

A COURSE OF INFORMATION SECURITY AND
APPLICATION PROGRAMMING EXPERIMENTS

信息安全与应用编程 实验教程

主 编 姜 斌 吕秋云
副主编 朱 芳 唐向宏



ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

内容简介

本书主要包括了四大部分实验:信息安全基础操作实验、编程基础训练实验、密码学编程实验和网络安全编程实验。

本书压缩了繁琐的理论指导,紧扣课程实验教学的目标,注重培养学生实际动手能力,发挥学生自我动手和创造能力。对实验案例的分析和讲解,力求做到简明、清晰和准确,通过有针对性的案例实践操作,使学生更高效地掌握相关理论依据和知识。

本书既可作为信息安全、通信和计算机专业信息安全方向的本科生和研究生的实验用书,也可供企业信息安全方面教学培训学习参考。

图书在版编目(CIP)数据

信息安全与应用编程实验教程 / 姜斌, 吕秋云主编.
—杭州: 浙江大学出版社, 2014. 2
ISBN 978-7-308-12841-4

I. ①信… II. ①姜… ②吕… III. ①信息安全—
高等学校—教材 ②程序设计—高等学校—教材
IV. ①TP309 ②TP311.1

中国版本图书馆 CIP 数据核字 (2014) 第 018403 号

信息安全与应用编程实验教程

姜 斌 吕秋云 主编

责任编辑	樊晓燕(fxy@zju.edu.cn)
封面设计	十木米
出版发行	浙江大学出版社 (杭州市天目山路 148 号 邮政编码 310007) (网址: http://www.zjupress.com)
排 版	杭州中大图文设计有限公司
印 刷	杭州杭新印务有限公司
开 本	787mm×1092mm 1/16
印 张	20
字 数	487 千
版 次	2014 年 2 月第 1 版 2014 年 2 月第 1 次印刷
书 号	ISBN 978-7-308-12841-4
定 价	39.00 元

版权所有 翻印必究 印装差错 负责调换

浙江大学出版社发行部联系方式: 0571-88925591; <http://zjdxcs.tmall.com>

前言

随着计算机科学技术的不断发展,计算机和网络已经成为人们学习和工作的重要组成部分,而随之产生的信息安全问题也日益受到人们的关注。实际上,信息安全已成为影响国家安全、经济发展、社会稳定、公民利益的重要问题。因此,国家和社会迫切需要高素质、有实战能力的信息安全类专业人才。

目前,国内高校各级、各类信息安全技术类课程的教学过程,在夯实理论知识的基础上,都大幅度提升了实验教学的比例,而且不同课程都在不同层面上引入实验内容,以期锻炼学生的理论联系实际的能力、实际动手能力以及创新能力。然而,每门课程的实验教学内容相对零散,往往不能构成一本实验教材。因此,本书力求为各类信息安全技术理论课程提供实验教学内容,方便教师指导,方便学生学习。

本书主要包括了四大部分:

第一部分是信息安全基础操作实验,包括网络数据信息抓包与安全分析实验、常见网络攻击实验、常见网络防御实验、操作系统安全配置、数据备份与恢复实验。这部分内容可以作为信息安全导论、信息安全技术等课程的实验素材,可以加深学生对信息安全、网络安全技术的感性认识和理解。

第二部分是编程基础训练实验,包括C和C++开发环境使用实验、信息安全编程基础实验。这部分内容的主要目的是训练学生的编程调试能力、可视化界面编程能力以及信息安全基本理论编程实现的能力。此部分内容适合非专业类的信息安全程序设计课程、信息安全专业低年级编程训练课程、信息安全数学基础课程使用。

第三部分是密码学编程实验,包括古典密码算法实验、对称密码算法实验、非对称密码算法实验。这部分内容主要服务于信息安全专业的核心基础课程——密码学课程,训练学生的各类加密算法实现能力。

第四部分是网络安全编程实验,包括网络通信编程实验、网络安全编程实验。这部分内容主要作为网络安全理论与技术相关课程的实验素材。

本书压缩了繁琐的理论指导,紧扣课程实验教学的目标,注重培养学生的实际动手能力,发挥学生自我动手和创造能力。本书对实验案例的分析和讲解,力求做到简明、清晰和准确,通过有针对性的案例实践操作,使学生更高效地掌握相关理论依据和知识。

本书适合信息安全、通信和计算机专业信息安全方向的本科生和研究生进行信息安全实验,也适合于企业进行信息安全方面的教学培训等。

本书由姜斌、吕秋云担任主编,负责制定全书大纲和审稿工作。由朱芳、唐向宏担任副主编。王秋华、王小军、吴震东等也参与了教材部分章节的编写。在此特别感谢卢毅、张程浩、缪金纬、周雷雷、常涛、潘腾蛟同学在教材编写中做的大量工作。

本教材在编写过程中得到了模拟实验训练系统软件厂商的大力支持,在此向他们表示衷心的感谢。

本教材在编写过程中,参考了一些国内外的教材和学术材料,在此向这些作者表示衷心的感谢。

浙江大学出版社大力支持了本书的出版,樊晓燕编审对本书的编写给予了很多有益的建议并认真负责地审阅了全书,在此表示衷心的感谢。

由于编者的水平有限,经验不足,时间仓促,教材中难免存在错误或不完善之处,恳请广大同行和读者予以批评指正,我们将在今后再版时改正。读者可以通过电子邮件(jiangbin@hdu.edu.cn, laqyzj@hdu.edu.cn)与编者联系。

编者

2013年12月于杭州电子科技大学

目 录

第 1 章 网络数据获取与安全分析实验	(1)
1.1 利用 Sniffer portable 软件进行数据包抓取	(1)
1.1.1 Sniffer portable 抓包工具使用实验	(1)
1.1.2 抓取一次完整的网络通信过程的数据包实验	(8)
1.2 利用 Sniffer portable 软件进行网络数据分析	(11)
1.2.1 基于协议的分析实验	(11)
1.2.2 基于关键字的安全分析实验	(13)
1.3 利用 Wireshark 软件进行数据包抓取	(18)
1.3.1 Wireshark 抓包工具使用实验	(18)
1.3.2 抓取一次完整的网络通信过程的数据包实验	(28)
1.4 利用 Wireshark 软件进行网络数据分析	(32)
1.4.1 TCP 协议的分析实验	(32)
1.4.2 HTTP 协议的分析实验	(39)
第 2 章 常见网络攻击实验	(46)
2.1 信息搜集实验	(46)
2.1.1 端口扫描实验	(46)
2.1.2 系统漏洞扫描实验	(50)
2.2 常见网络攻击实验	(57)
2.2.1 利用 IIS 缓冲区溢出漏洞实验	(57)
2.2.2 入侵网站管理系统实验	(62)
2.3 常见网络隐身实验	(65)
2.3.1 留后门实验	(65)
2.3.2 网络代理跳板使用实验	(69)
第 3 章 常见网络防御实验	(75)
3.1 防火墙实验	(75)
3.1.1 普通包过滤实验	(76)
3.1.2 状态检测实验	(80)
3.1.3 应用代理实验	(87)

3.2	入侵检测实验	(95)
3.3	病毒防护实验	(104)
3.3.1	网络炸弹脚本病毒	(104)
3.3.2	美丽莎宏病毒	(106)
第4章	操作系统安全配置	(110)
4.1	Windows 操作系统安全配置实验	(110)
4.1.1	系统安全配置实验	(110)
4.1.2	系统安全审核实验	(113)
4.1.3	NTFS 文件系统安全应用实验	(117)
4.2	Linux 操作系统安全设置实验	(119)
第5章	数据的备份与恢复实验	(126)
5.1	数据的备份与恢复	(126)
5.1.1	Acronis True Image 工具使用实验	(126)
5.1.2	数据的备份与恢复实验	(128)
5.2	系统的备份与恢复	(138)
5.2.1	系统的备份实验	(138)
5.2.2	误删除文件的恢复实验	(144)
第6章	C 和 C++ 开发环境使用实验	(147)
6.1	VC++6.0 开发工具使用实验	(147)
6.1.1	创建一个新的 C 语言的工程实验	(147)
6.1.2	添加一个文件到一个空的工程中实验	(152)
6.1.3	编写程序实验	(153)
6.1.4	运行程序实验	(156)
6.1.5	调试程序——设置断点实验	(158)
6.1.6	调试程序——动态察看变量的值	(159)
6.2	VC++6.0 下利用 MFC 实现友好界面编程实验	(161)
6.2.1	创建一个新 MFC 应用程序的工程实验	(161)
6.2.2	给对话框添加相关控件实验	(165)
6.2.3	编写 MFC 程序实验	(167)
6.3	Visual Studio 2012 开发工具使用实验	(169)
6.3.1	安装 Visual Studio 2012 实验	(170)
6.3.2	创建一个新的 C 语言的项目实验	(174)
6.3.3	添加一个文件到一个空的项目中实验	(178)
6.3.4	编写程序实验	(180)
6.3.5	运行程序实验	(182)
6.3.6	调试程序——设置断点实验	(183)

6.3.7 调试程序——动态察看变量的值	(185)
6.4 VS 2012 下利用 MFC 实现友好界面编程实验	(187)
6.4.1 创建一个基于对话框的 MFC 项目实验	(187)
6.4.2 编译运行生成的程序实验	(192)
6.4.3 给对话框添加相关控件实验	(194)
6.4.4 给控件添加消息处理函数实验	(196)
第 7 章 信息安全编程基础实验	(200)
7.1 大数的素性检测实验	(200)
7.2 大整数的加减法运算实验	(203)
7.3 利用矩阵变换实现加解密实验	(204)
第 8 章 古典密码算法编程实验	(207)
8.1 Caesar 密码	(207)
8.2 置换密码	(209)
第 9 章 对称密码算法编程实验	(212)
9.1 DES	(212)
9.2 三重 DES	(222)
9.3 AES	(223)
第 10 章 非对称密码算法编程实验	(241)
10.1 RSA	(241)
10.2 Elgamal 加密算法	(252)
第 11 章 网络通信编程实验	(255)
11.1 VC++6.0 下 CSocket 的基于 TCP 协议通信编程实验	(255)
11.2 VC++6.0 下 CSocket 的基于 UDP 协议通信编程实验	(262)
11.3 VC++6.0 下 CAsyncSocket 的基于 TCP 协议通信编程实验	(268)
11.4 VC++6.0 下 Socket 基于 TCP 协议的通信编程实验	(276)
11.5 VS2012 下 CSocket 基于 TCP 协议的通信编程实验	(283)
第 12 章 网络安全编程实验	(290)
12.1 端口扫描器编程实验	(290)
12.2 注册表安全防护编程实验	(296)
12.3 恶意代码及防护编程实验	(301)

A COURSE OF INFORMATION SECURITY AND
APPLICATION PROGRAMMING EXPERIMENTS

信息安全与应用编程实验教程

本书主要包括了四大部分实验：信息安全基础操作实验、编程基础训练实验、密码学编程实验和网络安全编程实验。

本书压缩了繁琐的理论指导，紧扣课程实验教学的目标，注重培养学生实际动手能力，发挥学生自我动手和创造能力。对实验案例的分析和讲解，力求做到简明、清晰和准确，通过有针对性的案例实践操作，使学生更高效地掌握相关理论依据和知识。

本书既可作为信息安全、通信和计算机专业信息安全方向的本科生和研究生的实验用书，也可供企业信息安全方面教学培训学习参考。

ISBN 978-7-308-12841-4



9 787308 128414 >

定价：39.00元