普通高等学校网络工程专业规划教材

网络安全与管理实验教程

王小妹　主　编
陈红松　副主编

清华大学出版社

普通高等学校网络工程专业规划教材

网络安全与管理实验教程

王小妹　主　编
陈红松　副主编

清华大学出版社
北京

内 容 简 介

本书是为适应信息化社会对于网络安全和管理人才的需求，培养学生在网络安全和管理方面的实践能力而编写的。内容从背景知识入手，对实验过程分步骤、分角色进行翔实描述，实验覆盖了当前网络安全的主要领域。

本书共分 18 章，第 1 和第 2 章对网络安全与管理实验作了概述；第 3 和第 4 章介绍 DES 和 RSA 两种基础算法；第 5 章介绍公钥基础设施 PKI；第 6 章介绍主动水印攻击；第 7～第 12 章实验内容包括 DDoS 攻击、ARP 欺骗攻击、TCP 端口扫描、模拟攻击方法、Winpcap 嗅探器、缓冲区溢出；第 13～第 16 章介绍 IDS、蜜罐、VPN 和防火墙的相关技术与实现；第 17 和第 18 章介绍计算机木马攻击和开源反病毒软件。

本书实验项目涵盖面广，知识结构层次清晰，从实验原理的讲解到课后思考题的设置，深入浅出，能够给不同知识背景的高校学生和教师自由发挥的空间。

本书可作为信息安全类相关专业本科生和研究生的课程实验教材，也可作为对于网络安全实训技能有需求的读者进行攻防模拟的参考书籍。

图书在版编目(CIP)数据

网络安全与管理实验教程/王小妹主编. —北京：清华大学出版社，2015
普通高等学校网络工程专业规划教材
ISBN 978-7-302-40767-6

Ⅰ. ①网… Ⅱ. ①王… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 161816 号

责任编辑：张　玥　赵晓宁
封面设计：常雪影
责任校对：梁　毅
责任印制：宋　林

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 装 者：三河市少明印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：10.5　　**字　　数**：263 千字
版　　次：2015 年 8 月第 1 版　　**印　　次**：2015 年 8 月第1次印刷
印　　数：1～2000
定　　价：29.50 元

产品编号：061815-01

FOREWORD

前　言

随着计算机、通信技术的飞速发展，网络已经广泛而又深刻地影响着人们的日常生活。与此同时，网络安全问题也成为当今社会的一个普遍存在的问题。近几年，大数据、云计算等新兴技术的出现，更是让我们意识到强调安全问题的必要性和重要性。

目前工科院校计算机大多设置密码学、信息安全、网络安全等相关专业，因为安全问题是计算机和互联网的重中之重。“网络安全与管理”是多所高校计算机和信息安全类本科生的专业基础类必修课，是学生接触网络安全和网络管理的理论和实践知识的起点。在安全问题日渐突出和成熟的情况下，实验动手能力显得尤为重要，实验课程是学生对理论知识消化理解、应用于实践的有效途径。本书针对网络安全和管理方面的技术，涉及知识点全面，实验内容具有代表性，且本书深入浅出的讲解方式，对于学生来说易上手、易操作。

本书是结合北京科技大学信息安全类专业及相关专业课程而设计编制的，书中所选用的部分实验内容是依据吉林中软吉大信息技术有限公司开发的网络信息安全综合实验系统中所提供的部分实验内容。全书共分为 18 章，涵盖了网络安全领域的基本实用技术，从而满足读者的实际学习和工作需要。第 1 和第 2 章是对网络安全与管理实验的概述，介绍了网络安全与管理的实验目的、要求、步骤和实验环境搭建等问题。第 3 和第 4 章介绍网络安全中应用到的两种加密算法——DES 算法和 RSA 算法。第 5～第 18 章，分别介绍了公钥基础设施 PKI 的应用、主动水印攻击、DDoS 攻击、ARP 欺骗攻击、TCP 端口扫描、模拟攻击方法、Winpcap 嗅探器、利用跳转指令实现缓冲区溢出、基于网络的入侵检测系统、自制蜜罐、利用 OpenVPN 构建企业 VPN、iptables 的应用、计算机木马攻击和反病毒软件。这些实验内容由背景知识入手，分步骤、分角色且图文并茂地讲解，并在实验最后设置了思考问题。

编者对于本书的编写主要侧重于以下几点：首先，对于实验内容从教材整体上体现系统、完善、循序渐进、层次化结构；注重实验项目的深度和广度的把握，使实验对于学生有可发挥的余地和可扩展的空间；其次，以综合实验为主，不乏理论知识的引导和梳理。让“网络安全与管理”等这类实验课成为高校安

FOREWORD

全类专业本科生进行动手实践训练和创新能力培养的起点，为后续课外科技创新活动、认识和生产实习、电子设计竞赛、毕业设计等打下基础，实现实践创新的一体化培养。

本教材的编写得到了“十二五”期间北京科技大学教材建设经费的资助。同时本书受北京市科技计划项目(No. D141100003414002)、北京市自然科学基金(No. 4142034)、北京市青年英才计划(No. YETP0380)及中央高校基本科研业务项目(No. FRF-TP-14-042A2)的资助。

在本书编写过程中，得到了北京科技大学计算机与通信工程学院副院长王建萍教授，软件工程系朱岩教授、张冬艳副教授和其他所有同事的大力支持和帮助，在此表示衷心的感谢！

由于编者水平有限，书中欠妥之处敬请广大读者批评指正。

编　者

2015 年 2 月于北京

CONTENTS

目　录

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

第1章　网络安全与管理实验概述

1.1　实验的目的与要求

目前，许多工科高等院校计算机学院设置了信息安全相关专业，因为安全问题是计算机和互联网稳步发展的一个必要条件和重中之重。本教材是根据高等院校网络安全、信息安全及密码学等专业的专业课程“网络安全与管理”编写的配套实验教材。“网络安全与管理实验教程”是计算机和信息安全类本科生巩固网络安全和网络管理理论知识的起点，是打下良好实践动手能力的起点。

编写本书的目的是通过学生亲自动手参与实验过程，能够巩固加深对于该课程理论知识的理解。在这个过程中以解决和分析具体网络安全问题为目的，按照由浅入深的思路，以任务驱动的方式，使学生掌握网络安全工具和网络管理工具的使用，并能对 Windows 平台和 Linux 平台的安全管理问题进行初步的分析和解决，全面掌握网络安全领域的实用技术，达到理论结合实践的最终目的。

1.2　实验课学习步骤

本教程中的实验要求学生进行每一个实验之前首先完成相关部分理论知识的学习，或者具有相关理论知识的基础。同学们在实验课程开始前需要对实验内容进行预习，了解实验原理、实验环境、实验任务，做好知识技能储备。每一章节的开始会对实验的背景知识做一个具体的介绍，同学们在动手实验之前应先掌握这些背景知识，也可以通过图书馆或网上查找资料进行扩充和细化。

1.3　实验报告要求

在实验过程中，严格遵守实验室规章和安全操作流程，对于单人任务，能够独立完成；对于多人任务能够良好地分工协作，完成任务，整个实验过程需要对重要图表数据截图保存，完成实验报告。对于实验中遇到的问题能够通过讨论、查找资料或者请教老师得到解决，课后完成实验教程中的思考问题。

实验报告中应具备以下内容：

（1）封面，应包括课程名称，学生的班级、姓名、学号、指导教师。

（2）内容，实验环境、组内分工、实验步骤说明和截图。

（3）实验小结和思考题，对实验的总结和体会，收获和疑惑；对课后思考题的思考过程和给出的解决办法。

1.4 实验室规则和安全操作流程

(1) 学生应有秩序地进入实验室,严禁大声喧哗、跑动,以保证安静良好的学习环境。

(2) 为了保证计算机及其他设备的安全和卫生,学生不得将食品、饮料等零食带入实验室。

(3) 做实验前先检查设备完好情况,若发现设备故障,应及时向教师报告情况。教师应详细记录设备故障情况,妥善进行处理。

(4) 正确开关机。在操作过程中不得随便或频繁开关机。如遇死机可采用热启动或系统复位方式重新启动系统。迫不得已关机后,需至少半分钟后才可开机。

(5) 在操作过程中,严禁随便拔插各类插头;严禁用力击打键盘;严禁在驱动器红灯亮时进行插、取盘操作;学生上机应使用学校提供统一管理的软盘,严禁私自携带各种磁盘进入实验室并上机操作,以防病毒侵入。对违反操作规程引起的设备损坏,要按原价赔偿。

(6) 操作完成后应正常退出所使用的软件,正确关闭计算机。将耳机、键盘、鼠标、椅子放好,认真填写设备记录后,方可离开。

(7) 特别严禁以下行为,对有违反者轻则做书面检查,屡教不改者学校将严肃处理:

① 对计算机进行加密。

② 将实验室内的软盘带出。

③ 私自携带软盘进入实验室。

④ 擅自修改、删除系统文件。

⑤ 损毁实验室设备。

(8) 除教学人员用机、学生上机、计算机活动课、计算机兴趣小组用机外,非经主管人员许可,外人不得进入实验室,不得擅自用机,违者后果自负。

(9) 不得让任何无关的人员使用自己的计算机,不要擅自或让其他非专业技术人员修改自己计算机系统的重要设置。

(10) 做实验期间禁止上网浏览任何与工作无关的信息。

(11) 严禁利用计算机系统上网发布、浏览、下载、传送反动、色情及暴力的信息。

(12) 严格遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》,严禁利用计算机非法入侵他人或其他组织的计算机信息系统。

第 2 章　网络安全与管理实验环境介绍

2.1　概述

随着现代通信技术的迅速发展和普及，因特网进入千家万户，计算机的应用也日益广泛和深入。同时，随着云计算、大数据等新兴技术的发展，信息安全和网络安全问题也日益突出，情况越来越复杂。实验教程针对信息安全和网络安全问题，由浅入深地给读者一个动手实践的方法和理解实际问题的途径。

本实验教程中部分实验是基于中软吉大网络信息安全教学实验系统进行的，中软吉大的网络信息安全教学实验系统是一套内容涵盖全面、知识层次递进的实验教学平台，适合高校信息安全专业的同学进行课堂实验和攻防训练。对于没有部署该套系统的读者，书中提供了相应的替代实验任务进行相同实验目的的练习，教师和同学们可以根据自身实验室环境进行灵活选择。

2.2　网络结构的选择与搭建

本教程中的部分实验需要两个人或多个人协作完成，在每个实验的实验环境中都会介绍本实验需要的人数和网络拓扑结构，为了统一起见，将主机间的位置关系归纳为交换网络结构和企业网络结构两种网络拓扑结构。这两种网络拓扑结构是根据实验的攻防角色的实际情况确定的，实验过程中教师可以根据自己班级的人数情况，或者同学根据自己的实际需求进行拓扑连接，也可以自己设计网络拓扑图，构建不同的主机的位置关系。

在交换网络结构中，实验组间主机可相互通信，实验组内各共享模块间可相互通信，并且实验主机可以访问应用服务器提供的各种服务和资源，如图 2.1 所示。

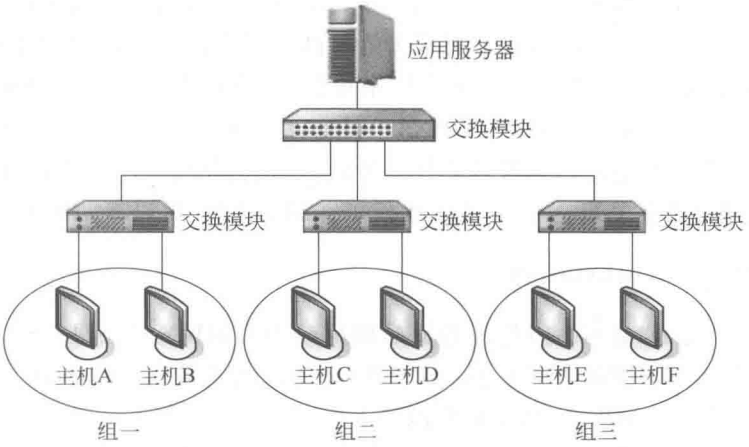

图 2.1　交换网络结构拓扑图

在企业网络结构中，实验组间相互独立，实验组内各共享模块间不能直接通信。通过对防火墙进行配置，可实现对实验组内主机进行区域划分：主机 A、B 为企业内网主机，主机 C、D 为企业 DMZ(非军事区)主机，主机 E、F 为外网主机。主机间的具体连接情况如图 2.2 所示。

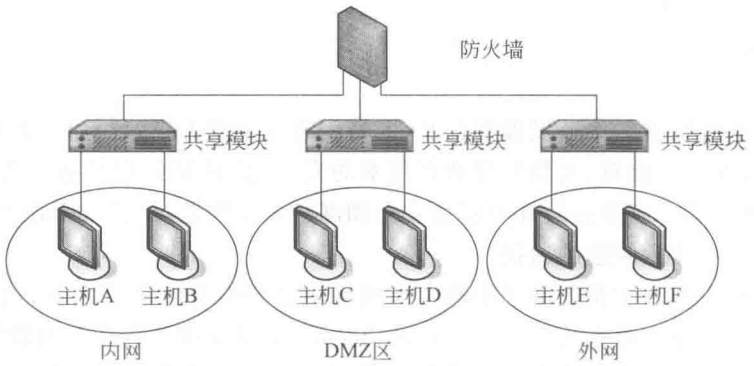

图 2.2　企业网络结构拓扑图

2.3　虚拟机的选择与使用

本实验教程中实验环境涉及多台主机安装多种操作系统，因此大量使用了虚拟机软件来模拟需要的主机和系统，学生在脱离实验室环境的情况下也可以自行安装虚拟机进行一些简单实验的练习。

虚拟机软件可以在计算机平台和终端用户之间建立一种环境，而终端用户则是基于这个软件所建立的环境来操作软件的。在计算机科学中，虚拟机是指可以像真实机器一样运行程序的计算机的软件实现。目前常用的虚拟机软件有以下几种。

2.3.1　VirtualBox

VirtualBox 最早是德国一家软件公司 InnoTek 所开发的虚拟系统软件，后来被 Sun 公司收购，改名为 Sun VirtualBox，性能有很大的提高。因为它是开源的，不同于 VM，而且功能强大，可以在 Linux、Mac 和 Windows 主机中运行，并支持在其中安装 Windows(NT 4.0、2000、XP、Server 2003、Vista)、DOS/Windows 3.x、Linux(2.4 和 2.6)、OpenBSD 等系列的客户操作系统。假如你有用过虚拟机软件经历的话，相信使用 VirtualBox 不在话下。即便你是第一次使用也没有关系，VirtualBox 提供了详细的文档，可以帮助你在短期内入门。

2.3.2　VMWare Workstation

VMWare(中文名“威睿”，纽约证券交易所代码为 VMW) 虚拟机软件，是全球桌面到数据中心虚拟化解决方案的领导厂商。VMWare 不需要重开机就能在同一台计算机上使用好几个操作系统。VMWare 的主要功能如下：

(1) 不需要分区或重开机就能在同一台 PC 上使用两种以上的操作系统。

(2) 完全隔离并且保护不同操作系统的操作环境以及所有安装在操作系统上面的应用