湖北高职“十一五”规划教材

HUBEIGAOZHI “SHIYIWU” GUIHUAJIAOCAI

湖北省高等教育学会高职专委会研制

总策划 李友玉
策 划 屠莲芳

WangLuo
AnQuanYuGuanLi

网络安全与管理

主 编 张月红 李京昆 黄泽钧

湖北长江出版集团
湖北省教材出版中心
湖北人民出版社

湖北高职“十一五”规划教材

HUBEI GAOZHI “SHIYIWU” GUIHUA JIAOCAI

湖北省高等教育学会高职专委会研制　　**总策划**　李友玉　**策　划**　屠莲芳

网络安全与管理

主　编　张月红　李京昆　黄泽钧

副主编　陈文明　任思佳　叶文涛　刘　华

编　者（按姓氏笔划为序）

王　跃　司　军　吴秉书　邱　松

邱　净　沈　强　张　博　张书田

陈　陆　陈　琛　陈玉平　邵　军

胡汉襄　崔俊峰　雷　雨

湖北长江出版集团

湖北省教材出版中心

湖北人民出版社

鄂新登字 01 号

图书在版编目(CIP)数据

网络安全与管理/张月红,李京昆,黄泽钧主编.
武汉:湖北人民出版社,2009.1

ISBN 978-7-216-05868-1

Ⅰ.网…
Ⅱ.①张…②李…③黄…
Ⅲ.计算机网络—安全技术—高等学校:技术学校—教材
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2009)第 002180 号

网络安全与管理 张月红 李京昆 黄泽钧 主编

出版发行:湖北长江出版集团 湖北省教材出版中心 湖北人民出版社

地址:武汉市雄楚大街 268 号

邮编:430070

印刷:武汉珞珈山学苑印刷有限公司
开本:787 毫米 ×1092 毫米 1/16
版次:2009 年 1 月第 1 版
书号:ISBN 978-7-216-05868-1

印张:22.5
字数:526 千字
印次:2009 年 1 月第 1 次印刷
定价:40.00 元

本社网址:http://www.hbpp.com.cn

湖北高职“十一五”规划教材

（计算机类）

凝聚集体智慧　研制优质教材

教材是教师教学的脚本，是学生学习的课本，是学校实现人才培养目标的载体。优秀教师研制优质教材，优质教材造就优秀教师，培育优秀学生。教材建设是学校教学最基本的建设，是提高教育教学质量最基础性的工作。

高职教育是中国特色的创举。我国创办高职教育时间不长，高职教材存在严重的“先天不足”，如中专延伸版、专科移植版、本科压缩版等。这在很大程度上制约着高职教育教学质量的提高。因此，根据高职教育培养“高素质技能型专门人才”的目标和教育教学实际需求，研制优质教材，势在必须。

2005年以来，湖北省高等教育学会高职高专教育管理专业委员会（简称“高职专委会”），高瞻远瞩，审时度势，深刻领会国家关于“大力发展职业教育”和“提高高等教育质量”之精神，准确把握高职教育发展之趋势，积极呼应全省高职院校发展之共同追求；大倡研究之风，大鼓合作之气；组织全省高职院校开展“教师队伍建设、专业建设、课程建设、教材建设”（简称“四个建设”）的合作研究与交流。旨在推进全省高职院校进一步全面贯彻党的教育方针，创新教育思想，以服务为宗旨，以就业为导向，工学结合、校企合作，走产学结合发展道路；推进高职院校培育特色专业、打造精品课程、研制优质教材、培养高素质的教师队伍，提升学校整体办学实力与核心竞争力；促进全省高职院校走内涵发展道路，全面提高教育教学质量。

湖北省教育厅将高职专委会“四个建设”系列课题列为“湖北省教育科学‘十一五’规划专项资助重点课题”。全省高职院校纷起响应，几千名骨干教师和一批生产、建设、服务、管理一线的专家，一起参加课题协同攻关。在科学研究过程中，坚持平等合作，相互交流；坚持研训结合，相互促进；坚持课题合作研究与教材合作研制有机结

合，用新思想新理念指导教材研制，塑造教材“新、特、活、实、精”的优良品质；坚持以学生为本，精心酿造学生成长的精神食粮。全省高职院校重学习研究，重合作创新蔚然成风。

这种以学会为平台，以学术研究为基础开展的“四个建设”，符合教育部关于提高教育教学质量的精神，符合高职院校发展的需求，符合高职教师发展的需求。

在湖北省教育厅和湖北省高教学会领导的大力支持下，在湖北省高教学会秘书处的指导下，经过两年多艰苦不懈的努力和深入细致的工作，“四个建设”合作研究初见成效。高职专委会与长江出版传媒集团、武汉大学出版社、复旦大学出版社等知名出版单位携手，正陆续推出课题研究成果：“湖北高职‘十一五’规划教材”，这是全省高职集体智慧的结晶。

交流出水平，研究出智慧，合作出成果，锤炼出精品。凝聚集体智慧，共创湖北高职教育品牌——这是全省高职教育工作者的共同心声！

湖北省高教学会高职专委会主任　黄木生

2009 年 1 月

前　言

《网络安全与管理》是湖北省高职“十一五”规划教材，是湖北省教育科学“十一五”规划专项资助重点课题成果，是高职计算机专业核心教材之一。

21 世纪，人类社会已进入信息时代，计算机的普及与互联网技术的飞速发展，使信息与信息系统成为一种重要的战略资源。随着信息网络地位的不断提高，电子商务的广泛开展，信息安全也成为 IT 领域的重中之重，更成为世人关注的社会问题和计算机科学的热点研究课题。因此，了解和掌握信息安全的相关知识是非常必要的。发展信息安全技术与产业，保障信息系统安全，培养信息安全领域的专业人才，已经成为当务之急。

鉴于此，越来越多的人希望了解并掌握信息安全领域的相关知识，在这种强大需求的推动下，各大中专院校纷纷开设了信息安全专业课程，加快培养熟悉信息安全攻防原理，掌握攻防对抗的实践经验，精通各种安全防护技术及相关产品的应用维护，能够独立完成各种系统的安全评估与加固，参与和管理复杂的信息资产保障课题，以及熟悉信息安全工程和标准的信息安全专业人员。

本书共有 18 个项目，隶属于三个大类。第一大类分析主机系统面临的威胁和系统安全的基本要素，共有 7 个项目，通过这些实践项目的学习，读者能够较为全面地掌握在没有任何防护产品的前提下，如何进行主机防护，从而更好地理解 PC 机的安全加固方法。第二大类介绍安全防护技术及安全产品的内容，共有 6 个实训项目辅助理解，通过学习，读者能够系统地掌握信息安全技术与产品的基础知识，深入了解加密技术、防火墙技术、入侵检测技术等。第三大类为主流攻击分析与对抗，共设计 5 个实训项目，使读者能更深入了解网络中的各类风险的产生与对抗方法。

湖北省高等教育学会副秘书长、湖北省教育科学研究所高教研究中心主任李友玉研究员，湖北省高等教育学会高职高专教育管理专业委员会教学组组长李家瑞教授、秘书长屠莲芳，负责本教材研制队伍的组建、管理和本教材研制标准、研制计划的制定和实施。

本书的项目设计由襄樊职院张月红和襄樊亮剑信息安全技术有限公司李京昆完成；第一部分项目由湖北三峡职院的陈文明老师和陈玉平老师、湖北水利水电职业技术学院的黄泽钧老师、张博老师和邵军老师共同完成；第二部分由武汉工业职业技术学院的叶文涛老师、邱松老师和襄樊职业技术学院的雷雨老师合作完成；第三部分由张月红老师带领襄樊亮剑信息安全技术有限公司的团队成员（任思佳、刘华、胡汉襄、崔俊峰、陈陆、邱净、吴秉书、王跃、沈强、司军、张书田、陈琛）共同完成项目的开发和文档编写。

本书既可以作为计算机及相关专业的教材使用，也可以作为已经学习和掌握了 IT 技术的相关工程技术人员、网络系统管理人员的参考用书。对于希望快速系统地掌握信息安全技术与产品基础知识的入门者，本书也是一本不可多得的参考资料。

全书的校阅由张月红老师和宋清龙教授负责，襄樊亮剑信息安全技术有限公司为本书提供大量实践项目支持。编者对大家一年来的辛勤劳动表示诚挚的感谢！

如果您在阅读本书时发现了问题，或者对本书有什么意见和建议，欢迎随时与我们联系，编者的电子邮件地址为 honey_bobo@ sina. com。

湖北高职“十一五”规划教材
《网络安全与管理》研制组
2009 年 1 月

目　录

项目1　查找隐藏账户 …… 1
1.1　背景知识 …… 1
1.1.1　用户账户概述 …… 1
1.1.2　用户账户的设置 …… 2
1.2　项目分析 …… 3
1.2.1　风险分析 …… 3
1.2.2　涉及知识 …… 3
1.3　实训内容 …… 3
1.3.1　实训流程 …… 3
1.3.2　实训准备 …… 4
1.3.3　实训1:建立CMD下隐藏账户 …… 10
1.3.4　实训2:建立“本地用户和组”下隐藏账户 …… 22
1.3.5　总结归纳 …… 32
1.4　Windows隐藏账户的防范 …… 32
1.4.1　管理层次 …… 32
1.4.2　技术层次 …… 33
1.5　项目小结 …… 38
项目2　设置IIS服务器中虚拟主机用户权限 …… 39
2.1　背景知识 …… 39
2.1.1　权限概述 …… 39
2.1.2　权限分类 …… 39
2.1.3　利用组策略设置权限 …… 40
2.1.4　利用DOS命令行设置用户权限 …… 41
2.2　项目分析 …… 41
2.2.1　风险分析 …… 41
2.2.2　涉及知识 …… 41
2.3　实训内容 …… 42
2.3.1　实训流程 …… 42
2.3.2　实训准备 …… 42
2.3.3　实训:IIS服务器中虚拟主机用户权限设置 …… 43
2.4　项目小结 …… 61
项目3　设置启动项安全策略 …… 63
3.1　背景知识 …… 63
3.1.1　Windows NT系统的引导过程 …… 63
3.1.2　自启动程序加载途径 …… 64
3.1.3　启动项管理工具Msconfig …… 64

3.2 项目分析 …… 65
3.2.1 风险分析 …… 65
3.2.2 涉及知识 …… 65
3.3 实训内容 …… 66
3.3.1 实训流程 …… 66
3.3.2 实训准备 …… 66
3.3.3 实训1:查看编辑启动项 …… 67
3.3.4 实训2:对启动项目进行防护 …… 69
3.3.5 实训3:使用360安全卫士监测启动项目 …… 71
3.4 项目小结 …… 72
项目4 检测进程信息 …… 73
4.1 背景知识 …… 73
4.1.1 进程概述 …… 73
4.1.2 解析 Windows 系统基本进程 …… 73
4.1.3 进程安全管理 …… 74
4.2 项目分析 …… 75
4.2.1 风险分析 …… 75
4.2.2 涉及知识 …… 75
4.3 实训内容 …… 76
4.3.1 实训流程 …… 76
4.3.2 实训准备 …… 76
4.3.3 实训:检测进程信息 …… 77
4.4 项目小结 …… 87
项目5 配置日志防护策略 …… 88
5.1 背景知识 …… 88
5.1.1 日志概述 …… 88
5.1.2 配置审核策略 …… 88
5.1.3 保护事件日志 …… 89
5.2 项目分析 …… 90
5.2.1 风险分析 …… 90
5.2.2 涉及知识 …… 90
5.3 实训内容 …… 91
5.3.1 实训流程 …… 91
5.3.2 实训准备 …… 91
5.3.3 实训:配置日志防护策略 …… 92
5.4 项目小结 …… 99
项目6 配置主机共享资源 …… 100
6.1 背景知识 …… 100
6.1.1 共享资源概述 …… 100
6.1.2 共享资源的管理 …… 101

6.1.3 提高共享资源的安全性 …… 101
6.2 项目分析 …… 102
6.2.1 风险分析 …… 102
6.2.2 涉及知识 …… 102
6.3 实训内容 …… 102
6.3.1 实训流程 …… 102
6.3.2 实训准备 …… 103
6.3.3 实训:共享资源安全设置 …… 103
6.4 项目小结 …… 115
项目7 WSUS 分发补丁 …… 116
7.1 背景知识 …… 116
7.1.1 补丁概述 …… 116
7.1.2 补丁查看、更新方法 …… 117
7.2 项目分析 …… 118
7.2.1 风险分析 …… 118
7.2.2 涉及知识 …… 118
7.3 实训内容 …… 119
7.3.1 实训流程 …… 119
7.3.2 实训准备 …… 119
7.3.3 实训:WSUS 分发补丁 …… 120
7.4 项目小结 …… 126
项目8 使用 PGP 加密 …… 127
8.1 背景知识 …… 127
8.1.1 对称加密算法 …… 127
8.1.2 非对称加密算法 …… 128
8.1.3 RSA …… 128
8.2 项目分析 …… 129
8.2.1 风险分析 …… 129
8.2.2 涉及知识 …… 129
8.3 实训内容 …… 129
8.3.1 实训流程 …… 129
8.3.2 实训准备 …… 130
8.3.3 实训 1:PGP 的安装及对文件加密 …… 131
8.3.4 实训 2:PGP 对硬盘分区加密 …… 136
8.3.5 实训 3:PGP 对邮件加密和数字签名 …… 140
8.4 项目小结 …… 148
项目9 搭建二级证书服务器 …… 149
9.1 背景知识 …… 149
9.1.1 PKI 的概念 …… 149
9.1.2 为什么需要 PKI …… 149

9.1.3 功能组成结构 …… 150
9.1.4 证书与证书授权中心 …… 150
9.1.5 Microsoft 证书服务 …… 151
9.2 项目分析 …… 151
9.2.1 风险分析 …… 151
9.2.2 涉及知识 …… 152
9.3 实训内容 …… 152
9.3.1 实训流程 …… 152
9.3.2 实训准备 …… 152
9.3.3 实训 1:安装证书服务并架设独立根 CA …… 153
9.3.4 实训 2:安装二级证书服务器(独立从属 CA 的安装) …… 157
9.4 项目小结 …… 164
项目10 申请、使用 IE 证书 …… 165
10.1 背景知识 …… 165
10.1.1 什么是数字证书 …… 165
10.1.2 为什么要用数字证书 …… 165
10.1.3 数字证书原理 …… 166
10.1.4 数字证书应用 …… 167
10.2 项目分析 …… 168
10.2.1 风险分析 …… 168
10.2.2 涉及知识 …… 168
10.3 实训内容 …… 168
10.3.1 实训流程 …… 168
10.3.2 实训准备 …… 169
10.3.3 实训:申请、使用 IE 证书 …… 169
10.4 项目小结 …… 176
项目11 配置防火墙策略 …… 177
11.1 背景知识 …… 177
11.1.1 防火墙定义 …… 177
11.1.2 防火墙应用范围 …… 177
11.1.3 防火墙主要功能 …… 178
11.2 项目分析 …… 180
11.2.1 风险分析 …… 180
11.2.2 涉及知识 …… 181
11.3 实训内容 …… 181
11.3.1 实训流程 …… 181
11.3.2 实训准备 …… 181
11.3.3 实训:配置防火墙策略 …… 182
11.4 项目小结 …… 197
项目12 安装和配置入侵检测系统 …… 198

12.1　背景知识 …… 198
12.1.1　HIDS …… 198
12.1.2　NIDS …… 199
12.1.3　混合型 …… 200
12.2　项目分析 …… 200
12.2.1　风险分析 …… 200
12.2.2　涉及知识 …… 200
12.3　实训内容 …… 200
12.3.1　实训流程 …… 200
12.3.2　实训准备 …… 201
12.3.3　实训:安装和配置入侵检测系统 …… 202
12.4　项目小结 …… 221
项目13　配置入侵检测系统策略 …… 222
13.1　背景知识 …… 222
13.1.1　规则应用类事件识别 …… 222
13.1.2　自定义特征类事件识别 …… 223
13.1.3　自身脆弱性事件识别 …… 223
13.1.4　其他设备类事件识别 …… 223
13.2　项目分析 …… 223
13.2.1　风险分析 …… 223
13.2.2　涉及知识 …… 223
13.3　实训内容 …… 224
13.3.1　实训流程 …… 224
13.3.2　实训准备 …… 224
13.3.3　实训:配置入侵检测系统策略 …… 225
13.4　项目小结 …… 229
项目14　网络协议分析工具使用 …… 230
14.1　背景知识 …… 230
14.1.1　协议分析的作用 …… 230
14.1.2　选择协议分析工具 …… 230
14.1.3　协议分析软件的部署 …… 231
14.2　项目分析 …… 233
14.2.1　风险分析 …… 233
14.2.2　涉及知识 …… 233
14.3　实训内容 …… 233
14.3.1　实训流程 …… 233
14.3.2　实训准备 …… 233
14.3.3　实训 1:网络协议分析工具的安装与测试 …… 235
14.3.4　实训 2:科来网络分析系统重要功能 …… 238
14.3.5　实训 3:监听 FTP 协议 …… 256

14.4 项目小结 …… 257
项目15 解析 ARP 欺骗攻击 …… 259
15.1 背景知识 …… 259
15.1.1 ARP 协议 …… 259
15.1.2 网内计算机常见通讯方式 …… 259
15.2 项目分析 …… 260
15.2.1 风险分析 …… 260
15.2.2 涉及知识 …… 261
15.3 实训内容 …… 261
15.3.1 实训流程 …… 261
15.3.2 实训准备 …… 262
15.3.3 实训 1:正常的网络通讯 …… 264
15.3.4 实训 2:局域网信息嗅探 …… 267
15.3.5 实训 3:破坏局域网计算机正常上网 …… 272
15.3.6 总结归纳 …… 277
15.4 ARP 防范 …… 279
15.5 项目小结 …… 280
项目16 清除和预防熊猫烧香病毒 …… 281
16.1 背景知识 …… 281
16.1.1 病毒概述 …… 281
16.1.2 病毒原理 …… 281
16.2 项目分析 …… 283
16.2.1 风险分析 …… 283
16.2.2 涉及知识 …… 283
16.3 实训内容 …… 283
16.3.1 实训流程 …… 283
16.3.2 实训准备 …… 284
16.3.3 实训:清除和预防熊猫烧香病毒 …… 285
16.4 项目小结 …… 292
项目17 检测木马网络特性 …… 293
17.1 背景知识 …… 293
17.1.1 木马概述 …… 293
17.1.2 木马原理 …… 293
17.1.3 木马防治 …… 295
17.2 项目分析 …… 295
17.2.1 风险分析 …… 295
17.2.2 涉及知识 …… 296
17.3 实训内容 …… 296
17.3.1 实训流程 …… 296
17.3.2 实训准备 …… 297

17.3.3　实训:检测木马网络特征 …… 298
17.4　项目小结 …… 306
项目18　分析和防范 SQL 注入提权 …… 307
18.1　背景知识 …… 307
18.1.1　基本概念 …… 307
18.1.2　检测与防范 …… 307
18.2　项目分析 …… 309
18.2.1　风险分析 …… 309
18.2.2　涉及知识 …… 309
18.3　实训内容 …… 309
18.3.1　实训流程 …… 309
18.3.2　实训准备 …… 310
18.3.3　实训:分析和防范 SQL 注入提权 …… 311
18.3.4　总结归纳 …… 336
18.4　SQL 注入防范策略 …… 336
18.5　项目小结 …… 337
参考文献 …… 338

项目1　查找隐藏账户

1.1　背景知识

1.1.1　用户账户概述

众所周知，Windows 是一个支持多用户、多任务的操作系统。用户账户的安全是保障系统不被滥用的第一道防线的一部分，即使许多企业拥有先进的数字化安全系统，如防火墙、VPN 及 PKI 等，如果没有对访问用户进行有效的识别和认证，这些安全措施终将成为沙滩上的城堡。

用户账户是指用户定义到 Windows 的所有信息组成的记录。这些记录包括用户名和用户登录所需的密码、用户账户所属的组，以及用户使用计算机和网络并访问资源的权利和权限。其中用户名是 Windows 标识用户账户的唯一名称。账户的用户名在其自身所在的域或工作组中必须是唯一的。

对于 Windows XP Professional 和成员服务器，用户账户由“本地用户和组”管理。对于 Windows Server 域控制器，用户账户由域服务器“Active Directory 用户和计算机”管理。可以在不同用户账户之间切换，而不必重新启动计算机。

从 Windows NT 之后，用户被分成许多组，组和组之间都有不同的权限，当然，一个组内的用户也可以有不同的权限。

下面简单介绍一下 Windows 系统中常见的用户组。

Administrators：管理员组，默认情况下，Administrators 中的用户对计算机/域有不受限制的完全访问权。分配给该组的默认权限允许对整个系统进行完全控制。所以，只有受信任的人员才可成为该组的成员。

Power users：高级用户组，Power users 可以执行除了为 Administrators 组保留的任务外的其他任何操作系统任务。分配给 Power users 组的默认权限允许 Power users 组的成员修改整个计算机的设置。但 Power users 不具有将自己添加到 Administrators 组的权限。在权限设置中，这个组的权限是仅次于 Administrators 的。

Users：普通用户组，这个组的用户无法进行有意或无意的改动。因此，用户可以运行经过验证的应用程序，但不可以运行大多数旧版应用程序。Users 组是最安全的组，因为分配给该组的默认权限不允许成员修改操作系统的设置或用户资料。Users 组提供了一个最安全的程序运行环境。在经过 NTFS 格式化的卷上，默认安全设置旨在禁止该组的成员危及操作系统和已安装程序的完整性。用户不能修改系统注册表设置、操作系统文件或程序文件。users 可以关闭工作站，但不能关闭服务器。Users 可以创建本地组，但只能修改自己创建的本地组。

Guests：来宾组，按默认值，来宾跟普通 Users 的成员有同等访问权，但来宾账户的限制

更多。

Everyone:顾名思义,所有的用户,这个计算机上的所有用户都属于这个组。

其实还有一个组也很常见,它拥有和 Administrators 一样、甚至比其还高的权限,但是这个组不允许任何用户的加入,在察看用户组的时候,它也不会被显示出来,它就是 System 组。系统和系统级的服务正常运行所需要的权限都是靠它赋予的。System 组只有一个用户 System,也许把该组归为用户的行列更为贴切。

权限是有高低之分的,有高权限的用户可以对低权限的用户进行操作,但除了 Administrators 之外,其他组的用户不能访问 NTFS 卷上的其他用户资料,除非他们获得了这些用户的授权。而低权限的用户无法对高权限的用户进行任何操作。默认情况下,系统安装完成后再进行创建的用户账户都属于 Users 组。但是,高权限的用户可以将新用户添加到其权限相同的组中。

基于安全因素,操作系统将用户和密码信息加密后存放在特定的地方和文件中,在 Windows NT 及以上版本的操作系统里,这些加密信息都保存于% systemroot% \system32\config\sam 文件中。

1.1.2 用户账户的设置

要对用户账户进行设置,可以通过图形化界面和命令行的方式进行。

1. 图形化界面设置用户账户

步骤如下:

请单击“开始”,指向“设置”,单击“控制面板”,然后双击“管理工具”中的“计算机管理”。

在“计算机管理”界面中选择“系统工具”中的“本地用户和组”。

在“本地用户和组”下的“用户”和“组”下都可以将用户账户添加到相应的组当中。

2. 命令行设置用户账户

图形化界面可以做到的,对命令行来说一样可以做到。在 Windows 操作系统中自带了 net 命令,其中 net user 命令可以对用户账户进行添加、删除、修改或查看。而 net group 或 net localgroup 可以对组当中的账户进行添加、删除操作。

其命令格式如下:

net user [UserName [Password | *] [options]] [/domain]

net user [UserName {Password | *} /add [options] [/domain]]

net user [UserName [/delete] [/domain]]

net group [groupname [/comment:"text"]] [/domain]

net group [groupname {/add [/comment:"text"] | /delete} [/domain]]

net group [groupname username[...]{/add | /delete} [/domain]]

net localgroup [GroupName [/comment:"text"]] [/domain]

net localgroup [GroupName {/add [/comment:"text"] | /delete} [/domain]]