

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

石磊 赵慧然 编著

可下载教学资料
<http://www.tup.tsinghua.edu.cn>

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

石磊 赵慧然 编著

清华大学出版社
北京

内 容 简 介

本书是根据作者多次讲授“网络安全”课程的教学经验以及进行实验指导的体会编写而成的。本书从实践出发,以基本理论的应用和网络安全工具的使用为中心,以理论讲述为基础,避免了一些传统网络安全教材理论过多、理论过难、操作性不强、理论和实际联系不紧的问题,重点介绍网络安全领域的最新问题和工具的运用。

全书分理论部分9章和实验部分6章。理论部分是对网络安全体系结构和技术的详细讲解,通过这一部分使学生在理论上有一个清楚的认识,每章后面都有各类习题供学生总结和复习所学的知识;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,达到理解运用的目的。附录中还提供了一个完整的应用系统网络安全解决方案,将网络安全理论知识与现实的工程项目综合起来,以便学生“看懂、学会、用上”。

本书可作为网络工程、计算机、信息安全等专业本科生的教科书与实验教材,也可供从事相关专业的教学、科研和工程人员参考。

本书配套的电子课件可从清华大学出版社网站(<http://www.tup.com.cn>)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 13701121933

图书在版编目(CIP)数据

网络安全与管理/石磊,赵慧然编著. —北京:清华大学出版社,2009.9

(21世纪高等院校计算机网络工程专业规划教材)

ISBN 978-7-302-20561-6

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

中国版本图书馆 CIP 数据核字(2009)第 151076 号

责任编辑:索 梅 徐跃进

责任校对:白 蕾

责任印制:孟凡玉

出版发行:清华大学出版社

地 址:北京清华大学学研大厦 A 座

<http://www.tup.com.cn>

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

印 装 者:北京国马印刷厂

经 销:全国新华书店

开 本:185×260 印 张:18.75 字 数:448 千字

版 次:2009 年 9 月第 1 版 印 次:2009 年 9 月第 1 次印刷

印 数:1~4000

定 价:28.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。联系电话:(010)62770177 转 3103 产品编号:033447-01

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普遍应用。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”是计算机专业、网络工程专业的主要专业课,学生应从四个方面掌握网络安全的基本概念、应用技术、管理工具的使用以及解决方案的设计。

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;从广义上说,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了基本的介绍,这些介绍主要包括各种技术的概念、分类、原理、特点等知识,而对于复杂而枯燥的算法和理论研究没有作详细介绍,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,及其他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了详细介绍。

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。在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到工程的质量。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。在附录 A 中给出了一个网络安全解决方案,通过这个方案使学生理解如何针对一个真实的网络设计安全方案。

本书是一本以网络安全管理应用为目的,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,以培养学生掌握基本网络安全理论知识和网络应用管理相结合为目的。教材从应用的角度系统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(9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。

本书可作为网络工程、计算机、信息安全等专业本科生的教科书,也可供从事相关专业的教学、科研和工程人员参考。

本书至少需要 48 学时来进行学习,其中理论授课 24 学时,实验 24 学时,在每章的后面都有习题以供学生总结和复习所学的知识,并在附录中给出了习题答案。

本书由石磊主编,其中第 3 章、第 4 章和实验 3 由赵慧然编写。由于作者水平有限,不当之处敬请读者提出宝贵意见。

在本书编写过程中,计算机工程学院李彤院长、张坤副院长、网络工程系主任肖建良给予了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

2009 年 7 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 互联网网民规模	2
1.2 网络安全介绍	3
1.2.1 网络安全吗	3
1.2.2 网络为什么不安全	3
1.2.3 网络安全防范	5
1.3 十大威胁企业安全的网络危险行为	6
1.4 常用网络密码安全保护技巧	7
1.5 威胁网络安全的因素	8
1.5.1 黑客	8
1.5.2 黑客会做什么	9
1.5.3 网络攻击分类	10
1.5.4 常见网络攻击形式	11
1.6 网络安全的目标	13
1.6.1 第 38 届世界电信日主题	13
1.6.2 我国网络安全的战略目标	13
1.6.3 网络安全的主要目标	13
课后习题	14
第 2 章 网络监控软件原理	16
2.1 网络监控软件介绍	16
2.1.1 为什么要使用网络监控软件	16
2.1.2 网络监控软件主要目标	16
2.1.3 网络监控软件的分类	17
2.2 Sniffer 工具介绍	18
2.2.1 Sniffer 的原理	18
2.2.2 Sniffer 的分类	18
2.2.3 网络监听的目的	18

2.2.4	Sniffer 的应用	19
2.2.5	Sniffer 的工作原理	19
2.3	Sniffer 的工作环境	20
2.4	Sniffer Pro 软件使用	21
2.6	网路岗工具介绍	22
2.6.1	网路岗的基本功能	22
2.6.2	网路岗对上网的监控能做到什么程度	22
2.6.3	网路岗安装方式	22
课后习题		24
第 3 章 操作系统安全		25
3.1	国际安全评价标准的发展及其联系	25
3.1.1	计算机安全评价标准	26
3.1.2	欧洲的安全评价标准	27
3.1.3	加拿大的评价标准	27
3.1.4	美国联邦准则	27
3.1.5	国际通用准则	27
3.2	我国安全标准简介	27
3.2.1	第一级 用户自主保护级	28
3.2.2	第二级 系统审计保护级	28
3.2.3	第三级 安全标记保护级	29
3.2.4	第四级 结构化保护级	29
3.2.5	第五级 访问验证保护级	30
3.3	安全操作系统的基本特征	30
3.3.1	最小特权原则	30
3.3.2	自主访问控制和强制访问控制	30
3.3.3	安全审计功能	31
3.3.4	安全域隔离功能	32
3.4	Windows 2003 的安全设置	32
3.4.1	Windows 安全漏洞及其解决建议	32
3.4.2	Windows 2003 的认证机制	32
3.4.3	Windows 2003 账号安全	33
3.4.4	Windows 2003 文件系统安全	33
3.4.5	Windows 文件保护	34
3.4.6	Windows 2003 的加密机制	35
3.4.7	Windows 2003 的安全配置	36
3.4.8	Windows 2003 文件和数据的备份	37
课后习题		39

第4章 密码技术	41
4.1 密码学的起源	41
4.2 密码学中的重要术语	45
4.3 密码体制	45
4.3.1 对称密码体制	46
4.3.2 非对称密码体制	46
4.4 哈希算法	47
4.5 著名密码体系	48
4.5.1 分组密码体系	48
4.5.2 DES 数据加密标准	50
4.5.3 公开密钥密码体制	50
4.5.4 公开密钥算法	52
4.6 PGP 加密软件	52
4.6.1 PGP 的技术原理	54
4.6.2 PGP 的密钥管理	54
4.7 软件与硬件加密技术	55
4.7.1 软件加密	55
4.7.2 硬件加密	55
4.8 数字签名与数字证书	56
4.8.1 数字签名	56
4.8.2 数字证书	57
4.9 PKI 基础知识	59
4.9.1 PKI 的基本组成	59
4.9.2 PKI 的安全服务功能	59
4.10 认证机构	61
4.10.1 CA 认证机构的功能	61
4.10.2 CA 系统的组成	62
4.10.3 国内 CA 现状	63
课后习题	65
第5章 病毒技术	68
5.1 病毒的基本概念	68
5.1.1 计算机病毒的定义	68
5.1.2 计算机病毒的特点	68
5.1.3 计算机病毒的分类	69
5.1.4 计算机病毒的发展史	71
5.1.5 其他破坏行为	72
5.1.6 计算机病毒的危害性	73

5.2 网络病毒	73
5.2.1 木马病毒的概念	75
5.2.2 木马病毒案例	76
5.2.3 蠕虫病毒的概念	77
5.2.4 蠕虫病毒案例	80
5.2.5 病毒、木马、蠕虫比较	83
5.2.6 网络病毒的发展趋势	84
5.3 病毒检测技术	85
5.3.1 传统的病毒检测技术	85
5.3.2 基于网络的病毒检测技术	86
课后习题	87
第6章 防火墙技术	89
6.1 防火墙概述	89
6.1.1 防火墙的功能	89
6.1.2 防火墙的基本特性	90
6.2 DMZ 简介	92
6.2.1 DMZ 的概念	92
6.2.2 DMZ 网络访问控制策略	93
6.2.3 DMZ 服务配置	93
6.3 防火墙的技术发展历程	94
6.3.1 第一代防火墙：基于路由器的防火墙	94
6.3.2 第二代防火墙：用户化的防火墙	95
6.3.3 第三代防火墙：建立在通用操作系统上的防火墙	95
6.3.4 第四代防火墙：具有安全操作系统的防火墙	95
6.4 防火墙的分类	96
6.4.1 软件防火墙	96
6.4.2 包过滤防火墙	96
6.4.3 状态检测防火墙	98
6.4.4 应用代理网关防火墙	99
6.5 防火墙硬件平台的发展	100
6.5.1 X86 平台	100
6.5.2 ASIC 平台	101
6.5.3 NP 平台	102
6.6 防火墙关键技术	103
6.6.1 访问控制	103
6.6.2 网络地址转换	104
6.6.3 虚拟专用网	105
课后习题	105

第 7 章 入侵检测系统	107
7.1 入侵检测系统是什么	107
7.2 入侵检测基本原理	108
7.3 入侵检测系统分类	109
7.3.1 按数据来源分类	109
7.3.2 按分析技术分类	111
7.4 入侵检测系统模型	113
7.4.1 入侵检测系统的 CIDF 模型	113
7.4.2 Denning 的通用入侵检测系统模型	113
7.5 分布式入侵检测系统	114
7.6 入侵检测技术的发展趋势	115
课后习题	116
第 8 章 VPN 技术	117
8.1 什么是虚拟专用网	117
8.2 VPN 的基本功能	117
8.3 VPN 所需的安全技术	118
8.3.1 隧道技术	118
8.3.2 加密技术	120
8.3.3 密钥分发和管理	121
8.3.4 身份认证技术	121
8.4 VPN 的分类	121
8.5 IP 安全协议	122
8.5.1 IPSec 的安全特性	123
8.5.2 基于电子证书的公钥认证	123
8.5.3 预置共享密钥认证	123
8.5.4 公钥加密	124
8.5.5 hash 函数和数据完整性	124
8.5.6 加密和数据可靠性	124
8.5.7 密钥管理	125
8.5.8 IPSec 的好处	125
8.6 安全套接层	125
8.7 SSL VPN 与 IPSec VPN 安全比较	127
8.8 VPN 技术应用案例	128
8.8.1 大学校园网 VPN 技术要求	128
8.8.2 某理工大学校园网 VPN 使用指南	129
课后习题	131

第9章 网络安全解决方案设计	133
9.1 网络安全方案概念	133
9.2 评价网络安全方案的质量	133
9.3 网络安全方案的框架	134
9.4 网络安全需求分析	134
9.4.1 项目要求	134
9.4.2 工作任务	134
9.5 解决方案设计	135
9.5.1 施工方公司背景简介	135
9.5.2 安全风险分析	135
9.5.3 解决方案	135
9.5.4 实施方案	136
9.5.5 技术支持和服务承诺	136
9.5.6 产品报价	136
9.5.7 产品介绍	136
9.5.8 第三方检测报告	136
9.5.9 安全技术培训	136
课后习题	137
第10章 实验1 Sniffer 软件的使用	138
10.1 实验目的及要求	138
10.1.1 实验目的	138
10.1.2 实验要求	138
10.1.3 实验设备及软件	138
10.1.4 实验拓扑	138
10.1.5 交换机端口镜像配置	138
10.2 Sniffer 软件概述	139
10.2.1 功能简介	139
10.2.2 报文捕获解析	140
10.2.3 设置捕获条件	141
10.2.4 网络监视功能	143
10.3 数据报文解码详解	144
10.3.1 数据报文分层	144
10.3.2 以太网帧结构	144
10.3.3 IP 协议	145
10.4 使用 Sniffer Pro 监控网络流量	146
10.4.1 设置地址簿	146
10.4.2 查看网关流量	147

10.4.3	找到网关的 IP 地址	147
10.4.4	基于 IP 层流量	148
10.5	使用 Sniffer Pro 监控“广播风暴”	150
10.5.1	设置广播过滤器	150
10.5.2	选择广播过滤器	151
10.5.3	网络正常时的广播数据	151
10.5.4	出现广播风暴时,仪表盘变化	152
10.5.5	通过 Sniffer Pro 提供的警告日志系统查看“广播风暴”	152
10.5.6	警告日志系统修改	153
10.6	使用 Sniffer Pro 获取 FTP 的账号和密码	153
	实验思考题	155
第 11 章	实验 2 网路岗软件的应用	156
11.1	实验目的及要求	156
11.1.1	实验目的	156
11.1.2	实验要求	156
11.1.3	实验设备及软件	156
11.1.4	实验拓扑	156
11.2	软件的安装	157
11.2.1	系统要求	157
11.2.2	重要子目录	157
11.2.3	绑定网卡	157
11.3	选择网络监控模式	158
11.3.1	启动监控服务	158
11.3.2	检查授权状态	158
11.3.3	检查目标机器的监控状态	159
11.3.4	查被监控的机器上网情况	159
11.3.5	封锁目标机器上网	159
11.4	各种网络监控模式	160
11.4.1	基于网卡的网络监控模式	160
11.4.2	基于 IP 的网络监控模式	162
11.5	常见系统配置	162
11.5.1	网络定义	162
11.5.2	监控项目	163
11.5.3	监控时间	164
11.5.4	端口配置	164
11.5.5	空闲 IP	164
11.5.6	深层拦截过滤	164
11.6	上网规则	165

11.6.1	上网时间	165
11.6.2	网页过滤	165
11.6.3	过滤库	166
11.6.4	上网反馈	166
11.6.5	邮件过滤	167
11.6.6	IP 过滤	167
11.6.7	封堵端口	167
11.6.8	外发尺寸	168
11.6.9	限制流量	168
11.6.10	绑定 IP	168
11.6.11	监控项目	169
11.7	日志查阅及日志报表	169
11.7.1	查阅网络活动日志	169
11.7.2	查阅外发资料日志	170
11.7.3	日志报表	172
	实验思考题	172

第 12 章 实验 3 Windows 操作系统的安全设置

173

12.1	实验目的及要求	173
12.1.1	实验目的	173
12.1.2	实验要求	173
12.1.3	实验设备及软件	173
12.2	有效的防范攻击措施	173
12.2.1	计算机常见的被入侵方式	173
12.2.2	有效防范攻击的手段	173
12.3	禁止默认共享	174
12.4	利用 IP 安全策略关闭端口	176
12.5	设置策略项,做好内部防御	178
12.5.1	服务策略——禁用服务	178
12.5.2	审核策略	179
12.5.3	安全选项	180
12.5.4	启用安全模板	180
12.5.5	新建安全模板	181
12.5.6	用户权利指派策略	181
12.5.7	账户锁定策略	182
12.5.8	用户策略	183
12.5.9	关闭自动运行功能	183
12.6	文件加密系统	184
12.6.1	加密文件或文件夹	184

12.6.2	备份加密用户的证书	184
12.7	文件和数据的备份	186
12.7.1	安排进行每周普通备份	186
12.7.2	安排进行每周差异备份	190
12.7.3	从备份恢复数据	190
12.8	利用 MBSA 检查和配置系统安全	191
	实验思考题	192
第 13 章	实验 4 PGP 软件的安装与使用	193
13.1	实验目的及要求	193
13.1.1	实验目的	193
13.1.2	实验要求	193
13.1.3	实验设备及软件	193
13.2	PGP 简介与基本功能	193
13.2.1	安装	193
13.2.2	创建和设置初始用户	194
13.2.3	导出并分发你的公钥	196
13.2.4	导入并设置其他人的公钥	196
13.2.5	使用公钥加密文件	197
13.2.6	文件、邮件解密	198
13.3	PGPmail 的使用	199
13.3.1	PGPmail 简介	199
13.3.2	分发 PGP 公钥并发送 PGP 加密邮件	199
13.3.3	收取 PGP 加密邮件	203
13.3.4	创建自解密文档	205
13.4	PGPdisk 的使用	206
13.4.1	PGPdisk 简介	206
13.4.2	创建 PGPdisk	206
13.4.3	装配使用 PGPdisk	208
13.4.4	PGP 选项	211
	实验思考题	213
第 14 章	实验 5 防火墙的安装与使用	214
14.1	实验目的及要求	214
14.1.1	实验目的	214
14.1.2	实验要求	214
14.1.3	实验设备及软件	214
14.2	登录防火墙 Web 界面	214
14.2.1	管理员证书	214

14.2.2	管理员配置管理	216
14.2.3	管理员首次登录	216
14.2.4	登录 Web 界面	216
14.3	防火墙实现带宽控制	218
14.3.1	背景描述	218
14.3.2	实验拓扑	218
14.3.3	实验原理	218
14.3.4	实验步骤	218
14.3.5	验证测试	220
14.4	防火墙实现地址绑定	220
14.4.1	背景描述	220
14.4.2	实验拓扑	220
14.4.3	实验原理	221
14.4.4	实验步骤	221
14.4.5	验证测试	222
14.5	防火墙实现访问控制	222
14.5.1	背景描述	222
14.5.2	实验拓扑	222
14.5.3	实验原理	222
14.5.4	实验步骤	222
14.5.5	验证测试	224
14.6	防火墙实现服务保护	225
14.6.1	背景描述	225
14.6.2	实验拓扑	225
14.6.3	实验原理	225
14.6.4	实验步骤	225
14.6.5	验证测试	226
14.7	防火墙实现抗攻击	227
14.7.1	背景描述	227
14.7.2	实验拓扑	227
14.7.3	实验原理	227
14.7.4	实验步骤	227
14.7.5	验证测试	229
14.8	防火墙实现链路负载	229
14.8.1	背景描述	229
14.8.2	实验拓扑	229
14.8.3	实验原理	229
14.8.4	实验步骤	229
	实验思考题	230

第 15 章 实验 6 VPN 设备的使用与配置	231
15.1 实验目的及要求	231
15.1.1 实验目的	231
15.1.2 实验要求	231
15.1.3 实验设备及软件	231
15.1.4 实验拓扑	231
15.2 锐捷 VPN 命令行操作	231
15.2.1 系统管理模式	231
15.2.2 管理员	232
15.2.3 串口管理	232
15.3 IPSec VPN 通信实验	232
15.3.1 设备的初始化设置	232
15.3.2 VPN 管理器的安装	233
15.3.3 VPN 首次配置	235
15.3.4 VPN 管理平台登录	236
15.3.5 网络接口设置	237
15.3.6 配置 IPSec VPN 隧道	237
15.3.7 RG-SRA 程序的使用	242
15.4 采用 USB-Key 的数字证书方式进行 VPN 通信	244
15.4.1 在远程用户管理中配置“认证参数”	244
15.4.2 证书管理系统 RG_CMS 的使用	244
15.4.3 RG-SRA 程序的使用	246
实验思考题	248
参考文献	249
附录 A 腾飞科技集团公司(公司名为虚构)网络信息系统的安全方案建议书	250
A1 需求分析	251
A1.1 网络安全集中管理的业务目标	251
A1.2 网络安全现状及需求说明	251
A1.3 需求分析及设计思路	251
A1.3.1 需求分析	251
A1.3.2 设计思路	252
A2 总体方案设计	253
A2.1 方案综述	253
A2.2 网络安全中心设计	253
A2.3 边界及互联安全设计	254
A2.4 分支机构网络安全设计	254

A3	网络安全中心的建设	255
A3.1	Windows 域建设	255
A3.2	桌面防病毒部署	255
A3.2.1	方案设计	255
A3.2.2	产品选型	256
A3.3	内网安全及管理	256
A3.3.1	方案设计	256
A3.3.2	产品选型	256
A3.4	文件保护及安全审计	257
A3.4.1	方案设计	257
A3.4.2	产品选型	257
A3.5	企业数字身份管理系统	258
A3.5.1	方案设计	258
A3.5.2	产品选型	258
A3.6	强身份认证	259
A3.7	企业安全管理平台	259
A3.7.1	方案设计	259
A3.7.2	产品选型	260
A3.8	安全管理体系(管理制度)	260
A3.8.1	安全管理体系(管理制度)样例	260
A3.8.2	总政策样例	260
A3.8.3	具体安全政策样例	261
A3.8.4	安全管理流程样例	262
A3.9	安全服务	262
A3.9.1	安全评估	262
A3.9.2	安全加固	265
A3.9.3	安全培训	265
A3.9.4	紧急响应服务	266
A3.10	账号整合(可选)	266
A4	网络安全中心与分支机构互联边界安全	266
A4.1	防火墙部署	266
A4.1.1	方案设计	266
A4.1.2	产品选型	267
A4.2	入侵检测及防护部署	267
A4.2.1	方案设计	267
A4.2.2	产品选型	268
A4.3	流量分析部署	268
A4.3.1	方案设计	268
A4.3.2	产品选型	268