国家信息化
计算机教育认证
CEAC
指定教材

北京大学
电子政务研究院认证
PCEG
指定教材

网络安全基础

■ CEAC国家信息化计算机教育认证项目电子政务与信息安全认证专项组
北京大学电子政务研究院电子政务与信息安全技术实验室　编著

人民邮电出版社
POSTS & TELECOM PRESS

国家信息化
计算机教育认证
CEAC
指定教材

北京大学
电子政务研究院认证
PCEG
指定教材

网络安全基础

■ CEAC国家信息化计算机教育认证项目电子政务与信息安全认证专项组
北京大学电子政务研究院电子政务与信息安全技术实验室　编著

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全基础 / CEAC 国家信息化计算机教育认证项目电子政务与信息安全认证专项组，北京大学电子政务研究院电子政务与信息安全技术实验室编著. —北京：人民邮电出版社，2008.5

国家信息化计算机教育认证 CEAC 指定教材. 北京大学电子政务研究院认证 PCEG 指定教材

ISBN 978-7-115-17811-4

Ⅰ. 网… Ⅱ. ①C…②北… Ⅲ. 计算机网络—安全技术—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2008）第 032657 号

国家信息化计算机教育认证 CEAC 指定教材

北京大学电子政务研究院认证 PCEG 指定教材

网络安全基础

◆ 编　　著　CEAC 国家信息化计算机教育认证项目电子政务与信息安全认证专项组

北京大学电子政务研究院电子政务与信息安全技术实验室

责任编辑　杨　璐

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号

邮编　100061　　电子函件　315@ptpress.com.cn

网址　http://www.ptpress.com.cn

北京顺义振华印刷厂印刷

新华书店总店北京发行所经销

◆ 开本：800×1000　1/16

印张：24.75

字数：604 千字　　2008 年 5 月第 1 版

印数：1 – 3 000 册　　2008 年 5 月北京第 1 次印刷

ISBN 978-7-115-17811-4/TP

定价：49.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223

反盗版热线：(010)67171154

内容提要

为了推进我国信息化人才建设，CEAC 国家信息化培训认证管理办公室组织 IT 和培训领域的资深专家精心编写了国家信息化计算机教育认证系列教材。本书作为国家信息化计算机教育认证项目电子政务与信息安全培训认证专项的教材之一，以国际主流的安全技术为基础，详细介绍了网络安全涉及的理论知识与应用技术。

本书根据企事业单位和信息安全从业人员的实际需求，深入浅出地介绍了网络安全的概念、常见的安全问题等，并结合实例讲解了软件系统安全技术、访问控制技术、防火墙技术、隔离网闸技术、入侵检测技术、漏洞扫描技术、虚拟专用网，以及负载均衡和网络流量控制技术等内容。

本书结构清晰，讲解详细，并在每课后配有丰富的思考和练习题。非常适合作为信息安全技术的标准培训教程，也可作为大中专院校、高职高专相应课程的教材和辅导书，还可供读者自学使用。

CEAC 国家信息化计算机教育认证

北京大学电子政务研究院 PCEG 认证

指定教材

编委会

前　言

据国际权威机构调查，中国在信息化的软硬件环境的整体投资比重与同类发展中国家相比毫不逊色，但在电子商务与电子政务等实现应用方面却远远落在了后面。要想解决这一矛盾，教育培训是至关重要的一个环节。因为企业信息化、社会信息化的根本是人的信息化。

进入“十一五”后，我国信息网络安全建设与应用领域有了较大的发展，信息化建设的重点已经进入到网络信息应用、网络信息安全应用的高速发展阶段。此时，网络信息应用的安全隐患暴露了出来。究其根本，使用者自身的素质是安全问题的主要原因之一。

可喜的是，近年来大家对信息安全有了较全面、较深入的理解，使用者对网络安全、信息传输安全、信息安全管理也有了迫切的需要。顺应这种趋势，我们开展了 CEAC 国家信息化计算机教育认证项目——电子政务与信息安全培训认证专项（以下简称“CEAC 安全专项”），旨在培养更多的信息安全专业人才。

1. 项目背景

CEAC 安全专项是在信息产业部的领导下，在 CEAC 原有数据库、网络、政务等课程培训认证体系的基础上，结合武警部队网络与信息安全重点实验室、北京大学电子政务研究院等单位多年的研究、教学经验及现有部分培训认证体系，帮助企业和政府培养具有分析能力、设计能力、实现能力和解决问题能力的实用型信息化人才。

2. 项目特点

（1）专业教学体系

项目吸取原有培训资源，培训内容涵盖网络建设、数据库、电子政务、信息安全等工作中涉及的大部分知识。课程由浅入深，分层次、分步骤进行多元立体化教学，按照企事业单位的实际需求，以应用层、技术层、决策层分类设置课程。

(2) 应用与安全结合

CEAC 安全专项体现业务应用与信息安全的结合施教，在办公电子化、业务应用信息化的基础上，重点解决企事业单位信息网络安全的建设与管理问题。

(3) 理论与实训结合

为最大程度地将理论与应用相结合，使学员在学习基本知识的同时能进行同步操作实训，CEAC 安全专项专门开发了“电子政务实训平台”和“信息网络安全实训平台”，使学习结合实际，保障学习效果。

3. 认证体系（双证）

CEAC 按照国际规范，依托 Internet/Intranet 技术，建立了远程计算机考试模式。目前，在信息安全方面设置了 3 个级别的考试：“信息安全应用专家”、“信息安全技术专家”和“信息安全决策专家”。读者只要通过相应课程的考试并合格后，就可获得由信息产业部 CEAC 认证管理办公室和北京大学电子政务研究院联合颁发的培训认证证书。

4. 实训平台

CEAC 安全专项开发的实训平台的目的是帮助学员加深对相关理论知识的理解，模拟行业安全案例，生动直观地使学员掌握相关产品在实际环境中的技术应用。它包括以下几个部分。

- 防火墙实训平台：掌握市场主流访问控制类产品的应用方法。
- IDS 实训平台：掌握市场主流入侵检测产品的应用方法。
- VPN 实训平台：掌握市场主流 VPN 产品的应用方法。
- 网闸实训平台：掌握市场主流网闸隔离技术。
- 漏洞扫描实训平台：掌握市场主流漏洞扫描产品的应用。
- CA 实训平台：掌握市场主流身份认证与鉴别技术产品的应用方法。

5. 教学支撑

(1) 教学资源包

课程方案配套开发“立体化教学支持资源包”，提供相关培训认证课程的现代教育技术支持手段，提供统一的教学资源，并规范课程教学过程，旨在帮助授课老师迅速把握课程的内容实质，提高备课和教学效率，也帮助学生更有效、迅速地掌握有关知识点、技能点，适应认证考试平台提供的技术支持。教学资源包包括内容如下。

- 教学大纲：课程纲要及授课重点。
- 教学教案：教师制定讲课计划、备课的主要参考手册。
- 教学素材：演示文档、案例。
- 实验手册：结合应用案例、利用实训平台模拟搭建应用环境的实验教学手册。
- 操作手册：实训平台设备操作说明。
- 试题库：模拟试题及考核内容，包括实训上机操作考核试题。
- 考试大纲：考核要点，复习指南。
- 考试系统：统一考试平台。

(2) 施教机构：北京大学电子政务研究院

CEAC 安全专项借力北京大学电子政务研究院多年研究培训经验，结合武警部队网络与信息安全重点实验室的先进技术支撑，以应用为先导，以安全为核心，组织专业授课教师进行培训和教学。

信息安全类教材严格按照国家信息化计算机教育认证项目的规划要求，由 CEAC 信息化培训认证管理办公室组织 IT 和培训领域的资深专家精心编著。教材以企事业单位的信息安全需求为依据，结合国际主流的信息安全技术，在强调培训结果实用有效的同时，还符合客观的培训学习的规律。

在编写信息安全类教材之前，我们经过了大量的培训实践。在培训中我们明显地感到，不同类型的用户对安全技术要求千差

万别，通过短短的几本书是无法满足他们的所有要求的。因此，我们归纳总结、精心挑选了那些最有价值和应用范围最广的技术，提供了大量具有代表性的示例和经验，希望能帮助用户熟练地掌握和使用这些技术，并能通过举一反三来提高学习效果。

严谨、求实、高品质是本系列教材追求的目标，尽管我们力求准确和完善，但由于时间紧迫，水平有限，书中难免会存在一些不足之处，衷心希望广大读者批评指正，并对教材的不足之处提出宝贵意见，我们将努力为您提供更完善的服务与支持。参与本书工作的还有史长虹、潘莹等，在此表示感谢。

CEAC 信息化培训认证管理办公室

武警部队网络与信息安全重点实验室

北京大学电子政务研究院

目　录

第1章

网络安全概述

本章要点

- ☆ 计算机网络安全的基本概念
- ☆ 计算机网络的主要安全威胁及产生的原因
- ☆ 主动攻击和被动攻击的概念
- ☆ IP 报头结构和 IP 协议的主要功能
- ☆ TCP 报头结构和主要功能
- ☆ IP 和 TCP 的安全漏洞
- ☆ 缓冲区溢出攻击和防御方法
- ☆ IP 欺骗产生的原因和防御方法
- ☆ 常见的网络应用服务的安全威胁
- ☆ 计算机网络中应用的安全技术

本章导读

本章将深入浅出地介绍计算机网络安全的概念，并说明网络中的安全威胁。然后对 IP 协议和 TCP 协议进行详细介绍，并讨论它们存在的安全问题和防御方法。最后对常见的网络安全威胁和安全技术进行概括介绍。

1.1 网络安全的概念

随着计算机网络的迅速发展，特别是 Internet 在全球的普及，计算机网络的安全问题已经引起人们的极大关注。由于计算机网络的安全直接影响到政治、军事、经济以及日常生活中的各个领域，因此如何有效地保证网络安全，已经成为计算机研究与应用中一个重要的课题。

1.1.1 什么是网络安全

什么是网络安全呢？国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此可以这样理解计算机网络的安全：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多门学科的综合性学科。从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全的具体含义会随着“角度”的变化而变化。比如，从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改和抵赖等手段侵犯用户的利益和隐私。从网络运行和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作进行保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。