1.1.2　Internet 的发展方向 …… 4
1.2　TCP/IP 协议体系 …… 6
1.3　IP 协议和 TCP 协议 …… 7
1.3.1　IP 协议 …… 7
1.3.2　IP 地址 …… 9
1.3.3　TCP 协议和 UDP 协议 …… 10
1.4　其他应用协议简介 …… 14
1.4.1　ARP 协议和 RARP 协议 …… 14
1.4.2　ICMP 协议 …… 14
1.4.3　网关路由选择协议 …… 14
1.5　小结 …… 16
习题 …… 16
参考文献 …… 16
第 2 章　安全问题概述 …… 17
2.1　常见的安全威胁与攻击 …… 17
2.1.1　窃取机密攻击 …… 17
2.1.2　非法访问 …… 18
2.1.3　恶意攻击 …… 19
2.1.4　社交工程 …… 22
2.1.5　计算机病毒 …… 22
2.1.6　不良信息资源 …… 22
2.1.7　信息战 …… 22
2.2　安全问题根源 …… 23
2.2.1　物理安全问题 …… 23
2.2.2　方案设计的缺陷 …… 24
2.2.3　系统的安全漏洞 …… 24
2.2.4　TCP/IP 协议的安全问题 …… 25
2.2.5　人的因素 …… 25

2.3 网络信息安全的内涵 …… 26
2.3.1 网络信息安全的要素 …… 26
2.3.2 可存活性简介 …… 27
2.3.3 网络安全的实质 …… 27
2.4 小结 …… 28
习题 …… 28
参考文献 …… 29

第二部分 安全框架与评估标准

第3章 安全体系结构与模型 …… 33
3.1 ISO/OSI 安全体系结构 …… 33
3.2 动态的自适应网络安全模型 …… 35
3.3 五层网络安全体系 …… 36
3.4 六层网络安全体系 …… 39
3.5 基于六层网络安全体系的网络安全解决方案 …… 40
3.6 小结 …… 43
习题 …… 44
参考文献 …… 44
第4章 安全等级与标准 …… 45
4.1 国际安全评价标准 …… 46
4.1.1 TCSEC 标准 …… 46
4.1.2 欧洲 ITSEC …… 47
4.1.3 加拿大 CTCPEC 评价标准 …… 48
4.1.4 美国联邦准则 FC …… 48
4.1.5 CC 标准 …… 48
4.1.6 BS 7799 标准 …… 49
4.2 我国计算机安全等级划分与相关标准 …… 53
4.3 小结 …… 54
习题 …… 55
参考文献 …… 55

第三部分 密码学理论

第5章 密码学概述 …… 59
5.1 密码学的起源、发展和应用 …… 59
5.2 密码学基础 …… 60
5.2.1 密码学概述 …… 60
5.2.2 不可攻破的密码系统 …… 61
5.2.3 密码分析 …… 62
5.3 传统密码技术 …… 63

5.3.1 换位密码 …… 63
5.3.2 代替密码 …… 64
5.3.3 转轮机 …… 66
5.4 流密码与分组密码 …… 66
5.4.1 流密码 …… 66
5.4.2 分组密码概述 …… 70
5.5 小结 …… 71
习题 …… 71
参考文献 …… 72
第6章 对称密码体系 …… 73
6.1 对称密码体系的原理 …… 73
6.2 DES …… 74
6.2.1 DES 分组密码系统 …… 74
6.2.2 二重 DES …… 79
6.2.3 对 DES 应用的不足点讨论 …… 80
6.3 IDEA 等其他算法介绍 …… 82
6.3.1 设计原理 …… 82
6.3.2 加密过程 …… 83
6.4 AES 简介 …… 88
6.4.1 RC6 …… 88
6.4.2 SERPENT …… 90
6.4.3 Rijndael 算法 …… 92
6.5 小结 …… 93
习题 …… 94
参考文献 …… 94
第7章 公钥密码体制 …… 95
7.1 公钥密码体制的设计原理 …… 95
7.2 RSA …… 98
7.2.1 算法描述 …… 98
7.2.2 RSA 算法中的计算问题 …… 99
7.2.3 RSA 的安全性 …… 100
7.3 椭圆曲线密码算法 …… 101
7.3.1 椭圆曲线 …… 101
7.3.2 有限域上的椭圆曲线 …… 102
7.3.3 椭圆曲线上的密码 …… 103
7.4 小结 …… 105
习题 …… 105

参考文献 …… 105
第 8 章　密钥分配与管理 …… 106
8.1　密钥分配方案 …… 106
8.1.1　常规加密密钥的分配 …… 107
8.1.2　公开加密密钥的分配 …… 109
8.1.3　利用公开密钥加密进行常规加密密钥的分配 …… 111
8.2　密钥的管理 …… 112
8.2.1　密钥的生成 …… 113
8.2.2　密钥的使用与存储 …… 114
8.2.3　密钥的备份与恢复 …… 114
8.2.4　密钥的销毁 …… 115
8.3　小结 …… 115
习题 …… 116
参考文献 …… 116
第 9 章　报文鉴别与散列函数 …… 117
9.1　报文鉴别码 …… 117
9.1.1　数据认证算法 …… 117
9.1.2　攻击策略 …… 118
9.2　散列函数 …… 119
9.2.1　简单散列函数 …… 120
9.2.2　攻击策略 …… 121
9.3　常见的散列算法 …… 121
9.3.1　MD5 …… 121
9.3.2　SHA …… 125
9.3.3　RIPEMD-160 …… 127
9.3.4　HMAC …… 131
9.4　小结 …… 132
习题 …… 133
参考文献 …… 133
第 10 章　数字签名与鉴别协议 …… 134
10.1　数字签名原理 …… 134
10.1.1　数字签名原理 …… 134
10.1.2　数字签名流程 …… 135
10.1.3　数字签名作用 …… 135
10.1.4　数字证书 …… 135
10.2　鉴别协议 …… 136
10.2.1　报文鉴别 …… 136
10.2.2　相互鉴别 …… 137
10.2.3　单向鉴别 …… 138

10.3 数字签名标准 …… 139
10.4 小结 …… 141
习题 …… 141
参考文献 …… 141
第 11 章 信息隐藏技术 …… 142
11.1 信息隐藏技术原理 …… 142
11.1.1 信息隐藏模型 …… 142
11.1.2 信息隐藏系统的特征 …… 143
11.1.3 信息隐藏技术的主要分支与应用 …… 144
11.2 数据隐写术 …… 145
11.2.1 替换系统 …… 145
11.2.2 变换域技术 …… 149
11.2.3 扩展频谱 …… 151
11.2.4 对隐写术的一些攻击 …… 153
11.3 数字水印 …… 154
11.3.1 数字水印模型与特点 …… 154
11.3.2 数字水印主要应用领域 …… 155
11.3.3 数字水印的一些分类 …… 156
11.3.4 数字水印算法 …… 156
11.3.5 数字水印攻击分析 …… 158
11.3.6 数字水印研究状况与展望 …… 160
11.4 小结 …… 161
习题 …… 161
参考文献 …… 161

第四部分 安全技术与产品

第 12 章 身份认证 …… 165
12.1 原理 …… 165
12.2 单机状态下的身份认证 …… 166
12.2.1 基于口令的认证方式 …… 166
12.2.2 基于智能卡的认证方式 …… 167
12.2.3 基于生物特征的认证方式 …… 168
12.3 网络环境下的身份认证 …… 171
12.3.1 一次性口令技术 …… 171
12.3.2 PPP 中的认证协议 …… 173
12.3.3 RADIUS 协议 …… 175
12.3.4 Kerberos 认证服务 …… 177
12.3.5 Single Sign On …… 185
12.4 Windows NT 安全子系统 …… 188

12.5 小结…… 191
习题…… 191
参考文献…… 192
第 13 章 授权与访问控制 …… 193
13.1 概念原理…… 193
13.2 常用的实现方法…… 194
13.2.1 访问控制矩阵 …… 194
13.2.2 访问能力表 …… 194
13.2.3 访问控制表 …… 195
13.2.4 授权关系表 …… 196
13.3 访问控制策略…… 197
13.3.1 自主访问控制 DAC …… 198
13.3.2 强制型的访问控制 MAC …… 198
13.3.3 基于角色的访问控制 …… 199
13.4 实例:Windows NT 提供的安全访问控制手段 …… 206
13.4.1 权力 …… 206
13.4.2 共享 …… 207
13.4.3 权限 …… 207
13.4.4 用户组…… 208
13.5 小结…… 208
习题…… 208
参考文献…… 209
第 14 章 PKI /PMI 技术 …… 210
14.1 理论基础…… 210
14.1.1 可认证性与数字签名 …… 210
14.1.2 信任关系与信任模型 …… 213
14.2 PKI 的组成…… 216
14.2.1 认证机关 …… 217
14.2.2 证书库…… 219
14.2.3 密钥备份及恢复系统 …… 219
14.2.4 证书作废处理系统 …… 220
14.2.5 PKI 应用接口系统 …… 220
14.3 PKI 的功能和要求…… 220
14.3.1 证书、密钥对的自动更换 …… 220
14.3.2 交叉认证…… 221
14.3.3 其他一些功能 …… 221
14.3.4 对 PKI 的性能要求 …… 222
14.4 PKI 相关协议…… 222
14.4.1 X.500 目录服务 …… 222

14.4.2 X.509 …… 223
14.4.3 公开秘钥证书的标准扩展 …… 224
14.4.4 LDAP 协议 …… 225
14.5 PKI 的产品、应用现状和前景 …… 226
14.5.1 PKI 的主要厂商和产品 …… 226
14.5.2 PKI 的应用现状和前景 …… 229
14.6 PMI …… 230
14.6.1 PMI 简介 …… 231
14.6.2 权限和角色管理基础设施标准确认(PERMIS)工程 …… 232
14.6.3 PERMIS 的权限管理基础设施(PMI)实现 …… 233
14.7 小结 …… 235
习题 …… 236
参考文献 …… 236
第 15 章 IP 的安全 …… 237
15.1 IP 安全概述 …… 237
15.2 IP 安全体系结构 …… 238
15.2.1 概述 …… 238
15.2.2 安全关联 …… 239
15.2.3 AH 协议 …… 241
15.2.4 ESP 协议 …… 243
15.2.5 ISAKMP 协议 …… 243
15.2.6 IKE 协议 …… 244
15.2.7 IPSec 的处理 …… 247
15.3 实例:Windows 2000 对 IPSec 的支持 …… 249
15.3.1 Windows 2000 的安全策略模式 …… 249
15.3.2 自动密钥管理 …… 249
15.3.3 安全服务 …… 251
15.3.4 实例 …… 252
15.4 小结 …… 252
习题 …… 253
参考文献 …… 253
第 16 章 电子邮件的安全 …… 254
16.1 电子邮件安全概述 …… 254
16.2 PGP …… 255
16.2.1 PGP 的历史及概述 …… 255
16.2.2 PGP 的算法 …… 256
16.2.3 PGP 的安全性 …… 257
16.3 S/MIME …… 259
16.4 垃圾邮件 …… 261

16.5 实例:PGP 软件的使用 …… 262
16.6 小结 …… 265
习题 …… 265
参考文献 …… 266
第 17 章 Web 与电子商务的安全 …… 267
17.1 Web 与电子商务的安全分析 …… 267
17.1.1 对 Web 服务器的安全威胁 …… 267
17.1.2 对 Web 浏览客户机的安全威胁 …… 268
17.1.3 对通信信道的安全威胁 …… 269
17.2 Web 安全防护技术 …… 269
17.2.1 Web 程序组件安全防护 …… 269
17.2.2 其他安全防护技术 …… 270
17.3 SSL …… 271
17.3.1 SSL 概述 …… 271
17.3.2 SSL 握手过程 …… 271
17.3.3 SSL 的缺点 …… 273
17.4 电子商务的安全 …… 273
17.5 主页防修改技术 …… 276
17.5.1 主页监控 …… 276
17.5.2 主页恢复 …… 277
17.6 小结 …… 277
习题 …… 278
参考文献 …… 278
第 18 章 防火墙技术 …… 279
18.1 防火墙的基本概念 …… 279
18.1.1 定义 …… 279
18.1.2 防火墙结构 …… 279
18.1.3 防火墙应满足的条件 …… 279
18.1.4 防火墙的功能 …… 279
18.1.5 防火墙的不足之处 …… 280
18.2 防火墙的类型 …… 281
18.2.1 类型 …… 281
18.2.2 分组过滤路由器 …… 281
18.2.3 应用级网关 …… 281
18.2.4 电路级网关 …… 282
18.3 防火墙的体系结构 …… 282
18.3.1 双宿/多宿主机模式 …… 283
18.3.2 屏蔽主机模式 …… 283
18.3.3 屏蔽子网模式 …… 284

18.4 防火墙的基本技术与附加功能 …… 285
18.4.1 基本技术 …… 285
18.4.2 附加功能 …… 286
18.5 防火墙技术的几个新方向 …… 287
18.5.1 透明接入技术 …… 287
18.5.2 分布式防火墙技术 …… 288
18.5.3 以防火墙为核心的网络安全体系 …… 288
18.6 常见的防火墙产品 …… 289
18.6.1 常见的防火墙产品 …… 289
18.6.2 选购防火墙的一些基本原则 …… 290
18.7 小结 …… 291
习题 …… 291
参考文献 …… 291
第 19 章 VPN 技术 …… 292
19.1 VPN 的基本原理 …… 292
19.2 VPN 的应用领域 …… 294
19.3 VPN 的关键安全技术 …… 296
19.4 VPN 的实现方法 …… 297
19.5 VPN 产品与解决方案 …… 299
19.5.1 解决方案一 …… 299
19.5.2 解决方案二 …… 299
19.6 小结 …… 300
习题 …… 300
参考文献 …… 301
第 20 章 安全扫描技术 …… 302
20.1 常见黑客攻击过程 …… 302
20.1.1 目标探测和信息攫取 …… 302
20.1.2 获得访问权(Gaining Access) …… 306
20.1.3 特权提升(Escalating Privilege) …… 306
20.1.4 掩踪灭迹(Covering Tracks) …… 306
20.1.5 创建后门(Greating Back Door) …… 306
20.1.6 总结 …… 306
20.2 安全扫描技术分类 …… 307
20.2.1 基于主机的扫描技术 …… 307
20.2.2 基于网络的扫描检测技术 …… 309
20.3 安全扫描系统的设计 …… 310
20.3.1 设计原理 …… 310
20.3.2 安全扫描的逻辑结构 …… 311
20.4 安全扫描技术的发展趋势 …… 313

20.5 常见安全扫描工具与产品介绍 …… 314
20.5.1 常见的免费扫描工具介绍 …… 314
20.5.2 常见的商业安全扫描产品 …… 315
20.6 小结 …… 317
习题 …… 317
参考文献 …… 317
第 21 章 入侵检测与安全审计 …… 319
21.1 入侵检测系统概览 …… 319
21.1.1 入侵检测系统的功能 …… 319
21.1.2 入侵检测的发展 …… 320
21.2 入侵检测系统的分类 …… 320
21.2.1 基于主机、网络以及分布式的入侵检测系统 …… 320
21.2.2 离线和在线检测系统 …… 321
21.2.3 异常检测和特征检测 …… 322
21.3 入侵检测系统的系统结构 …… 322
21.3.1 CIDF 模型 …… 322
21.3.2 简单的分布式入侵检测系统 …… 323
21.3.3 基于智能代理技术的分布式入侵检测系统 …… 324
21.4 入侵检测系统的分析方法 …… 326
21.4.1 异常检测分析方法 …… 328
21.4.2 滥用检测分析方法 …… 330
21.5 入侵检测的发展方向 …… 334
21.6 典型入侵检测系统简介 …… 336
21.6.1 免费的 IDS——Snort …… 336
21.6.2 商业 IDS 的代表——ISS 的 RealSecure …… 337
21.7 现代安全审计技术 …… 340
21.7.1 安全审计现状 …… 340
21.7.2 CC 标准中的网络安全审计功能定义 …… 342
21.7.3 一个分布式入侵检测和安全审计系统 S_Audit 简介 …… 344
21.8 小结 …… 347
习题 …… 347
参考文献 …… 348
第 22 章 网络病毒防范 …… 350
22.1 病毒的发展史 …… 350
22.2 病毒的原理与检测技术 …… 353
22.2.1 计算机病毒的定义 …… 353
22.2.2 计算机病毒的特性 …… 353
22.2.3 计算机病毒的命名 …… 354
22.2.4 计算机病毒的分类 …… 354

22.2.5 计算机病毒的传播途径 …… 355
22.2.6 计算机病毒的检测方法 …… 356
22.3 病毒防范技术措施 …… 359
22.3.1 单机下病毒防范 …… 360
22.3.2 小型局域网的防范 …… 362
22.3.3 大型网络的病毒防范 …… 365
22.4 病毒防范产品介绍 …… 366
22.4.1 计算机病毒防治产品的分类 …… 366
22.4.2 防杀计算机病毒软件的特点 …… 367
22.4.3 对计算机病毒防治产品的要求 …… 367
22.4.4 常见的计算机病毒防治产品 …… 368
22.5 小结 …… 369
习题 …… 369
参考文献 …… 370
第 23 章 系统增强技术 …… 371
23.1 操作系统安全增强 …… 371
23.1.1 打好补丁与最小化服务 …… 371
23.1.2 增强用户认证和访问控制 …… 372
23.1.3 系统漏洞扫描与入侵检测 …… 374
23.1.4 安全审计和其他 …… 374
23.2 特定应用服务安全增强 …… 375
23.3 小结 …… 382
习题 …… 382
参考文献 …… 382
第 24 章 安全应急响应 …… 384
24.1 概述 …… 384
24.1.1 安全应急响应的提出 …… 384
24.1.2 CERT 的主要目的和作用 …… 384
24.1.3 应急响应和安全团队论坛(FIRST) …… 385
24.1.4 相关概念 …… 385
24.2 建立安全应急响应 …… 386
24.2.1 确定应急响应的目标和范畴 …… 386
24.2.2 应急响应的队伍建设 …… 386
24.2.3 应急响应的流程建设 …… 391
24.2.4 安全应急响应体系的建立 …… 392
24.3 应急响应的运作 …… 393
24.3.1 质量与服务模型 …… 393
24.3.2 应急响应的服务 …… 393