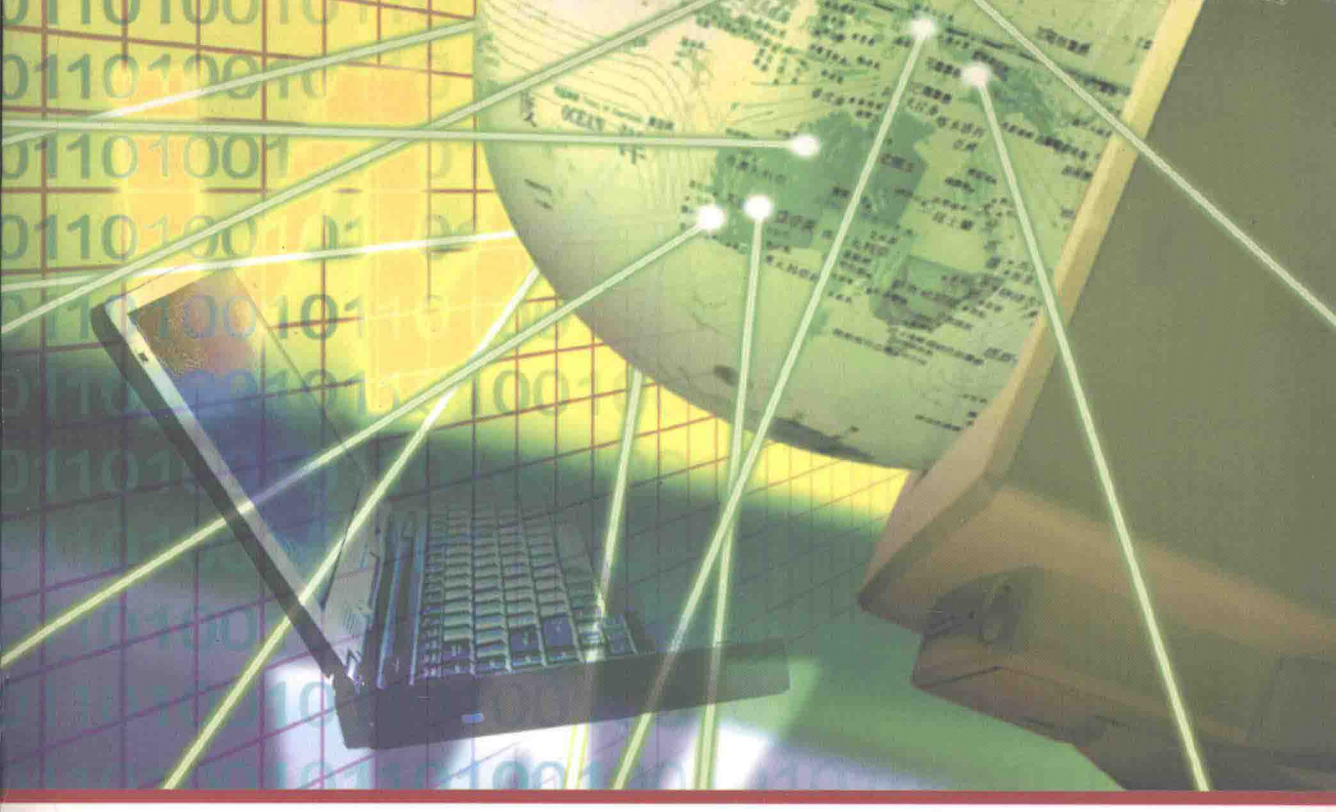

信息产业部信息化推进司指定国家信息化培训教材

信息安全技术

国家信息化安全教育认证管理中心
Informatization Security Education Certification
编著

广州出版社

信息产业部信息化推进司指定
国家信息化培训教材

信息安全技术

Information Security Technology

ISEC 国家信息化安全教育认证管理中心　编著

广州出版社

图书在版编目(CIP)数据

信息安全技术/ISEC 国家信息化安全教育认证管理中心编著
—广州：广州出版社，2003.12
ISBN 7-80655-565-X
Ⅰ.国… Ⅱ.1… Ⅲ.计算机网络-安全技术-技术手册 Ⅳ.TP393.08-62
中国版本图书馆 CIP 数据核字(2003)第 083293 号

信息安全技术
Information Security Technology

出版发行 广州出版社
地址：广州市人民中路同乐路 10 号 邮政编码：510121
印 刷 广州市番禺友联彩印厂
地址：番禺区沙湾陈涌工业综合开发区 邮政编码：511400
责任编辑 欧阳杰锋
责任校对 一 文
封面设计 谢成华
开 本 787×1092 1/16
总 印 张 44.25
总 字 数 533 千
印 数 1-5000 套
版次印次 2003 年 12 月第 1 版第 1 次
书 号 ISBN 7-80655-565-X/TP·8
总 定 价 96.00 元(全两册)

发行专线 020-37602590 020-83794401
经 营 部 广州市合群一马路 111 号广东省图批 112 档

编委会成员名单

编委会主任：宋　玲　国家信息化推进工作办公室主任

信息产业部信息化推进司司长

编委会副主任：赵小凡　国务院信息化工作办公室推广应用组副组长

原信息产业部信息化推进司副司长

蔡金荣　原国家税务总局信息中心主任

中国税务协会教授级高级工程师

曲成义　中国航天工业总公司第七零一研究所高级研究员

沈志工　公安部科技局总工程师研究员

王玉学　中国人民解放军体育学院副院长、教授

邹　生　广东省信息产业厅副厅长、博士、高级工程师

编委会成员：张会生　张宝泰　洪京一　林　鹏　孙论强　刘树安

许增元　霍　光　刘　旸　马志谦　宁宇鹏　薛静锋

李　晖　阎　慧　王　宏　罗耀春　胡　铮　祁　明

张　艺　周　涛　谢赞福　李振坤　赵　科　蔡贤庆

序　言

党的十五届五中全会把大力推进国民经济和社会信息化放到了覆盖现代化建设的全局高度，这标志着我国信息化建设进入了一个全面快速发展的重要时期。信息化建设是渗透在政府行政管理、社会公共服务和企业生产经营各领域并具有丰富内涵的一项开拓性事业。在这项事业快速发展的同时，也出现了利用传播电脑病毒、进行非法入侵等手段对信息系统实施破坏的恶性事件，对我国的信息化建设以及政府、企业等部门的正常运行造成了极大的危害。信息网络安全的保障成为国家信息化工作中的一项重要内容。

对于信息化建设问题，党中央高度重视，《中共中央关于制定国民经济和社会发展第十个五年计划的建议》不仅明确了信息化的重要战略地位和发展思路，还指出了在全社会普及信息化知识的重要性和必要性。这是“十五”计划期间国家信息化人才培养工作的重要指导方针。没有大批的懂技术会管理的建设型和应用型信息安全人才，就难以承担国家和时代赋予我们的信息化建设重任，我们必须在全社会范围内普及信息安全知识，增强信息安全意识，提高信息安全技术应对能力。

ISEC 国家信息化安全教育认证管理中心组织编写的信息安全培训教材，是面向党政机关、企事业单位、直至广大计算机爱好者使用者的普及型读物，有助于提高各级领导与基层工作者的信息安全意识。同时，这部教材也涵盖了病毒防控、

建立安全保障体系等方面的内容，对于广大的计算机用户具有一定的指导意义。相信这部教材的出版会使读者在了解信息安全知识、防止电脑病毒感染、非法入侵、掌握相关技术方面有所获益。

二零零三年十二月

前　言

自从计算机网络诞生以来，安全问题随着网络应用的发展变得越来越重要。尤其是近几年来，随着 Internet 的蓬勃发展，网络设备（各种线缆、集线器、路由器等）的价格逐渐降低，越来越多的设备连接到网络上，越来越多的人使用网络，安全的问题也就变得越来越尖锐。现在 Internet 比以往任何时候都更可供使用，网络带宽也日益增加，访问速度更快，尤其是“宽带接入”的兴起，使人们任何时间、任何地点访问 Internet 变得可能。昨天看起来不可能的事情，在网络带宽允许的条件下也会变得可能。

与此相应的是，黑客们不断地想出新办法，通过利用服务器上的错误、Web 浏览器的缺陷、访问权限的配置不当、口令设置的脆弱性、特洛伊木马程序以及其他各种各样的管理漏洞来入侵网络。更糟糕的是新发现的安全上的漏洞很快就被公布到网上，甚至有人将这一过程编写成脚本，这样那些没有任何经验的人也能发现这些漏洞并利用它来破坏网络。

这个世界上没有绝对的安全。不存在绝对安全的服务器、路由器、网络操作系统或其他网络组件，也没有什么不可摧毁的网络，除非将计算机从网络中断开。

这样，对用户来说，最好的防范方法就是具备充足的信息安全方面的知识。本书可以帮助读者做好这方面的起始工作，但是要强调一点，即使这样，也不能保证您的网络不被入侵，因为网络世界有太多的不确定性，你永远都不会知道所有的事情，学会所有的方法。

同时，在保卫信息和系统的战斗中，用户并不孤单，他们有很多伙伴。这些伙伴包括网络安全分析专家和公司；政府和教育部门的网络安全机构；当然也包括了网络安全的产品，如防火墙和入侵检测系统。在本书中都提到了这些伙伴，并且对第三类伙伴作了重点介绍。虽然本书中重点介绍了信息安全中可以使用的技术、产品，但是本书始终围绕的主题是：

安全是一个过程，安全不能单单靠产品和技术实现。安全是一个包括了硬件、软件、网络、人力因素以及四者交互接口的复杂系统，在这个系统中任何一个环节出现问题或者交互接口出现问题都会使精心构筑的安全系统失效。

所以，本书也强调了教育/培训的重要性。通过对用户的教育/培训，可以防止社交欺骗的攻击、口令攻击和一些其他形式的来自网络内部和外部的攻击。如果没有对网络用户进行教育/培训并取得他们的合作，想要保持长久的安全是不可能的。

本书编写的目的就是帮助读者加强对安全的理解，不要因噎废食，并指导读者适当地设置安全措施，在安全受到破坏时可以探测出来。

本书在编写过程中得到了信息产业部信息化推进司的大力支持；也得到了中国航天科技集团公司第 710 研究所总工程师、863 专家级专家

曲成义研究员，原国家税务总局信息中心主任蔡金荣高级工程师，中华人民共和国公安部科技局总工程师沈志工研究员，ISEC 国家信息化安全教育认证管理中心刘旸主任、马志谦主任，ISEC 国家信息化安全教育认证广东省管理分中心胡铮主任的热情帮助，在此一并表示深切感谢！

编著者

2003 年 12 月

内容简介

本书完整地介绍了有关网络安全的基础知识，其主要内容有：网络基础知识；各种不同网络的运作方式；网络潜在的安全漏洞；查找和修复漏洞的方法；病毒基础知识以及防病毒的基本原理和方法；操作系统安全基础知识；各种网络防火墙技术原理的应用方式；入侵检测技术的原理以及应用方式。书中还通过对许多具体实例的讲解，指导读者在网络中采取各种保护措施。

通过对本书的学习，读者可以解决常见的网络系统和协议的问题，保证系统工作正常和安全；掌握增强网络安全性的工具的使用方法和技巧，如防火墙和入侵检测系统的配置和应用。无论读者是网络新手还是富有经验的网络高手，都可以从本书中获得所需要的答案、解释和实例。

本书适用于网络管理员、信息安全管理人员、各高等院校计算机及相关专业以及关注网络安全的技术人员和各级主管人员阅读。

目 录

操作系统安全

防火墙技术

入侵检测技术