工业和信息产业职业教育教学指导委员会“十二五”规划教材
全国高等职业教育计算机系列规划教材

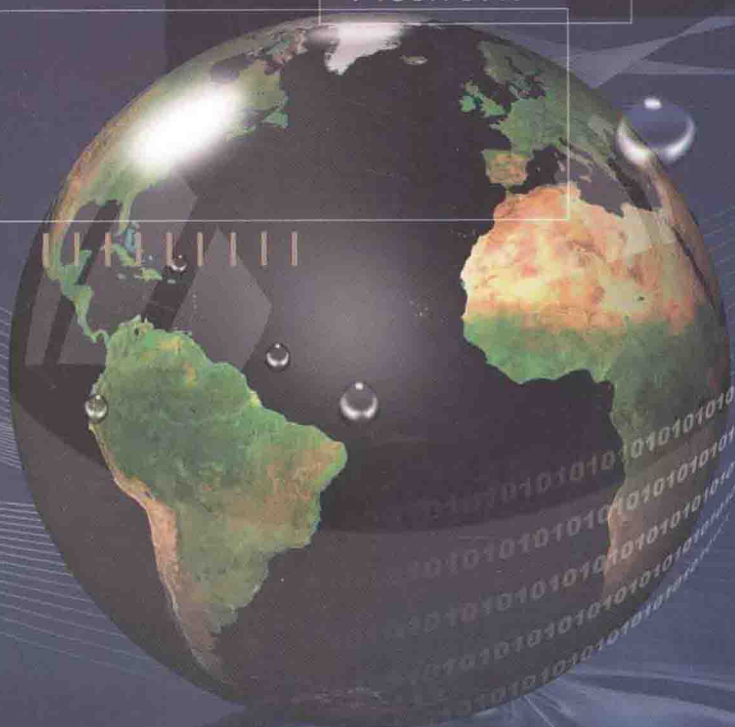
网络信息安全项目教程

◎丛书编委会

Network

http://www.phei.com.cn

Information Security



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

工业和信息产业职业教育教学指导委员会“十二五”规划教材
全国高等职业教育计算机系列规划教材

网络信息安全项目教程

◎丛书编委会

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书采用全新的项目实做的编排方式，真正实现了基于工作过程、项目教学的理念。本书由 4 个项目 11 个模块组成：项目 1 实现了配置单机系统安全，包括 Windows 系统加固和病毒的防治；项目 2 实现了防护网络安全，从防火墙、网络监听、网络扫描和黑客攻击与入侵检测的角度介绍了网络安全的策略、措施、技术和方法；项目 3 实现了信息安全，从信息加密、数字签名和数据存储的角度介绍了保证信息安全的方法、技术、手段；项目 4 实现了构建安全的网络结构，从网络结构的角度来探讨和总结了影响网络安全的因素和具体实现措施。

本书内容丰富，结构清晰，通过完整的实例对网络信息安全的概念和技术进行了透彻的讲述。本书不仅适用于高职高专教学需要，而且也是适合网络信息安全初学者的入门书籍和中级读者的提高教程。

图书在版编目（CIP）数据

网络信息安全项目教程 /《全国高等职业教育计算机系列规划教材》编委会编. —北京：电子工业出版社，2010.10
工业和信息产业职业教育教学指导委员会“十二五”规划教材　全国高等职业教育计算机系列规划教材

ISBN 978-7-121-11940-8

Ⅰ. ①网… Ⅱ. ①全… Ⅲ. ①计算机网络—安全技术—高等学校：技术学校—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 193390 号

策划编辑：左　雅
责任编辑：左　雅
印　　刷：北京市李史山胶印厂
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：19　　字数：486 千字
印　　次：2010 年 10 月第 1 次印刷
印　　数：4 000 册　定价：31.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

丛书编委会

本书编委会

主　　编　迟俊鸿　崔　炜

副 主 编　祖晓东　李立功　徐　伟　罗晓东

参　　编　崔　萃　唐振刚　董彧先　刘金鑫　张革华　张建忠

丛书编委会院校名单

（按拼音排序）

保定职业技术学院
渤海大学
常州信息职业技术学院
大连工业大学职业技术学院
大连水产学院职业技术学院
东营职业学院
河北建材职业技术学院
河北科技师范学院数学与信息技术学院
河南省信息管理学校
黑龙江工商职业技术学院
吉林省经济管理干部学院
嘉兴职业技术学院
交通运输部管理干部学院
辽宁科技大学高等职业技术学院
辽宁科技学院
南京铁道职业技术学院苏州校区
山东滨州职业学院
山东经贸职业学院
山东省潍坊商业学校
山东司法警官职业学院
山东信息职业技术学院
沈阳师范大学职业技术学院
石家庄信息工程职业学院
石家庄职业技术学院
苏州工业职业技术学院
苏州托普信息职业技术学院
天津轻工职业技术学院
天津市河东区职工大学
天津天狮学院
天津铁道职业技术学院
潍坊职业学院
温州职业技术学院
无锡旅游商贸高等职业技术学校
浙江工商职业技术学院
浙江同济科技职业学院

前　言

本书作为高职高专教学用书，是根据当前高职高专学生和教学环境的现状，结合职业需求，采用“工学结合”的思路，基于工作过程、以“项目实做”的形式贯穿全书。本书也适用于网络信息安全初学者及中级读者。

本书在编写上，打破传统的章节编排方式，改以任务实做为主，由浅入深，先基础后专业、先实做后理论的编排宗旨。全书采用“项目—模块—工作任务”三级结构，对应每一个具体模块，采用“六步”教学法依次展开：学习目标、工作任务、实践操作、问题探究、知识拓展、检查与评价。围绕工作任务，先进行具体的实做操作，再进行理论升华，然后进行拓展和提高，最后是检查与评价。

本书在内容上力求突出实用、全面、简单、生动的特点。通过本书的学习，能够让读者对网络信息安全有一个比较清晰的概念，能够配置单机系统的安全，能够防范网络攻击，能够保证信息安全，能够进行网络结构安全的分析和设计。

第 38 届世界电信日的主题是“让全球网络更安全”，由此也可以看出：“网络安全问题是当今网络最大的问题，网络安全专家是今后网络建设和管理所急需的人才”。为了培养和塑造更多网络安全人才，为了让网络更安全，由企业专家和高校教师进行深入调研和探讨，精选了部分经典案例和流行工具，采用“教、学、做”一体的模式，将网络安全知识通过本书呈现给各位读者。

本书精心组织了 4 个项目共 11 个模块：项目 1 配置单机系统的安全、项目 2 防范网络攻击、项目 3 保证信息安全、项目 4 构建安全的网络结构。

项目 1 实现了配置单机系统安全，包括两个模块。模块 1 为 Windows 系统安全加固，从 Windows 系统本身的安全防护措施入手，通过注册表、安全策略、系统配置等方法对单机系统的日常使用进行安全保障；模块 2 为病毒的防治，从日常病毒的防治入手，讲解了使用 McAfee、360 安全卫士清除病毒和预防日常病毒，以及病毒的基本知识和原理。

项目 2 实现了防护网络安全，从防火墙、网络监听、网络扫描和黑客攻击与入侵检测的角度对网络安全的策略、措施、技术和方法进行了描述。本任务包括四个模块。模块 3 讲述了防火墙的安装部署、配置策略等；模块 4 讲述了系统漏洞的扫描、主机扫描以及防护等方法和措施；模块 5 讲述了使用网络监听手段解决网络安全隐患、提高网络性能的方法和技术；模块 6 讲述了黑客攻击的常见方法、技术，以及相对应入侵检测的手段。

项目 3 实现了信息安全，从信息加密、数字签名和数据存储的角度描述了保证信息安全的方法、技术、手段。本项目包括三个模块。模块 7 讲述了对数据的简单加密方法，对文件的加密技术和工具；模块 8 讲述了应用数字签名保证网络传输安全性的具体方法和技术；模块 9 讲述了应用 RAID5 保证数据存储安全的具体方法和步骤，以

及发生灾难后数据的恢复方法。

项目 4 实现了构建安全的网络结构，包括两个模块，从网络结构的角度来探讨和总结了影响网络安全的因素和具体实现措施。

本书由迟俊鸿、崔炜主编并负责规划和统筹，祖晓东、李立功、徐伟、罗晓东担任副主编，崔萃、唐振刚、董彧先、刘金鑫、张革华、张建忠等教师参加了编写和审校工作。

由于编者水平有限，时间仓促，书中错误在所难免，恳切希望读者批评指正。联系方式：llg_wsq@126.com，QQ：393182984。

编　者

全国软件专业人才设计与开发大赛

为推动软件开发技术的发展，促进软件专业技术人才培养，向软件行业输送具有创新能力和实践能力的高端人才，提升高校毕业生的就业竞争力，全面推动行业发展及人才培养进程，工业和信息化部人才交流中心特举办“全国软件专业人才设计与开发大赛”，大赛包括两个比赛项目，即“JAVA 软件开发”和“C 语言程序设计”，并分别设置本科组和高职高专组。该大赛是工业和信息化部指导的面向大学生的学科竞赛和群众性科技活动。该大赛的成功举办，将有力推动学校软件类学科课程体系和课程内容的改革，培养学生的实践创新意识和能力，提高学生工程实践素质以及学生分析和解决实际问题的能力，有利于加强我国软件专业人才队伍后备力量的培养，提高我国软件专业技术人才的创新意识和创新精神。

大赛宗旨： 立足行业，结合实际，实战演练，促进就业

大赛特色： 政府、企业、协会联手构筑的人才培养、选拔平台；
预赛广泛参与，决赛重点选拔；
以赛促学，竞赛内容基于所学专业知识；
以个人为单位，现场比拼，公正公平。

2010 年全国软件专业人才设计与开发大赛简介

主办单位： 工业和信息化部人才交流中心

承办单位： 北京大学软件与微电子学院

协办单位： 中国软件行业协会
教育部高等学校高职高专计算机类专业教学指导委员会

支持单位： 大连东软信息学院　　国信蓝点信息技术有限公司

大赛网址： http://www.miit-nstc.org/

2010 年全国软件专业人才设计与开发大赛在北京、上海、天津、重庆、江苏、浙江等省市自治区共设立 24 个分赛区，53 个赛点，来自近 400 所高校的 5000 余名选手参加了比赛。2010 年 8 月 19 日，大赛在北京举行了决赛，来自北京邮电大学世纪学院的于俊超同学和来自安徽财贸职业学院的高伟同学分别获得“JAVA 软件开发”本科组与高职高专组特等奖；来自北京信息科技大学的郑程同学和石家庄信息工程职业学院的王海龙同学则分别获得“C 语言程序设计”本科组与高职高专组特等奖。北京工商大学、桂林电子科技大学、湖北工业大学等院校获得了优秀组织单位荣誉称号，北京信息科技大学、北京理工大学、青岛大学等 30 所院校获得了大赛优胜学校。

2010 年 8 月 21 日，大赛在北京大学百周年纪念讲堂举行了隆重的颁奖典礼。国务院参事，大赛组委会主任，中国电子商会会长，原国务院信息化工作办公室常务副主任曲维枝女士，工业和信息化部副部长杨学山先生、中国工程院院士倪光南先生、北京大学秘书长杨开忠教授、工业和信息化部信息化推进司徐愈司长、工业和信息化部人事教育司史晓光副司长、工业和信息化部软件服务业司郭建兵副司长、工业和信息化部科技司沙南生副司长、教育部高等教育司综合处调研员张庆国先生、中国软件行业协会理事长陈冲先生，教育部高等学校高职高专计算机类教学指导委员会主任温涛先生，北京大学软件与微电子学院院长张兴先生、大赛组委会副主任，北京大学教授陈钟先生，工业和信息化部人才交流中心主任石怀成先生、工业和信息化部人才交流中心顾问刘玉珍女士等近 40 位领导嘉宾出席了颁奖典礼。IBM、Intel 等企业也派代表出席了颁奖典礼。

目　录

背景知识

天津某学院校园网开通已有1年多的时间了，到现在仍然没有一个专职的网络管理员，网管工作一直由信息系李老师代管。在这1年多的时间里，校园网发生了很多和安全有关的事件，比如说校园网内病毒泛滥、Web服务器被攻击，学生科网站数据丢失，等等。为了解决校园网管理的问题，学校计划聘请校园网管理员专门来做校园网的管理工作。

小张毕业于某职业技术学院网络技术专业，毕业后立志做网管工作。一个偶然的机会看到某学院招聘网管的工作，小张抱着试试看的心情去应聘。

应聘的结果是不错的，小张顺利通过了网管职位的各种考试，做了该学校的网管工作，全面负责整个校园网的安全管理和维护。

在校园网的安全管理和维护中，小张都做了哪些工作？小张管理的校园网都发生了哪些事件？小张……

项目 1　配置单机系统安全

本项目重点介绍单机系统的安全防护，包含两个模块，模块1 Windows系统安全加固，主要介绍Windows系统的安全管理功能，如注册表调整、系统安全组策略方面的部署、目录服务及用户账户管理等。模块2病毒防治，主要介绍目前流行的查杀病毒软件的安装、升级、设置及日常使用。

通过本项目的学习，应达到以下目标：

1. 知识目标

◇ 理解Windows操作系统安全的基本理论；
◇ 理解用户账户及访问权限的基本概念；
◇ 掌握账户安全策略在系统安全中的作用；
◇ 掌握注册表的功能及其在系统安全中的作用；
◇ 理解IE安全设置的基本概念；
◇ 理解病毒的基本概念；
◇ 理解病毒的危害及病毒防治的意义；
◇ 理解木马的基本含义、类型、特性、危害；
◇ 理解恶意软件的概念、分类、来源、危害。

2. 能力目标

◇ 熟悉Windows Server 2003操作系统；
◇ 配置用户访问权限及磁盘访问权限；
◇ 配置注册表安全策略；
◇ 配置账户安全策略及审核策略等组策略；
◇ 配置IE安全策略。
◇ 能安装、升级、配置流行杀毒软件；
◇ 能操作流行杀毒软件查杀病毒；
◇ 能安装、升级、配置流行木马专杀工具软件；
◇ 能操作流行木马专杀工具查杀木马；
◇ 能操作流行恶意软件卸载工具。

模块 1

Windows系统安全加固

随着互联网的日益普及，人们对互联网络的依赖越来越强，网络已经成为人们生活中不可或缺的一部分。但是，Internet是一个面向大众的开放系统，而信息保密和系统安全的工作并没有随着计算机网络技术的飞速发展得到更好的改进，于是互联网上的攻击和破坏事件层出不穷。网络安全技术，已经成为一个重要的学科，得到计算机领域的高度重视。人们不惜投入大量的人力、物力和财力来提高计算机网络系统的安全性。

提到计算机网络安全，首推操作系统安全。操作系统是整个系统的运行平台和网络安全的基础。Windows Server 2003是当前最普及的服务器操作系统之一，具有高性能、高可靠性和高安全性等特点。但因服务器操作系统的特殊性，使其在默认安装完成后还需要网络管理员对其进行加固，进一步提升服务器操作系统的安全性，以保证应用系统以及数据库系统的安全。

对于普通PC机而言，大多数人会选择安装杀毒软件和防火墙，不过杀毒软件对病毒反应的滞后性使得它心有余而力不足，只有在病毒已经造成破坏后才能被发现并查杀。其实大多数人都忽略了Windows系统本身的安全功能，认为Windows弱不禁风。其实只要设置好，Windows就是非常强大的安全保护软件。Windows操作系统本身自带的安全策略非常丰富，依托Windows系统本身的安全机制，并通过杀毒软件和防火墙的配合，这样才能打造出安全稳固的系统工作平台。

Windows系统的安全管理功能在注册表中被发挥得淋漓尽致。修改注册表，可以让系统更加安全，使威胁远离用户的机器。对于系统中安全方面的部署，组策略又以其直观化的表现形式更受用户青睐。通过组策略，可以禁止第三方非法更改地址，也可以禁止别人随意修改防火墙配置参数，更可以提高共享密码强度使其免遭破解。因此如果注意使用Windows中的组策略，就可以轻松地打造一个相对安全的Windows。目录服务是一种分布式数据库，用于存储与网络资源有关的信息，以便于查找和管理。Microsoft Active Directory是用于Windows Server 2003的目录服务实现。Active Directory与安全服务紧密集成，如Kerberos网络认证协议、公钥基础设施（PKI）、加密文件系统（EFS）、安全设置管理器和组策略等。