

国外经典初学者入门教程系列

Mc
Graw
Hill Education



Fundamentals of Network Security

网络安全 基础教程

Eric Maiwald 著

马海军 王泽波 等译



清华大学出版社

网络安全基础教程

Eric Maiwald 著
马海军 王泽波 等 译

清华大学出版社
北 京

Eric Maiwald
Fundamentals of Network Security
EISBN: 0-07-223093-2

Copyright © 2004 by The McGraw-Hill Companies, Inc.

Original language published by The McGraw-Hill Companies, Inc. All Rights reserved. No part of this publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

Simplified Chinese translation edition is published and distributed exclusively by Tsinghua University Press under the authorization by McGraw-Hill Education(Asia) Co., within the territory of the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan. Unauthorized export of this edition is a violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书中文简体字翻译版由美国麦格劳-希尔教育出版(亚洲)公司授权清华大学出版社在中华人民共和国境内(不包括中国香港、澳门特别行政区和中国台湾地区)独家出版发行。未经许可之出口,视为违反著作权法,将受法律之制裁。未经出版者预先书面许可,不得以任何方式复制或抄袭本书的任何部分。

北京市版权局著作权合同登记号 图字:01-2004-3533

版权所有,翻印必究。举报电话:010-62782989 13501256678 13801310933

本书封面贴有 McGraw-Hill 公司防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

网络安全基础教程/麦伍德(Maiwald, E.)著;马海军,王泽波等译. —北京:清华大学出版社,2005.7
书名原文:Fundamentals of Network Security
ISBN 7-302-10902-8

I. 网… II. ①麦… ②马… ③王… III. 计算机网络-安全技术-教材 IV. TP393.08

中国版本图书馆 CIP 数据核字(2005)第 039745 号

出版者:清华大学出版社 地址:北京清华大学学研大厦
<http://www.tup.com.cn> 邮 编:100084
社总机:010-62770175 客户服务:010-62776969

责任编辑:冯志强

印装者:北京鑫海金澳胶印有限公司

发行者:新华书店总店北京发行所

开 本:185×230 印张:32 字数:714 千字

版 次:2005 年 7 月第 1 版 2005 年 7 月第 1 次印刷

书 号:ISBN 7-302-10902-8/TP·7251

印 数:1~3000

定 价:49.00 元

前言

关于本书

安全已经成为高等教育的重要课题。国家安全机构已经在全国的许多所大学建立了信息保证中心。本书是为了向该领域的学生提供信息安全的基础概念。在编写本书的时候，我还挑选了作为安全官员和顾问在日常工作遇到的那些棘手问题，其中大多数问题曾经困扰我多年，精通所有这些信息会对我有很大的帮助。

安全仍然是机构面临的大问题。我们不仅仅听说过成功侵入网站和机构的事例，而且还知道现在已经制定了新的法律和法规来保护信息。为了解决这些问题，越来越多的公司开发了安全保护工具。从这些情况看来，似乎安全中的最大问题通过技术就可以解决。遗憾的是，安全问题远远比这复杂。最低限度，安全也是大的问题。不管我们针对该问题开发多少技术，最好的做法都莫过于简化安全从业人员的工作难度。我们不仅仅通过技术解决基本的安全问题，而且还必须通过应用深思熟虑的安全进程和过程来管理安全问题。

学习信息安全的学生需要理解基本的概念才能在现实环境中应用这些概念。希望本书能够提供基本的认识。本书说明了开发计算机安全和信息保证的专业方法的重要性，实现了技术性和管理性问题之间的良好平衡。本书总体的编写形式和风格将进一步说明这种平衡。示例非常清晰，使初学者能够迅速掌握要点，并且会提出问题让读者进一步学习。另一方面，本书也是为那些希望了解更多计算机安全知识，以保护其信息资产的科技工作者提供的优秀书籍。本书使读者清楚地知道，信息安全是一种过程，而不是工具的操作。

本书可以用于在理工科课程上为二年级学生讲授网络安全基础知识，它还可以用作高年级学生的教材，用来学习结合网络操作知识和网络安全管理的高级网络课程。此外，本书还适用于非理工科硕士学位计划的信息保证课程。本书包含了联邦标准 NCSSI 4013 的所有要点以及 NSTISSC 4011 的大部分内容。

教师资源

教师资源是通过教师包提供的，包括以下内容：

—反映本书组织结构的教师指南。

II 前 言

- 本书章尾内容的答案
- 生成许多组基于书面或网络测试和自动升级功能的 Exam View Pro 测试题库软件
- 由资深 IT 教师编写的数百道问答题
- 各种题型和不同难度，使教师能够自己制订每一次测试，以便使学生的学习进程最佳化
- 支持与所讲授题目有关的 PowerPoint 幻灯片

作者简介

Eric Maiwald 是 Bluefire Security Technologies 公司的产品管理和支持负责人。Eric 在信息安全领域具有长达 16 年的丰富阅历，他既在政府部门工作过，也为商业公司工作过。他为大型金融机构、保健公司进行工作评估、开发策略，并实现安全解决方案。Eric 获得了 Rensselaer Polytechnic Institute 的电子工程学士学位，Stevens Institute of Technology 的工程硕士学位，并且是信息系统安全认证专家(CISSP)。他在大量著名的安全会议上做过发言，并编写了 Security Planning and Disaster Recovery (与 William Sieglein 合作，此书由 McGraw-Hill/Osborne 出版)，与他人合作编写了 Hacking Linux Exposed and Hacker's Challenge (由 McGraw-Hill/Osborne 出版)。他的通信方式是 emaiwald@fred.net。

本书丛书编辑

Corey D. Schou, Ph. D. 是 Idaho State 大学商学院信息与联络系的教授。在长达 25 年的时间里，他一直都在参与建立计算机安全以及信息保证培训和标准。他的研究领域包括信息保证、道德规范、隐私和协作决策。他曾为 CNSS(国家安全系统委员会，Committee on National Security Systems)负责编纂和编辑计算机安全标准和培训资料。

尽管 Schou 曾从事过研究和服务事务，但是在他的整个职业生涯中，他仍是一名活跃的教师。他是 NIATEC(国家信息保证培训和教育中心，National Information Assurance Training and Education Center)的创立董事，该中心被指定为 National Center of Excellence in Information Assurance Education。

1996 年，ISSA(信息系统安全协会，Information Systems Security Association)表彰了他的研究中心为安全行业做出的杰出贡献，他被 FISSEA(联邦信息系统安全教育家协会，Federal Information Systems Security Educators Association)选举为该年度的教育家。1997 年，Masie Institute and TechLearn Consortium 认可了他在远程教育方面做出的贡献。2001 年，Dr. Schou 被 ISC(国际信息系统安全认证协会，International Information Systems Security Certification Consortium)授予了 Tipton 奖章，以表彰他在计算机安全的专业化方面做出的工作，以及他所开发的用于信息保证专业认证的 CBK(Common Body of Knowledge)。

Schou 担任 CISSE(信息系统安全教育学术讨论会，Colloquium for Information Systems Security Education)主席。在他的领导下，这家学术讨论会为那些与信息安全和信息保证教育有关的政府、工业和学术界领导创建了相互交流和对话的环境。此外，他还是信息系统安全(Information Systems Security)的编辑，而且也是多家专业机构的董事会成员。

本书合作作者

Philip Cox 是 SystemExperts Corporation 的顾问。他是业界公认的顾问、作家和演讲家，

IV 作者简介

做出过许多业绩。Phil 是权威图书 Windows 2000 Security Handbook (由 McGraw-Hill/Osborne 出版)的主要作者。他获得了 College of Charleston 的计算机专业自然科学学士学位,还是 Microsoft Certified Systems Engineer(微软认证系统工程师, MCSE)。

Gray Sparks 是 Metropolitan Community 学院的专职人员,该校计算机和办公技术领域的系代表,微软认证专家和 Nebraska Air National Guard 的计算机操作专家。他毕业于 Bellevue 大学,取得了信息系统管理学位,目前正在集中精力考取计算机法律的硕士。Gray 拥有 18 年在美国空军工作的信息系统、信息、物理和个人安全方面的经验。他是 Metropolitan Community 学院的 Midwest Center for Information Technology 现场协调员,也是 Bellevue Public Schools 的 IT 顾问委员会成员,曾在国家会议上做过有关信息和网络安全的发言。

本书技术编辑

John Bock 是一位 CISSP,是 Foundstone 的研发工程师,主要研究方向是网络评估技术和无线网络的安全。他负责设计 Foundstone Enterprise Risk Solutions 产品线新的评估特征。John 在网络安全方面具有深厚的顾问阅历,领导了一个企业安全小组。在加入 Foundstone 之前,他完成了入侵测试和安全评估,是 Internet Security Systems(ISS)的无线网络安全顾问。

Mariana Hentea 是位于印第安那州 Calumet 的 Purdue University 的助教,她是 IEEE 和 SWE 的成员。她获得了位于芝加哥的 Illinois Institute of Technology 的计算机硕士和博士学位,以及位于罗马尼亚的 Polytechnic Institute of Timisoara 的电子工程学士学位和计算机硕士学位。她发表了关于通信、钢铁和化学工业方面计算机软件和工程应用方面的大量论文。1995 年, Mariana 参与设计和实施了美国国防部的计算机和网络安全。

评论者

下列人员提供了富有见解的评论、批评意见和有益的建议。

Dan Byram, 美国加利福尼亚州圣塔阿那的 Corinthian 大学

Elsa Lankford, 马里兰州巴尔的摩的巴尔的摩大学

Matt Pope, 加利福尼亚州圣何塞市的 Corinthian 大学

Tom Trevethan, 弗吉尼亚州弗吉尼亚海滩的 ECPI 科技大学

致 谢

本书得以出版,得到了众人的帮助。McGraw-Hill 的工作人员,包括 Jane Brownlow、Chris Johnson、Laura Stone 和 Jody Mckenzie 是本书背后的推动力量。其他人员,包括 Lee Kelly、John Alexander、Rob Fike、Dave Henning、Sam Hinson、Robert Burnett 和 Lauren Schuler 为本书提供了技术支持。

目 录

前言	I
----------	---

第1部分 信息安全基础知识

第1章 信息安全	2
1.1 信息安全定义	3
1.2 安全是一个过程，而不是静止产品	9
1.2.1 防病毒软件	9
1.2.2 访问控制	9
1.2.3 防火墙	9
1.2.4 智能卡	10
1.2.5 生物统计学系统	10
1.2.6 入侵检测	11
1.2.7 策略管理	11
1.2.8 薄弱点扫描	11
1.2.9 加密	11
1.2.10 物理安全机制	12
项目1 检查计算机安全认证	12
1.3 总结与练习	13
1.3.1 本章小结	13
1.3.2 关键术语	14
1.3.3 关键术语题	14
1.3.4 多项选择题	15
1.3.5 问答题	16
1.3.6 实验项目	16
第2章 攻击类型	17
2.1 定义访问攻击	18
2.1.1 监听	18
2.1.2 窃听	18
2.1.3 截听	20
2.1.4 访问攻击是如何完成的	20
2.2 定义修改攻击	23
2.2.1 更改攻击	23
2.2.2 插入攻击	23
2.2.3 删除攻击	23
2.2.4 如何完成修改攻击	23

2.3 定义拒绝服务攻击	24
2.3.1 拒绝对信息进行访问	25
2.3.2 拒绝对应用程序进行访问	25
2.3.3 拒绝对系统进行访问	25
2.3.4 拒绝对通信进行访问	25
2.3.5 如何实现 DoS 攻击	25
2.4 定义否认攻击	26
2.4.1 伪装	26
2.4.2 否认事件	27
2.4.3 如何实现否认攻击	27
项目2 检查系统的薄弱点	28
2.5 总结与练习	29
2.5.1 本章小结	29
2.5.2 关键术语	30
2.5.3 关键术语题	31
2.5.4 多项选择题	31
2.5.5 问答题	33
2.5.6 实验项目	33
第3章 黑客技术	34
3.1 识别黑客的动机	35
3.1.1 挑战	35
3.1.2 贪婪	36
3.1.3 恶意	37
3.2 学习历史上的黑客技术	37
3.2.1 开放共享	37
3.2.2 糟糕的密码	39
3.2.3 编程中的漏洞	40
3.2.4 社会工程	40
3.2.5 缓存溢出	41
3.2.6 拒绝服务	43
3.3 学习高级技术	47
3.3.1 嗅闻交换网络	47
3.3.2 IP 哄骗	49
3.4 识别恶意代码	52
3.4.1 病毒	52

VI 目 录

3.4.2 特洛伊木马病毒	53	4.5 总结与练习	85
3.4.3 蠕虫病毒	53	4.5.1 本章小结	85
3.4.4 Slapper 蠕虫示例	54	4.5.2 关键术语	86
3.4.5 混合体	54	4.5.3 关键术语题	87
3.5 识别无目标黑客的方法	55	4.5.4 多项选择题	88
3.5.1 目标	55	4.5.5 问答题	89
3.5.2 侦察	55	4.5.6 实验项目	89
3.5.3 攻击手段	57		
3.5.4 利用已受攻击的系统	57	第2部分 基础工作	
3.6 识别有目标黑客的方法	62	第5章 信息安全的法律问题	92
3.6.1 目标	62	5.1 美国刑法	93
3.6.2 侦察	62	5.1.1 计算机诈骗与滥用 (18US Code 1030)	93
3.6.3 攻击方法	65	5.1.2 信用卡诈骗 (18 US Code 1029)	94
3.6.4 利用被攻击的系统	67	5.1.3 版权(18 US Code 2319)	94
项目3 完成对你的站点的侦察	67	5.1.4 截听(18 US Code 2511)	94
3.7 总结与练习	68	5.1.5 对电子信息的访问 (18 US Code 2701)	95
3.7.1 本章小结	68	5.1.6 其他犯罪条款	95
3.7.2 关键术语	70	5.1.7 Patriot 法案	95
3.7.3 关键术语题	71	5.1.8 国土安全法案	97
3.7.4 多项选择题	72	5.2 州法律	97
3.7.5 问答题	73	5.3 其他国家的法律	98
3.7.6 实验项目	74	5.3.1 澳大利亚	98
第4章 信息安全服务	75	5.3.2 巴西	98
4.1 定义机密性	76	5.3.3 印度	99
4.1.1 文件的机密性	76	5.3.4 中华人民共和国	99
4.1.2 传输中信息的机密性	77	5.3.5 英国	99
4.1.3 通信数据流的机密性	78	5.4 起诉	99
4.1.4 可以防止的攻击	79	5.4.1 收集证据	100
4.2 定义完整性	79	5.4.2 联系执法机关	101
4.2.1 文件的完整性	80	5.5 民事问题	101
4.2.2 信息传输的完整性	80	5.5.1 员工问题	102
4.2.3 可以预防的攻击	81	5.5.2 连带责任	102
4.3 定义可用性	81	5.6 隐私问题	103
4.3.1 备份	81	5.6.1 客户信息	103
4.3.2 故障还原	82	5.6.2 HIPAA	104
4.3.3 灾难还原	82	5.6.3 “可选择的”与必要的组成 部分	104
4.3.4 可以预防的攻击	82	5.6.4 安全规则的要求	104
4.4 定义责任性	82	5.6.5 Graham-Leach-Bliley 财务	
4.4.1 识别和认证	83		
4.4.2 审核	83		
4.4.3 可以预防的攻击	84		
项目4 保护信息	84		

服务现代化法案	106	6.6 总结与练习	138
项目 5 起诉违法人员	107	6.6.1 本章小结	138
5.7 总结与练习	108	6.6.2 关键术语	140
5.7.1 本章小结	108	6.6.3 关键术语题	140
5.7.2 关键术语	110	6.6.4 多项选择题	141
5.7.3 关键术语题	111	6.6.5 问答题	143
5.7.4 多项选择题	112	6.6.6 实验项目	143
5.7.5 问答题	114	第 7 章 管理风险	144
5.7.6 实验项目	114	7.1 风险定义	145
第 6 章 策略	115	7.1.1 薄弱点	145
6.1 策略的重要性	116	7.1.2 威胁	146
6.1.1 定义安全性	116	7.1.3 威胁 + 薄弱点 = 风险	149
6.1.2 让所有人看到	116	7.2 确认机构的风险	150
6.2 定义不同的策略	117	7.2.1 确认薄弱点	150
6.2.1 信息策略	117	7.2.2 确认真正威胁	151
6.2.2 安全策略	119	7.2.3 检查防范措施	151
6.2.3 计算机使用策略	122	7.2.4 确认风险	152
6.2.4 Internet 使用策略	123	7.3 评估风险	153
6.2.5 邮件策略	123	7.3.1 金钱	153
6.2.6 用户管理过程	124	7.3.2 时间	154
6.2.7 系统管理过程	125	7.3.3 资源	154
6.2.8 备份策略	126	7.3.4 形象	155
6.2.9 应急响应过程	127	7.3.5 业务损失	155
6.2.10 配置管理过程	130	7.3.6 评估风险的方法	155
6.2.11 设计方法论	130	项目 7 确认机构的电子风险	156
6.2.12 灾难还原计划	132	7.4 总结与练习	157
6.3 制定正确的策略	133	7.4.1 本章小结	157
6.3.1 定义重要策略	133	7.4.2 关键术语	158
6.3.2 定义可接受的行为	134	7.4.3 关键术语题	159
6.3.3 确认利益相关人	134	7.4.4 多项选择题	159
6.3.4 定义正确的大纲	134	7.4.5 问答题	161
6.3.5 制定策略	134	7.4.6 实验项目	161
6.4 部署策略	135	第 8 章 信息安全过程	162
6.4.1 策略被接受	135	8.1 评估	163
6.4.2 教育	135	8.1.1 网络	165
6.4.3 实现	136	8.1.2 物理安全	166
6.5 有效使用策略	136	8.1.3 策略和过程	167
6.5.1 新的系统和项目	136	8.1.4 预防措施	168
6.5.2 现有系统和项目	136	8.1.5 安全意识	169
6.5.3 审核	137	8.1.6 人员	169
6.5.4 策略复查	137	8.1.7 工作量	170
项目 6 制定机构内部使用策略	137	8.1.8 态度	170

8.1.9 遵守情况	170	9.2.1 网络连接性	197
8.1.10 业务	171	9.2.2 恶意代码的防护	198
8.1.11 评估结果	171	9.2.3 身份验证机制	199
8.2 制定策略	172	9.2.4 监控	200
8.2.1 选择制定策略的顺序	172	9.2.5 加密	201
8.2.2 升级现有的策略	173	9.2.6 补丁系统	201
8.3 实现安全	173	9.2.7 备份和还原	202
8.3.1 安全报告系统	174	9.2.8 物理安全	202
8.3.2 身份验证系统	174	9.3 应用 ISO 17799	204
8.3.3 Internet 安全	175	9.3.1 此标准中的关键概念	204
8.3.4 入侵检测系统	175	9.3.2 如何使用此标准	205
8.3.5 加密	176	项目 9 缺口分析	205
8.3.6 物理安全	177	9.4 总结与练习	206
8.3.7 工作人员	177	9.4.1 本章小结	206
8.4 安全意识培训	178	9.4.2 关键术语	208
8.4.1 员工	178	9.4.3 关键术语题	209
8.4.2 管理员	178	9.4.4 多项选择题	209
8.4.3 开发人员	178	9.4.5 问答题	211
8.4.4 主管人员	178	9.4.6 实验项目	211
8.4.5 安全人员	179		
8.5 审核	179	第 3 部分 安全技术	
8.5.1 策略遵守情况审核	179	第 10 章 防火墙	214
8.5.2 定期项目评估和新的项目 评估	180	10.1 防火墙的类型	215
8.5.3 入侵测试	180	10.1.1 应用层防火墙	215
项目 8 部署安全意识程序	181	10.1.2 数据包过滤防火墙	216
8.6 总结与练习	181	10.1.3 混合型	218
8.6.1 本章小结	181	10.2 防火墙的配置	219
8.6.2 关键术语	184	10.2.1 体系结构 1: 防火墙之外 Internet 可以访问的系统	219
8.6.3 关键术语题	184	10.2.2 体系结构 2: 单一防 防火墙	220
8.6.4 多项选择题	185	10.2.3 体系结构 3: 双重防 防火墙	222
8.6.5 问答题	187	10.3 设计防火墙规则集	223
8.6.6 实验项目	187	项目 10 学习各种防火墙之间的区别	223
第 9 章 信息安全最佳实践	188	10.4 总结与练习	224
9.1 管理性安全	189	10.4.1 本章小结	224
9.1.1 策略和过程	189	10.4.2 关键术语	225
9.1.2 资源	190	10.4.3 关键术语题	226
9.1.3 责任	191	10.4.4 多项选择题	227
9.1.4 教育	192	10.4.5 问答题	228
9.1.5 突发事故计划	194	10.4.6 实验项目	229
9.1.6 安全项目计划	195		
9.2 技术性安全	197		

第 11 章 虚拟专用网络	230	12.3.1 公钥加密	261
11.1 虚拟专用网络	231	12.3.2 Diffie-Hellman 密钥 交换	262
11.2 部署用户 VPN	233	12.3.3 RSA	263
11.2.1 用户 VPN 的优点	234	12.3.4 其他公钥算法	265
11.2.2 用户 VPN 的问题	234	12.4 数字签名	266
11.2.3 管理用户 VPN	236	12.4.1 数字签名概述	266
11.3 部署站点 VPN	236	12.4.2 安全的哈希函数	267
11.3.1 站点 VPN 的优点	237	12.5 密钥管理	267
11.3.2 站点 VPN 的问题	237	12.5.1 创建密钥	268
11.3.3 管理站点 VPN	238	12.5.2 密钥分发	269
11.4 标准 VPN 技术	239	12.5.3 密钥证书	269
11.4.1 VPN 服务器	239	12.5.4 密钥保护	270
11.4.2 加密算法	241	12.5.5 密钥注销	271
11.4.3 认证系统	241	12.6 理解系统中的信任	271
11.4.4 VPN 协议	242	12.6.1 分层模型	271
11.5 VPN 系统的类型	243	12.6.2 Web	274
11.5.1 硬件系统	243	项目 12 设计加密系统	275
11.5.2 软件系统	244	12.7 总结与练习	276
11.5.3 基于 Web 的系统	244	12.7.1 本章小结	276
项目 11 研究不同 VPN 的区别	244	12.7.2 关键技术语	278
11.6 总结与练习	245	12.7.3 关键技术语题	280
11.6.1 本章小结	245	12.7.4 多项选择题	281
11.6.2 关键技术语	247	12.7.5 问答题	282
11.6.3 关键技术语题	248	12.7.6 实验项目	282
11.6.4 多项选择题	248	第 13 章 入侵检测	284
11.6.5 问答题	250	13.1 入侵检测系统的类型	286
11.6.6 实验项目	250	13.1.1 基于主机的 IDS	286
第 12 章 加密	251	13.1.2 基于网络的 IDS	289
12.1 加密的基本概念	252	13.1.3 是否某种 IDS 更优	291
12.1.1 加密的术语	252	13.2 安装 IDS	291
12.1.2 针对加密系统的攻击	253	13.2.1 定义 IDS 的目标	291
12.2 私钥加密	254	13.2.2 选择监视内容	293
12.2.1 私钥加密	254	13.2.3 选择响应方式	295
12.2.2 替换密文	255	13.2.4 设置临界值	298
12.2.3 一次性便条	255	13.2.5 实现系统	299
12.2.4 数据加密标准	256	13.3 管理 IDS	300
12.2.5 三重 DES	258	13.3.1 理解 IDS 可以提供的 信息	300
12.2.6 密码加密	259	13.3.2 调查可疑事件	303
12.2.7 高级加密标准: Rijndael	260	13.4 理解入侵预防措施	306
12.2.8 其他私钥算法	261	13.4.1 如何使用 IDS 预防入侵	
12.3 公钥加密	261		

活动	306	15.3.2 日志文件	347
13.4.2 入侵预防问题	307	15.3.3 隐藏文件	347
项目 13 部署网络 IDS	308	15.3.4 SUID 和 SGID 文件	348
13.5 总结与练习	309	15.3.5 所有人都可以写的文件	348
13.5.1 本章小结	309	15.3.6 查找可疑迹象	348
13.5.2 关键术语	312	项目 15 审核 Unix 系统	352
13.5.3 关键术语题	313	15.4 总结与练习	353
13.5.4 多项选择题	313	15.4.1 本章小结	353
13.5.5 问答题	315	15.4.2 关键术语	355
13.5.6 实验项目	315	15.4.3 关键术语题	356
 		15.4.4 多项选择题	356
第 4 部分 实际应用与针对平台的实现		15.4.5 问答题	358
第 14 章 桌面保护	318	15.4.6 实验项目	358
14.1 防止恶意代码	319	第 16 章 Windows NT 的安全问题	360
14.1.1 病毒、特洛伊木马和蠕虫问题	319	16.1 安装系统	361
14.1.2 有效使用反病毒软件	321	16.1.1 注册表设置	361
14.2 使用 Internet	322	16.1.2 系统配置设置	364
14.2.1 连接到 Internet	322	16.2 用户管理	368
14.2.2 共享文件	323	16.2.1 向系统添加用户	368
14.3 防止物理篡改	326	16.2.2 设置文件权限	369
14.3.1 桌面加密	326	16.2.3 从系统中删除用户	369
14.3.2 提高警惕	327	16.3 系统管理	370
项目 14 测试个人防火墙	327	16.3.1 审核系统	370
14.4 总结与练习	328	16.3.2 日志文件	371
14.4.1 本章小结	328	16.3.3 查找可疑迹象	371
14.4.2 关键术语	329	项目 16 配置 Windows NT 系统	372
14.4.3 关键术语题	329	16.4 总结与练习	374
14.4.4 多项选择题	330	16.4.1 本章小结	374
14.4.5 问答题	332	16.4.2 关键术语	375
14.4.6 实验项目	332	16.4.3 关键术语题	376
第 15 章 Unix 的安全问题	333	16.4.4 多项选择题	377
15.1 安装系统	334	16.4.5 问答题	379
15.1.1 启动文件	334	16.4.6 实验项目	379
15.1.2 允许的服务	335	第 17 章 Windows 2000/Windows 2003 Server 的安全问题	380
15.1.3 系统配置文件	338	17.1 安装系统	381
15.1.4 补丁程序	343	17.1.1 本地安全策略设置	381
15.2 用户管理	343	17.1.2 系统配置	385
15.2.1 向系统中添加用户	344	17.1.3 Windows 2003 的特殊配置问题	391
15.2.2 从系统中删除用户	345	17.2 用户管理	393
15.3 系统管理	346		
15.3.1 审核系统	346		

17.2.1 向系统中添加用户	393	18.5 理解网络地址转换	437
17.2.2 设置文件权限	395	18.5.1 网络地址转换	438
17.2.3 从系统中删除用户	396	18.5.2 专用类地址	438
17.3 系统管理	396	18.5.3 静态 NAT	439
17.3.1 secedit 命令	396	18.5.4 动态 NAT	440
17.3.2 审核系统	399	18.6 伙伴网络	441
17.3.3 日志文件	400	18.6.1 使用伙伴网络	441
17.3.4 查找可疑迹象	400	18.6.2 安装	441
17.4 使用活动目录	402	18.6.3 寻址问题	442
17.4.1 安全设置和安装	403	项目 18 创建 Internet 体系结构	443
17.4.2 管理	403	18.7 总结与练习	444
17.4.3 组策略和安全	404	18.7.1 本章小结	444
17.4.4 AD 用户和组管理	411	18.7.2 关键技术语	446
项目 17 使用 secedit 管理		18.7.3 关键技术语题	447
Windows 2000 安全配置	411	18.7.4 多项选择题	447
17.5 总结与练习	412	18.7.5 问答题	449
17.5.1 本章小结	412	18.7.6 实验项目	449
17.5.2 关键技术语	415	第 19 章 电子商务安全要求	450
17.5.3 关键技术语题	416	19.1 理解电子商务服务	451
17.5.4 多项选择题	416	19.1.1 电子商务服务与常规 DMZ 服务的区别	452
17.5.5 问答题	418	19.1.2 电子商务服务的例子	452
17.5.6 实验项目	418	19.2 可用性的重要性	454
第 18 章 Internet 体系结构	419	19.2.1 B-to-C 问题	454
18.1 提供的服务	420	19.2.2 B-to-B 问题	454
18.1.1 邮件	420	19.2.3 全球时间	455
18.1.2 加密的电子邮件	420	19.2.4 客户的满意程度	455
18.1.3 Web	421	19.2.5 停机时间带来的损失	456
18.1.4 对 Internet 的内部访问	421	19.2.6 解决可用性问题	456
18.1.5 从外部访问内部系统	422	19.3 客户端安全性	457
18.1.6 控制服务	422	19.3.1 通信安全	457
18.2 不应该提供的服务	423	19.3.2 在客户系统上保存 信息	458
18.3 开发通信体系结构	424	19.3.3 否认	459
18.3.1 单线访问	425	19.4 服务器端安全性	460
18.3.2 对单个 ISP 的多线 访问	426	19.4.1 存储在服务器上的 信息	460
18.3.3 对多个 ISP 的多线 访问	428	19.4.2 保护服务器不受 攻击	460
18.4 设计非军事区	431	19.5 实现应用程序的安全	464
18.4.1 定义 DMZ	431	19.5.1 正确的应用程序 设计	465
18.4.2 应该放入 DMZ 中的 系统	432		
18.4.3 合适的 DMZ 体系结构	434		

19.5.2 正确的编程技术	466	第 20 章 无线安全	481
19.5.3 向外界展示代码	466	20.1 当前采用的无线技术	482
19.5.4 配置管理	467	20.1.1 标准体系结构	483
19.6 数据库服务器的安全性	467	20.1.2 数据传输安全	483
19.6.1 数据库的位置	468	20.1.3 身份验证	485
19.6.2 与电子商务服务器 通信	468	20.2 无线安全问题	487
19.6.3 对内部访问进行 保护	470	20.2.1 WLAN 检测	487
19.7 电子商务体系结构	470	20.2.2 窃听	487
19.7.1 服务器的位置和 连接性	470	20.2.3 主动式攻击	488
19.7.2 可用性	471	20.2.4 潜在的法律问题	490
19.7.3 薄弱点扫描	472	20.3 安全地部署无线网络	490
19.7.4 审核信息和问题检测	472	20.3.1 接入点安全	490
项目 19 设计电子商务体系结构	472	20.3.2 传输安全	491
19.8 总结与练习	473	20.3.3 工作站安全	491
19.8.1 本章小结	473	20.3.4 站点安全	491
19.8.2 关键术语	477	项目 20 实现无线 LAN	492
19.8.3 关键术语题	477	20.4 总结与练习	492
19.8.4 多项选择题	478	20.4.1 本章小结	492
19.8.5 问答题	480	20.4.2 关键术语	494
19.8.6 实验项目	480	20.4.3 关键术语题	495
		20.4.4 多项选择题	495
		20.4.5 问答题	497
		20.4.6 实验项目	497

第 1 部分

信息安全基础知识



第1章.....

信息安全

1.1 信息安全定义

1.2 安全是一个过程,而不是静止产品

1.3 总结与练习

