



新一代高职教育信息通信规划教材

计算机网络与信息安全

JISUANJI WANGLUO YU XINXI ANQUAN

梁军 毛振寰 编著



北京邮电大学出版社
www.buptpress.com

新一代高职教育信息通信规划教材

计算机网络与信息安全

梁 军 毛振寰 编著

北京邮电大学出版社

·北京·

内 容 提 要

随着互联网的飞速发展,计算机安全已经成为一个潜在的巨大问题,而且逐渐影响到网络的发展。

计算机的安全性是一个涉及面很广泛的问题(还会涉及计算机犯罪),其中包括访问控制、攻击与防御、信息的保护、病毒的防治等问题。

本书从实用性出发,站在系统管理员、安全管理员或安全审计人员的角度,深入探讨了各种安全隐患的存在及其解决方案,给出了在各种安全事件发生的情况下应该采取的应对方法和措施,同时书中包含了20个典型的实验供演示和练习之用。

图书在版编目(CIP)数据

计算机网络与信息安全/梁军,毛振寰编著. —北京:北京邮电大学出版社,2005

ISBN 7-5635-0951-8

I. 计... II. ①梁... ②毛... III. ①电子计算机—安全技术②计算机病毒—防治 IV. TP309

中国版本图书馆 CIP 数据核字(2005)第 106870 号

书 名: 计算机网络与信息安全

作 者: 梁 军 毛振寰

责任编辑: 王晓丹

出 版 者: 北京邮电大学出版社(北京市海淀区西土城路 10 号) 邮编:100876

发行部电话:(010)62282185 62283578(传真)

电子信箱: publish@bupt.edu.cn

经 销: 各地新华书店

印 刷: 北京源海印刷有限责任公司

开 本: 787 mm×1 092 mm 1/16

印 张: 16

字 数: 389 千字

印 数: 1—3 000 册

版 次: 2005 年 5 月第 1 版 2005 年 5 月第 1 次印刷

ISBN 7-5635-0951-8/TP·126

定价: 25.00 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·

新一代高职教育信息通信规划教材 编委会

主任：肖传统

副主任：张孝强 张干生 严潮斌

委员：(以姓氏笔画为序)

王立平 王巧明 王晓军 王颖 宁帆

刘翠霞 李飞 李文海 苏开荣 吴正书

李转年 迟学芬 吴瑞萍 张一鸣 张敏华

张献居 张新瑛 杨泉 顾生华 孟祥真

徐淳宁 曹晓川 蒋青泉 傅德月

秘书：王琴秋

编委会的话

随着我国高等教育规模的扩大和信息通信产业的迅速发展,通信院校专业课程教学面临着新的标准和新的要求。作为普通高等教育组成部分的高等职业教育在新的教学理念和信息化手段影响下,对教材这一重要的教学要素提出了新的需求。

教材已经成为传授规范知识和方法、完成教学大纲的主要载体。教材的编写质量和使用状况亦体现了任课教师的教学水准,成为课程建设和学科发展水平的重要标志,成为学校的强势学科和特色专业走向成熟的主要表现。所以,各级学校领导和教师历来十分重视教材建设。

近年来,高等职业教育发展迅猛,其宏观规模发生了历史性变化。为适应社会的需求,高等职业教育的教学模式、教学方法都应不断进行改革。与此相适应,需对高职教材进行重新调整与定位,突出自身的特色。

20世纪,原邮电高等函授教学指导委员会讨论审批、推荐出版了一大批教材。现在,它们的成员单位和部分成员重新组织在一起,成立了“新一代高职教育信息通信规划教材”编委会,开始酝酿教材建设的规划和思路。在这个编委会里,有通信职业技术学院的领导和教师,也有原邮电院校成人教育的专家教授。大家纷纷响应,且群策群力,就是为了一个共同的愿望:通过信息交流,统一规划,共同编写、出版和使用一批优秀教材。这样的优秀教材应体现现代教育观念,反映信息通信技术发展的最新成果,具有先进性、科学性和教学的适用性,充分体现高职教育的特征和本质要求,充分运用现代教育技术、手段与方法。该套教材将以立体化形式和配套教学资源完整地呈现出来。

编委会汇集了长沙通信职业技术学院、广东邮电职业技术学院、四川邮电职业技术学院、南京邮电学院吴江职业技术学院、石家庄邮电职业技术学院、黑龙江信息技术职业学院、河北省通信职业技术学院、北京邮电大学网络教育学院、南京邮电学院继续教育学院、重庆邮电学院成人教育学院、西安邮电学院继续教育学院、吉林大学通信学院的领导及教学一线的教师。大家在一起对高职

教育中的教学及教材建设进行了认真的研讨,一致认为:目前,通信行业的高职院校大部分是在原中专学校的基础上发展起来的,各校在教学中遇到的一个带有共性的问题,就是缺少适合于高职教育的教材,大部分院校都在借用本科甚至中专的教材,这种状况亟待改变。因而高职教材成为各院校教材建设的重中之重。高职教材的建设应从两方面齐头并进:一方面针对专业课和基础课教材以适用性为特征,强调简便易行;另一方面是着手进行实训课程教材的编写。各院校,尤其是各邮电职业技术学院将携手推出“新一代高职教育信息通信规划教材”。

“新一代高职教育信息通信规划教材”将陆续与广大教师和学生见面,它凝聚着编委会成员及所在院校领导和专家的辛勤努力,凝聚着一批优秀教师和作者的智慧结晶,也许其中有些内容因时间仓促而略显瑕疵,但我们相信,有各个院校教师的关爱和斧正,有广大读者的建议和支持,我们所付出的努力必将得到越来越多的人们的赞赏和承认。

“新一代高职教育信息通信规划教材”编委会

2003年12月

目 录

网络安全与防火墙篇

第 1 章 网络安全概念

1.1 引言	3
1.2 安全的定义	4
1.3 黑客活动	4
1.4 风险	5
1.5 百分之百的安全	5
1.6 安全即寻求平衡	5
1.7 建立有效的安全矩阵	6
1.8 保护资源	6
1.8.1 终端用户资源	6
1.8.2 网络资源	7
1.8.3 服务器资源	7
1.8.4 信息存储资源	7
1.9 黑客的分类	7
1.9.1 偶然的破坏者	8
1.9.2 坚定的破坏者	8
1.9.3 间谍	8
1.10 安全标准	8
1.10.1 安全服务	9
1.10.2 安全机制	9
1.10.3 额外的安全标准	9
本章小结	10
问题讨论	10

第 2 章 安全的基本元素

2.1 引言	10
2.2 安全的基本元素	11

2.3 安全策略	11
2.3.1 系统分类	12
2.3.2 明智地为系统分类	12
2.3.3 资源优先级划分	13
2.3.4 指定危险因数	13
2.3.5 定义可接受和不可接受活动	13
2.3.6 定义教育标准	14
2.3.7 谁负责管理策略	15
2.4 加密	15
2.5 认证	15
2.6 特殊的认证技术	17
2.7 访问控制	18
2.7.1 访问控制列表	18
2.7.2 执行控制列表	18
2.8 审计	19
2.8.1 被动式和主动式审计	19
2.8.2 安全的权衡考虑和缺点	19
本章小结	19
问题讨论	19

第3章 应用加密

3.1 引言	20
3.2 加密的优势	20
3.3 加密强度	20
3.4 建立信任关系	21
3.5 对称加密	22
3.6 对称加密算法	23
3.6.1 数据加密标准	23
3.6.2 Triple DES	23
3.6.3 RSA 安全公司的对称算法	23
3.6.4 Blowfish and Twofish	24
3.6.5 Skiack and MARS	24
3.6.6 高级加密标准	24
3.7 非对称加密	24
3.8 HASH 加密	25
3.8.1 HASH 算法	25
3.8.2 安全 HASH 算法(SHA)	26
3.9 签名	26
3.10 应用加密的执行过程	27

3.10.1 电子邮件(E-mail)	27
3.10.2 加密文件	29
3.10.3 Web 服务器加密	29
3.10.4 网络级协议	29
3.11 虚拟专用网络(VPN)协议	30
3.11.1 PPTP 与 IPSec 在安全性上的比较	30
3.11.2 保护与服务	30
3.12 公钥体系结构(PKI)	31
3.12.1 PKI 标准	31
3.12.2 PKI 术语	31
本章小结	32
问题讨论	32

第 4 章 典型的攻击方式及安全规则

4.1 引言	33
4.2 安全攻击类型	33
4.2.1 前门攻击和暴力攻击	33
4.2.2 BUG 和后门	34
4.2.3 社交工程和非直接攻击	34
4.2.4 拒绝服务攻击	35
4.3 网络安全实施的通用规则	36
4.3.1 努力成为“偏执狂”	36
4.3.2 必须有完整的安全策略	36
4.3.3 不要采用单独的系统或技术	37
4.3.4 部署公司范围的强制策略	37
4.3.5 提供培训	38
4.3.6 根据需要购置设备	38
4.3.7 识别安全的商业问题	38
4.3.8 考虑物理安全	39
本章小结	39
问题讨论	40

第 5 章 协议层安全

5.1 引言	40
5.2 TCP/IP 和网络安全	40
5.3 TCP/IP 协议集和 OSI 参考模型	41
5.3.1 网络接入层	41
5.3.2 网络层	41
5.3.3 传输层	42

5.3.4 应用层.....	44
本章小结	46
问题讨论	47

第6章 保护资源

6.1 引言.....	47
6.2 安全保护的实施过程.....	47
6.3 保护 TCP/IP 的相关服务.....	49
6.3.1 Web Server	49
6.3.2 文件传输协议服务器(FTP).....	51
6.3.3 简单邮件传输协议(SMTP)	51
6.4 测试和评估.....	52
6.4.1 测试评估系统.....	52
6.4.2 安全测试软件.....	53
本章小结	54
问题讨论	54

第7章 防火墙基础

7.1 引言.....	54
7.2 防火墙技术现状.....	54
7.3 防火墙的定义和描述.....	55
7.4 防火墙的任务.....	55
7.5 防火墙术语.....	56
7.6 防火墙默认的配置.....	58
7.6.1 包过滤的概念和功能.....	58
7.6.2 包过滤的规则和字段.....	59
7.6.3 包过滤的优点和缺点.....	60
7.7 状态多层检测.....	60
7.8 代理服务器.....	61
7.8.1 代理服务器的用处.....	61
7.8.2 代理服务器的基本类型.....	61
7.8.3 代理服务器的优点.....	62
7.8.4 代理服务器的缺点.....	63
7.9 防火墙的一些高级特性.....	63
7.9.1 认证.....	64
7.9.2 日志和告警.....	64
7.10 远程访问和虚拟专用网	64
本章小结	65
问题讨论	65

第 8 章 防火墙体系结构

8.1 引言	65
8.2 防火墙策略和目的	65
8.3 建立防火墙	66
8.4 堡垒主机的类型	67
8.5 硬件采购问题	68
8.6 操作系统、服务和进程	68
8.7 防火墙设计	69
本章小结	71
问题讨论	71

第 9 章 检测和迷惑黑客

9.1 引言	72
9.2 前期检测	72
9.2.1 自动安全扫描	72
9.2.2 使用登陆脚本	72
9.2.3 自动审计分析	73
9.2.4 Checksum 分析	73
9.3 迷惑黑客	73
9.3.1 假账号	74
9.3.2 假文件	74
9.3.3 Tripwire 和 Jails	74
9.4 惩罚黑客	75
9.4.1 方法	75
9.4.2 工具	75
本章小结	76
问题讨论	76

第 10 章 事件响应

10.1 引言	76
10.2 安全事件响应的具体措施	76
10.3 分析和学习	78
本章小结	78
问题讨论	78

操作系统安全篇

第 11 章 网络安全基础

11.1 引言	81
---------	----

11.2	安全的定义	81
11.3	评估标准	82
11.4	可信任计算机系统评估标准	82
11.4.1	C2级和F-C2,E2级要求	83
11.4.2	公共标准(CC)	83
11.4.3	其他重要概念	83
11.5	安全等级	84
11.6	安全机制	84
11.6.1	特殊安全机制	84
11.6.2	广泛安全机制	85
11.7	安全管理	85
11.8	Windows 2000 的安全	85
11.8.1	安全结构	86
11.8.2	安全组件	86
11.8.3	对象	86
11.8.4	安全的组成部分	87
11.8.5	安全子系统	88
11.9	Unix 的安全	89
11.9.1	一般 Unix 的安全漏洞	89
11.9.2	缓冲区溢出	90
	本章小结	90
	问题讨论	91

第 12 章 账号安全

12.1	引言	91
12.2	关于账号密码	91
12.2.1	密码的重要性	91
12.2.2	Windows 2000 下的密码安全	92
12.2.3	Unix 下的密码安全	92
12.3	Windows 2000 账号安全	92
12.4	Unix 账号安全	93
	本章小结	97
	问题讨论	97

第 13 章 文件系统安全

13.1	引言	97
13.2	Windows 2000 文件系统安全	98
13.3	Unix 文件系统安全	100
13.3.1	Unix 下的文件格式	100
13.3.2	常用命令	100

本章小结·····	104
问题讨论·····	104
第 14 章 评估风险	
14.1 引言·····	105
14.2 安全威胁·····	105
14.3 攻击的类型·····	106
14.4 Windows 2000 的安全风险 ·····	107
14.5 Unix 的安全风险 ·····	107
14.5.1 rlogin 命令 ·····	107
14.5.2 NIS 的安全·····	108
14.5.3 NFS 的安全问题 ·····	111
14.6 系统扫描·····	112
本章小结·····	112
问题讨论·····	113
第 15 章 降低风险	
15.1 引言·····	113
15.2 patches 和 fixes ·····	113
15.2.1 Microsoft service packs ·····	114
15.2.2 Red Hat Linux 勘误表 ·····	114
15.3 注册表的安全性·····	114
15.3.1 注册表结构·····	115
15.3.2 注册表访问控制·····	116
15.3.3 注册表的审核·····	116
15.4 禁止和删除 Windows 2000 中不必要的服务 ·····	116
15.5 加强网络连接安全·····	117
15.6 其他配置的更改·····	118
15.7 禁止和删除 Unix 中不必要的服务 ·····	120
15.8 TCP Wrapper ·····	121
15.9 MD5 ·····	122
15.10 Windows 2000 中的日志记录 ·····	123
本章小结·····	124
问题讨论·····	124

安全审计、攻击和威胁分析篇

第 16 章 安全审计

16.1 引言·····	127
16.2 安全审计人员的职责·····	127

16.2.1 从安全管理者的角度考虑	127
16.2.2 从黑客的角度考虑	128
16.3 安全审计人员的工作	128
16.3.1 内部威胁分析	129
16.3.2 风险评估	129
本章小结	132
问题讨论	133

第 17 章 侦查手段和工具

17.1 引言	133
17.2 安全扫描	133
17.3 企业级的审计工具	138
17.4 社会工程	141
17.5 获得信息	141
17.5.1 网络级别的信息	142
17.5.2 主机级别的信息	142
17.5.3 合法和非法的网络工具	142
本章小结	143
问题讨论	143

第 18 章 服务器渗透和攻击技术审计

18.1 引言	143
18.2 常见攻击类型和特征	143
18.2.1 常见的攻击方法	144
18.2.2 容易遭受攻击的目标	144
18.3 服务器安全	145
18.3.1 Web 页面涂改	145
18.3.2 邮件服务	145
18.3.3 名称服务	145
18.4 审计系统 bug	146
18.4.1 审计 trap door 和 root kit	146
18.4.2 审计和后门程序	147
18.5 审计拒绝服务攻击	147
18.6 审计非法服务,特洛伊木马和蠕虫	148
18.7 结合所有攻击定制审计策略	148
本章小结	151
问题讨论	152

第 19 章 控制阶段的安全审计

19.1 引言	152
19.2 控制阶段	152
19.2.1 获得 root 的权限	153
19.2.2 创建额外账号	153
19.2.3 获得信息	153
19.2.4 开启新的安全漏洞	154
19.2.5 擦除渗透的痕迹	155
19.2.6 攻击其他系统	155
19.3 控制方法	155
19.3.1 系统缺省设置	155
19.3.2 合法及非法的服务,进程和可装载的模块	155
19.3.3 NetBus	156
19.3.4 BackOrifice 和 BackOrifice2000	159
19.3.5 LophtCrack 工具	161
19.3.6 Unix 密码安全	161
19.4 审计阶段	162
19.4.1 审计 Unix 文件系统	162
19.4.2 审计 Windows 2000	163
本章小结	164
问题讨论	164

第 20 章 入侵监测系统

20.1 引言	164
20.2 入侵监测的概念	165
20.2.1 入侵监测的功能	165
20.2.2 入侵监测系统的必要性	166
20.3 入侵监测系统的构架	166
20.3.1 网络级 IDS	166
20.3.2 主机级 IDS	167
20.4 IDS 规则	168
20.5 入侵监测系统软件	170
20.6 购买 IDS 注意事项	173
本章小结	173
问题讨论	174

第 21 章 审计和日志分析

21.1 引言	174
---------	-----

21.2 基线的建立	174
21.3 操作系统日志	175
21.3.1 记录 Unix 系统日志	175
21.3.2 记录 Windows 2000 系统日志	175
21.4 日志过滤	176
21.4.1 在 Windows 2000 中过滤日志	176
21.4.2 在 Linux 中过滤日志	177
21.5 关于审核日志的其他问题	178
21.5.1 防火墙和路由器日志	178
21.5.2 可疑的活动	178
21.5.3 其他类型日志	179
21.5.4 日志存储	179
21.5.5 审计和系统性能下降	179
本章小结	180
问题讨论	180

第 22 章 审计结果

22.1 建议审计执行过程	180
22.2 建立审计报告	181
22.3 增强一致性	182
22.4 安全审计和安全标准	182
22.4.1 ISO 7498-2	182
22.4.2 英国标准 7799(BS 7799)	183
22.4.3 Common Criteria(CC)	183
22.5 增强路由器安全	185
22.6 提前检测	186
22.7 主机审计解决方案	187
22.7.1 清除“感染”	187
22.7.2 个人防火墙软件	187
22.7.3 IPSec 和加密	188
22.7.4 加密和安全策略的一致性	188
22.7.5 修补系统漏洞	188
22.7.6 Windows 2000 中的 TCP 序列	188
22.7.7 IPv6	188
22.7.8 升级和替代服务	189
22.7.9 Secure Shell(SSH)	189
本章小结	191
问题讨论	191

实 验 篇

实验 1	使用 PGP 创建密钥对	195
实验 2	导出 PGP 公钥对及签名	196
实验 3	使用 PGP 密钥对加密、解密信息	197
实验 4	用 PGP 加密和解密文件	198
实验 5	使用 md5sum 创建 hash 校验和	199
实验 6	使用 PGP 实现 VPN 的实施	201
实验 7	使用 sniffer 捕获加密包和非加密包	202
实验 8	在 IIS 中实现 SSL	203
实验 9	使用 NAT 进行蛮力攻击	205
实验 10	发送伪造的 E-mail	206
实验 11	Tribe Flood Network(TFN)攻击	207
实验 12	在 Windows 2000 下关闭端口	209
实验 13	在 Windows 下使用 NC(NetCat)开放后门端口	210
实验 14	在 IIS 中配置安全的 Web 站点	211
实验 15	在 IIS 中配置安全的 FTP 服务	212
实验 16	配置简单的网络检测	213
实验 17	用 Winroute 创建包过滤规则	214
实验 18	账号锁定策略与暴力攻击	215
实验 19	强制使用“强壮”的密码	216
实验 20	在 Windows 2000 下卸载和删除一些不必要的服务	217
附录	端口大全	218