

21

世纪高等院校计算机网络工程专业规划教材

网络安全与管理 (第二版)

石磊 赵慧然 编著



清华大学出版社

21世纪高等院校计算机网络工程专业规划教材

网络安全与管理

(第二版)

石磊 赵慧然 编著

清华大学出版社
北京

内 容 简 介

本书针对培养应用型人才的需求,介绍了网络安全的基本理论和安全管理工具的应用。全书共分为理论部分10章和实验部分6章。理论部分是对网络安全基本理论和技术的详细讲解,通过这一部分使读者在理论上有一个清楚的认识。实验部分选择了目前常用的几种网络安全工具,通过对工具的使用与操作,把理论和实践联系起来,达到理解运用的目的。

本书可作为网络、计算机、软件、信息管理等专业本科生的教科书,也可供从事相关专业的网络管理、教学、科研和工程人员参考。

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 13701121933

图书在版编目(CIP)数据

网络安全与管理/石磊,赵慧然编著.--2版.--北京:清华大学出版社,2015

21世纪高等院校计算机网络工程专业规划教材

ISBN 978-7-302-40491-0

I. ①网… II. ①石… ②赵… III. ①计算机网络-安全技术 IV. ①TP393.08

中国版本图书馆CIP数据核字(2015)第136827号

责任编辑:魏江江 赵晓宁

封面设计:常雪影

责任校对:焦丽丽

责任印制:杨 艳

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦A座 邮 编:100084

社总机:010-62770175

邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课 件 下 载: <http://www.tup.com.cn>, 010-62795954

印 刷 者:北京富博印刷有限公司

装 订 者:北京市密云县京文制本装订厂

经 销:全国新华书店

开 本:185mm×260mm

印 张:26.25

字 数:636千字

版 次:2009年9月第1版

2015年9月第2版

印 次:2015年9月第1次印刷

印 数:1~2000

定 价:46.00元

产品编号:062505-01

前 言

21 世纪是互联网时代，网络安全的内涵发生了根本性的变化。网络安全在信息领域中的地位从一般性的防卫手段变成了非常重要的安全防御措施；网络安全技术从之前只有少部分人研究的专门领域变成了生活中无处不在的应用。当人类步入 21 世纪这一信息社会的时候，网络安全问题成为了互联网的焦点，我们每个人都时刻关注着与自身密不可分的网络系统的安全，从应用和管理的角度建立起一套完整的网络安全体系，无论对于单位还是个人都显得尤为重要。提高网络安全意识，掌握网络安全管理工具的使用逐步提到日程上来。

“网络安全与管理”是计算机、网络、软件、信息管理等专业的主要专业课，学生应从以下 4 个方面掌握网络安全的基本概念、应用技术、管理工具的使用及解决方案的设计。

（1）网络安全的基本概念

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。本书从网络安全的各个方面进行基本介绍，主要包括各种技术的概念、分类、原理、特点等知识，对于复杂而枯燥的算法和理论研究没有详细介绍，通过对这些知识的学习来理解网络安全体系中各部分之间的联系。

（2）网络安全应用技术

网络安全应用技术是指致力于解决诸如如何有效进行访问控制，以及如何保证数据传输的安全性的技术手段，主要包括网络监控技术、密码技术、病毒防御技术、防火墙技术、入侵检测技术、VPN 技术、无线网络安全技术、电子商务安全技术，以及其他的安全服务和安全机制策略。单一的网络安全技术和网络安全产品无法解决网络安全的全部问题，应根据应用需求和安全策略，综合运用各种网络安全技术以达到全面保护网络的要求。本书对于这些技术分章节地进行详细介绍。

（3）网络安全管理工具

如果想对网络安全进行综合处理，就要使用多种网络安全管理工具。同时将管理工具和系统工具配合使用，才会起到事半功倍的作用。本书的实验部分对常用的网络安全管理工具进行了相应的练习，通过学习使用这些常用的工具来理解网络安全方案的具体解决方法。

（4）网络安全解决方案设计

网络安全建设是一个系统工程，网络安全解决方案的设计直接影响工程的质量。一个完善的解决方案应该包含哪些部分、应该提供哪些服务、如何评估方案的质量都是学生需

要学习并理解的。

在本书的附录 A 中给出了一个网络安全知识手册,通过这个知识手册使学生能够快速了解目前常见的网络安全问题及其解答。

本书是一本以了解网络安全知识为目的,网络安全工具使用为重点,理论讲述为基础的系统性、应用性较强的网络安全教材。本教材摒弃了传统网络安全教材中理论过多、过难、实用性不强、理论和实践不配套、管理工具不通用等问题,旨在培养学生掌握基本网络安全理论知识和网络安全管理相结合为目的的教材。教材从应用的角度,系统地讲述了网络安全所涉及的理论及技术。以网络安全管理工具的使用能力为培养目的,通过实验演练,使学生能够综合运用书中所讲授的技术进行网络信息安全方面的实践。

本书分为理论部分 10 章和实验部分 6 章。理论部分是对网络安全基本理论和技术的详细讲解,通过这一部分使学生在理论上有一个清楚的认识。实验部分选择了目前常用的几种网络安全工具,通过对工具的使用与操作,把理论和实践联系起来,达到理解运用的目的。

本书至少需要 56 学时进行学习,其中理论授课 32 学时,实验 24 学时,在每章的后面都有习题供学生总结和复习所学的知识。

本书第 1、第 2、第 5、第 7、第 8、第 10~第 12 和第 16 章由石磊编写,第 3 章、第 4 章、实验 3 和实验 4 由赵慧然编写,第 6 章和实验 5 由肖建良编写,第 9 章由敖磊编写。由于作者水平有限,不当之处在所难免,敬请读者提出宝贵意见。

本书在编写过程中,计算机工程学院李彤院长和张坤副院长、网络工程系主任肖建良给予作者深切的关怀与鼓励,对于本书的编写提供了帮助与指导,在此表示衷心的感谢。

编 者

2015 年 3 月

目 录

第 1 章 网络安全概述	1
1.1 互联网介绍	1
1.1.1 互联网的影响	1
1.1.2 互联网的意义	2
1.1.3 我国互联网规模与使用	2
1.2 网络安全介绍	4
1.2.1 网络安全概念	4
1.2.2 网络安全的重要性	4
1.2.3 网络安全的种类	5
1.3 威胁网络安全的因素	6
1.3.1 黑客	6
1.3.2 黑客会做什么	8
1.3.3 黑客攻击	9
1.3.4 史上最危险的计算机黑客	9
1.3.5 网络攻击分类	11
1.3.6 常见网络攻击形式	11
1.4 国内网络安全的基本现状	14
1.4.1 中国网民信息安全总体现状	15
1.4.2 中国网民计算机上网安全状况	15
1.4.3 中国网民手机信息安全状况	17
1.4.4 中国网民信息安全环境	17
1.5 个人数据信息面临的网络威胁	18
1.5.1 Cookie 的使用	18
1.5.2 利用木马程序侵入计算机	19
1.5.3 钓鱼网站	20
1.5.4 监视网络通信记录	20
1.5.5 手机厂商侵犯隐私	21
1.6 常用网络安全技术简介	22
1.7 常用网络密码安全保护技巧	23
1.8 网络安全的目标	25
1.8.1 第 38 届世界电信日主题	25

1.8.2 我国网络安全的战略目标	25
1.8.3 网络安全的主要目标	25
课后习题	26

第2章 网络监控原理 31

2.1 网络监控介绍	31
2.1.1 为什么要使用网络监控	31
2.1.2 网络监控的主要目标	31
2.1.3 网络监控的分类	32
2.2 Sniffer 工具	35
2.2.1 Sniffer 介绍	35
2.2.2 Sniffer 原理	35
2.2.3 Sniffer 的工作环境	36
2.2.4 Sniffer 攻击	36
2.2.5 如何防御 Sniffer 攻击	37
2.2.6 Sniffer 的应用	38
2.3 Sniffer Pro 软件介绍	39
2.3.1 Sniffer Pro 软件简介	39
2.3.2 Sniffer Pro 软件使用	39
2.4 网路岗软件介绍	40
2.4.1 网路岗的基本功能	40
2.4.2 网路岗对上网的监控程度	40
2.4.3 网路岗安装方式	41
课后习题	42

第3章 操作系统安全 44

3.1 国际安全评价标准的发展及其联系	44
3.1.1 计算机安全评价标准	45
3.1.2 欧洲的安全评价标准	46
3.1.3 加拿大的评价标准	46
3.1.4 美国联邦准则	46
3.1.5 国际通用准则	47
3.2 我国安全标准简介	47
3.2.1 用户自主保护级	47
3.2.2 系统审计保护级	48
3.2.3 安全标记保护级	48
3.2.4 结构化保护级	49
3.2.5 访问验证保护级	49
3.3 安全操作系统的基本特征	49

3.3.1 最小特权原则.....49

3.3.2 访问控制.....50

3.3.3 安全审计功能.....51

3.3.4 安全域隔离功能.....52

3.4 Windows 操作系统安全.....52

3.4.1 远程攻击 Windows 系统的途径.....52

3.4.2 取得合法身份后的攻击手段.....53

3.4.3 Windows 安全功能.....54

3.4.4 Windows 认证机制.....56

3.4.5 Windows 文件系统安全.....57

3.4.6 Windows 的加密机制.....58

3.4.7 Windows 备份与还原.....59

3.5 Android 操作系统安全.....60

3.5.1 Android 安全体系结构.....60

3.5.2 Linux 安全性.....61

3.5.3 文件系统许可/加密.....61

3.5.4 Android 应用安全.....61

课后习题.....62

第 4 章 密码技术.....66

4.1 密码学的发展历史.....66

4.1.1 古典密码.....67

4.1.2 隐写术.....71

4.1.3 转轮密码机.....75

4.1.4 现代密码（计算机阶段）.....79

4.1.5 密码学在网络信息安全中的作用.....80

4.2 密码学基础.....81

4.2.1 密码学相关概念.....81

4.2.2 密码系统.....83

4.2.3 密码学的基本功能.....84

4.3 密码体制.....85

4.3.1 对称密码体制.....85

4.3.2 常用的对称密钥算法.....86

4.3.3 非对称密码体制.....87

4.3.4 常用公开密钥算法.....89

4.4 哈希算法.....92

4.5 MD5 简介.....93

4.6 PGP 加密软件.....95

4.6.1 PGP 的技术原理.....96

4.6.2	PGP 的密钥管理	96
4.7	软件与硬件加密技术	97
4.7.1	软件加密	97
4.7.2	硬件加密	97
4.8	数字签名与数字证书	98
4.8.1	数字签名	98
4.8.2	数字证书	99
4.9	PKI 基础知识	101
4.9.1	PKI 的基本组成	101
4.9.2	PKI 的安全服务功能	101
4.10	认证机构	103
4.10.1	CA 认证机构的功能	104
4.10.2	CA 系统的组成	104
4.10.3	国内 CA 现状	105
	课后习题	107
第 5 章	病毒技术	114
5.1	病毒的基本概念	114
5.1.1	计算机病毒的定义	114
5.1.2	计算机病毒的特点	114
5.1.3	计算机病毒分类	115
5.1.4	计算机病毒的发展史	117
5.1.5	其他的破坏行为	118
5.1.6	计算机病毒的危害性	119
5.1.7	知名计算机病毒简介	121
5.2	网络病毒	124
5.2.1	木马病毒的概念	125
5.2.2	木马的种类	127
5.2.3	木马病毒案例	129
5.2.4	木马病毒的防治	130
5.2.5	蠕虫病毒的概念	133
5.2.6	蠕虫病毒案例	134
5.2.7	蠕虫病毒的防治	140
5.2.8	病毒、木马、蠕虫比较	142
5.2.9	网络病毒的发展趋势	143
5.2.10	计算机防毒杀毒的常见误区	144
5.3	流氓软件	145
5.3.1	流氓软件定义	145
5.3.2	流氓软件的分类	146

5.3.3 流氓软件的防治	147
5.4 计算机病毒发展趋势	148
5.5 病毒检测技术	150
5.5.1 传统的病毒检测技术	150
5.6.2 基于网络的病毒检测技术	151
课后习题	152
第 6 章 防火墙技术	156
6.1 防火墙概述	156
6.1.1 防火墙的功能	156
6.1.2 防火墙的基本特性	157
6.1.3 防火墙的主要缺点	159
6.2 DMZ 简介	160
6.2.1 DMZ 的概念	160
6.2.2 DMZ 网络访问控制策略	161
6.2.3 DMZ 服务配置	162
6.3 防火墙的技术发展历程	163
6.3.1 第一代防火墙: 基于路由器的防火墙	163
6.3.2 第二代防火墙: 用户化的防火墙	163
6.3.3 第三代防火墙: 建立在通用操作系统上的防火墙	164
6.3.4 第四代防火墙: 具有安全操作系统的防火墙	164
6.4 防火墙的分类	164
6.4.1 软件防火墙	165
6.4.2 包过滤防火墙	165
6.4.3 状态检测防火墙	168
6.4.4 应用网关(代理)防火墙	170
6.5 防火墙硬件平台的发展	171
6.5.1 x86 平台	171
6.5.2 ASIC 平台	172
6.5.3 NP 平台	173
6.6 防火墙关键技术	174
6.6.1 访问控制	174
6.6.2 NAT	174
6.6.3 VPN	175
6.7 个人防火墙	176
课后习题	178
第 7 章 无线网络安全	182
7.1 无线网络安全概述	182

7.1.1	无线网络的分类	182
7.1.2	WLAN 技术	182
7.1.3	无线网络存在的安全隐患	185
7.1.4	无线网络安全的关键技术	186
7.2	WLAN 安全	187
7.2.1	WLAN 的访问控制技术	187
7.2.2	WLAN 的数据加密技术	188
7.2.3	WAPI 与 WiFi 的竞争	190
7.3	无线网络安全的防范措施	191
7.3.1	公共 WiFi 上网安全注意事项	191
7.3.2	提高无线网络安全的方法	193
	课后习题	195
第 8 章	VPN 技术	197
8.1	VPN 概述	197
8.1.1	什么是 VPN	197
8.1.2	VPN 的发展历程	198
8.1.3	VPN 的基本功能	198
8.1.4	VPN 特性	199
8.2	常用 VPN 技术	199
8.2.1	IPSec VPN	199
8.2.2	SSL VPN	204
8.2.3	MPLS VPN	208
8.2.4	SSL VPN、IPSec VPN、MPLS VPN 比较	209
8.3	VPN 采用的安全技术	210
8.3.1	隧道技术	210
8.3.2	加密技术	212
8.3.3	密钥管理技术	213
8.3.4	使用者与设备身份认证技术	213
8.4	VPN 的分类	214
8.5	VPN 技术应用	215
8.5.1	大学校园网 VPN 技术要求	215
8.5.2	某理工大学校园网 VPN 使用指南	216
	课后习题	218
第 9 章	电子商务安全	221
9.1	互联网安全概述	221
9.1.1	风险管理	221
9.1.2	电子商务安全分类	221

9.1.3	安全策略和综合安全	222
9.2	客户端的安全	222
9.2.1	Cookies	222
9.2.2	Java 小程序	224
9.2.3	JavaScript	225
9.2.4	ActiveX 控件	225
9.2.5	图形文件与插件	226
9.2.6	数字证书	227
9.2.7	信息隐蔽	228
9.3	通信的安全	229
9.3.1	对保密性的安全威胁	229
9.3.2	对完整性的安全威胁	230
9.3.3	对即需性的安全威胁	231
9.3.4	对互联网通信信道物理安全的威胁	231
9.3.5	对无线网的威胁	231
9.3.6	加密	232
9.3.7	用散列函数保证交易的完整性	234
9.3.8	用数字签名保证交易的完整性	234
9.3.9	保证交易传输	235
9.4	服务器的安全	235
9.4.1	对 WWW 服务器的安全威胁	235
9.4.2	对数据库的安全威胁	236
9.4.3	对其他程序的安全威胁	236
9.4.4	对 WWW 服务器物理安全的威胁	237
9.4.5	访问控制和认证	237
9.5	电子商务安全实例	238
	课后习题	239
第 10 章	校园网网络安全解决方案设计	241
10.1	校园网现状分析	241
10.1.1	校园网网络安全现状分析	242
10.1.2	校园网威胁成因分析	243
10.1.3	校园网安全需求	243
10.2	校园网网络安全方案设计	244
10.2.1	校园网网络安全方案设计的原则	244
10.2.2	安全设计遵循的标准	246
10.2.3	各层次的校园网络安全防范系统设计	246
10.3	校园网出口安全设计	249
10.4	统一身份认证系统的设计	249

课后习题	251
------	-----

第 11 章 实验 1 Sniffer 软件的使用 252

11.1 实验目的及要求	252
11.1.1 实验目的	252
11.1.2 实验要求	252
11.1.3 实验设备及软件	252
11.1.4 实验拓扑	252
11.1.5 交换机端口镜像配置	252
11.2 Sniffer 软件概述	253
11.2.1 功能简介	253
11.2.2 报文捕获解析	254
11.2.3 设置捕获条件	256
11.2.4 网络监视功能	257
11.3 数据报文解码详解	258
11.3.1 数据报文分层	258
11.3.2 以太网帧结构	259
11.3.3 IP 协议	260
11.4 使用 Sniffer Pro 监控网络流量	261
11.4.1 设置地址簿	261
11.4.2 查看网关流量	262
11.4.3 找到网关的 IP 地址	262
11.4.4 基于 IP 层流量	263
11.5 使用 Sniffer Pro 监控“广播风暴”	265
11.5.1 设置广播过滤器	265
11.5.2 选择广播过滤器	265
11.5.3 网络正常时的广播数据	266
11.5.4 出现广播风暴时仪表盘变化	267
11.5.5 通过 Sniffer Pro 提供的警告日志系统查看“广播风暴”	267
11.5.6 警告日志系统修改	267
11.6 使用 Sniffer Pro 获取 FTP 的账号和密码	268
实验思考题	270

第 12 章 实验 2 网路岗软件的应用 271

12.1 实验目的及要求	271
12.1.1 实验目的	271
12.1.2 实验要求	271
12.1.3 实验设备及软件	271
12.1.4 实验拓扑	271

12.2	软件的安装	272
12.2.1	系统要求	272
12.2.2	重要子目录	272
12.2.3	绑定网卡	272
12.3	选择网络监控模式	273
12.3.1	启动监控服务	273
12.3.2	检查授权状态	273
12.3.3	检查目标机器的监控状态	274
12.3.4	检查被监控的机器上网情况	274
12.3.5	封锁目标机器上网	274
12.4	各种网络监控模式	275
12.4.1	基于网卡的网络监控模式	275
12.4.2	基于 IP 的网络监控模式	276
12.5	常见系统配置	277
12.5.1	网络定义	277
12.5.2	监控项目	278
12.5.3	监控时间	279
12.5.4	端口配置	279
12.5.5	空闲 IP	279
12.5.6	深层拦截过滤	279
12.6	上网规则	280
12.6.1	上网时间	280
12.6.2	网页过滤	280
12.6.3	过滤库	281
12.6.4	上网反馈	281
12.6.5	邮件过滤	282
12.6.6	IP 过滤	282
12.6.7	封堵端口	282
12.6.8	外发尺寸	283
12.6.9	限制流量	283
12.6.10	绑定 IP	283
12.6.11	监控项目	284
12.7	日志查阅及日志报表	284
12.7.1	查阅网络活动日志	284
12.7.2	查阅外发资料日志	286
12.7.3	日志报表	287
12.8	代理服务器软件 CCProxy 的配置	287
12.8.1	CCProxy 的基本设置	288
12.8.2	客户端的设置	288

实验思考题.....	289
------------	-----

第 13 章 实验 3 Windows 操作系统的安全设置.....	290
------------------------------------	-----

13.1 实验目的及要求.....	290
13.1.1 实验目的.....	290
13.1.2 实验要求.....	290
13.1.3 实验设备及软件.....	290
13.2 禁止默认共享.....	290
13.3 服务策略.....	292
13.4 关闭端口.....	293
13.5 使用 IP 安全策略关闭端口.....	296
13.6 本地安全策略设置.....	301
13.6.1 账户策略.....	301
13.6.2 账户锁定策略.....	302
13.6.3 审核策略.....	302
13.6.4 安全选项.....	303
13.6.5 用户权利指派策略.....	303
13.7 用户策略.....	304
13.8 安全模板设置.....	305
13.8.1 启用安全模板.....	305
13.8.2 新建安全模板.....	306
13.9 组策略设置.....	306
13.9.1 关闭自动运行功能.....	307
13.9.2 禁止运行指定程序.....	307
13.9.3 防止菜单泄漏隐私.....	308
13.10 文件加密系统.....	309
13.10.1 加密文件或文件夹.....	309
13.10.2 备份加密用户的证书.....	309
13.11 文件和数据的备份.....	311
13.11.1 安排进行每周普通备份.....	311
13.11.2 安排进行每周差异备份.....	313
13.11.3 从备份恢复数据.....	314
实验思考题.....	315

第 14 章 实验 4 PGP 软件的安装与使用.....	316
-------------------------------	-----

14.1 实验目的及要求.....	316
14.1.1 实验目的.....	316

14.1.2	实验要求	316
14.1.3	实验设备及软件	316
14.2	PGP 简介与基本功能	316
14.2.1	安装	316
14.2.2	创建和设置初始用户	317
14.2.3	导出并分发公钥	318
14.2.4	导入并设置其他人的公钥	319
14.2.5	使用公钥加密文件	320
14.2.6	文件、邮件解密	321
14.3	PGPmail 的使用	321
14.3.1	PGPmail 简介	321
14.3.2	分发 PGP 公钥并发送 PGP 加密邮件	322
14.3.3	收取 PGP 加密邮件	325
14.3.4	创建自解密文档	327
14.4	PGPdisk 的使用	328
14.4.1	PGPdisk 简介	328
14.4.2	创建 PGPdisk	328
14.4.3	装配使用 PGPdisk	330
14.4.4	PGP 选项	332
	实验思考题	334
第 15 章	实验 5 防火墙的安装与使用	335
15.1	实验目的及要求	335
15.1.1	实验目的	335
15.1.2	实验要求	335
15.1.3	实验设备及软件	335
15.2	登录防火墙 Web 界面	335
15.2.1	管理员证书	335
15.2.2	管理员配置管理	337
15.2.3	管理员首次登录	337
15.2.4	登录 Web 界面	337
15.3	防火墙实现带宽控制	339
15.3.1	背景描述	339
15.3.2	实验拓扑	339
15.3.3	实验原理	339
15.3.4	实验步骤	339
15.3.5	验证测试	341
15.4	防火墙实现地址绑定	341

15.4.1	背景描述	341
15.4.2	实验拓扑	341
15.4.3	实验原理	342
15.4.4	实验步骤	342
15.4.5	验证测试	342
15.5	防火墙实现访问控制	343
15.5.1	背景描述	343
15.5.2	实验拓扑	343
15.5.3	实验原理	343
15.5.4	实验步骤	343
15.5.5	验证测试	345
15.6	防火墙实现服务保护	346
15.6.1	背景描述	346
15.6.2	实验拓扑	346
15.6.3	实验原理	346
15.6.4	实验步骤	346
15.6.5	验证测试	347
15.7	防火墙实现抗攻击	348
15.7.1	背景描述	348
15.7.2	实验拓扑	348
15.7.3	实验原理	348
15.7.4	实验步骤	348
15.7.5	验证测试	350
15.8	防火墙实现链路负载	350
15.8.1	背景描述	350
15.8.2	实验拓扑	350
15.8.3	实验原理	350
15.8.4	实验步骤	350
	实验思考题	352
第 16 章 实验 6 VPN 服务的配置与使用		353
16.1	实验目的及要求	353
16.1.1	实验目的	353
16.1.2	实验要求	353
16.1.3	实验设备及软件	353
16.1.4	实验拓扑	353
16.2	实验内容及步骤	353
16.2.1	应用情景	353
16.2.2	PPTP 协议实现 VPN 服务	354