清华大学计算机安全译丛

PEARSON Prentice Hall

计算机安全基础

Computer Security Fundamentals

Chuck Easttom 著
贺民 等 译

PEARSON Education

清华大学出版社

清华大学计算机安全译丛

计算机安全基础

Computer Security Fundamentals

Chuck Easttom 著
贺民 等 译

清华大学出版社
北京

EISBN: 0-13-171129-6

图书在版编目(CIP)数据

计算机安全基础/(美)伊斯特姆(Easttom, C.)著;贺民等译. —北京: 清华大学出版社, 2008.10

书名原文:Computer Security Fundamentals

ISBN 978-7-302-17627-5

Ⅰ. 计… Ⅱ. ①伊… ②贺… Ⅲ. 电子计算机—安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2008)第 073238 号

责任编辑: 龙啟铭 李玮琪

责任校对: 徐俊伟

责任印制: 杨 艳

出版发行: 清华大学出版社

http://www.tup.com.cn

社 总 机: 010-62770175

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

地 址: 北京清华大学学研大厦 A 座

邮 编: 100084

邮 购: 010-62786544

印 装 者: 北京鑫海金澳胶印有限公司

经 销: 全国新华书店

开 本: 185×230 **印 张**: 17.75 **字 数**: 424 千字

版 次: 2008 年 10 月第 1 版 **印 次**: 2008 年 10 月第 1 次印刷

印 数: 1～3000

定 价: 35.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。

联系电话: 010-62770177 转 3103 产品编号: 026833-01

安全系列丛书

安全系列丛书是为将要从事信息技术安全职业的学员准备的一套丛书。这套丛书提供了来自业界专家的实践箴言，和对你手把手的培训。该丛书中的每本书，都列举了现实生活中大量的例子。这些例子能帮助你将所学到的知识应用到你的工作中去。以下是本书的几个关键元素，这些元素的目的是帮助学员解决学习过程中的一些问题。

本章目标：这些扼要、可行的目标概括了该章将涵盖哪些内容。

本章导论：每章开始先阐释一下每个主题的重要性，以及这些主题在整本书篇章结构中的地位。

实例：从书中提取出概念，而且展示这些概念是如何用在实际场所中的。

提示：和主题相关、但是超出了本书讨论范围的额外信息。

注意：不可忽视的、关键的信息。这些信息和上下文直接相关。

技能测试：每章末都附有习题，这些习题呼应该章目标，巩固相关的知识点。每章有四种题型：

- **多项选择题**：测验读者对该章内容的理解程度。
- **练习题**：围绕章节中出现的个别概念设计的简要、引导性的课程项目。
- **项目题**：综合一章内若干知识点的较长、引导性的课程项目。
- **案例研究**：运用该章中的知识点来解决问题的实际场景。

本系列丛书包括：

- 计算机安全基础
- 信息安全：原理与实践
- 防火墙与 VPN：原理与实践
- 安全策略与规程：原理与实践
- 网络防御与安全对策：原理与实践

“计算机安全”类图书还有：

书　名	书　号	定　价
密码学与网络安全	978-7-302-11490-1(翻译版)	43.00 元
	978-7-302-09967-3(影印版)	48.00 元
网络安全基础：应用与标准(第 3 版)	978-7-302-15435-8(翻译版)	39.00 元
	978-7-302-15451-8(影印版)	39.00 元
经典密码学与现代密码学	978-7-302-10740-8(翻译版)	35.00 元
	978-7-302-11156-6(影印版)	23.00 元
网络安全：加密原理、算法与协议	978-7-302-15259-0	39.00 元

译者序

近年来，随着计算机和 Internet 的广泛普及，各行各业对计算机的依赖性日益增强，许多计算机中存储着关乎个人、公司甚至国家机密的重要信息，但我国计算机安全防护能力尚不发达，计算机很容易受到内部窃贼、计算机病毒和网络黑客的攻击，具有极大的风险性和危险性。重要数据、文件的滥用、泄露、丢失和被盗，不仅会给国家、企业和个人造成巨大的经济损失，而且严重危及到国家安全和社会稳定。如何保护计算机中的信息不被非法获取、盗用、篡改和破坏，已成为令人关注和急待解决的问题。

本书详细介绍了信息安全领域的各个方面，主要内容有：基本的计算机安全知识；网络操作的实际工作经验；评估系统脆弱性的工具使用；各种黑客攻击类型；拒绝服务；系统评估与防护；加密；各种 Internet 犯罪形式，如欺骗和网络犯罪、网络工业间谍网络恐怖袭击和信息战；网络侦查；计算机安全软硬件。

本书具有完善的知识体系。知识的讲解细致详尽，循序渐进，通俗易懂，易于入手，深入浅出地剖析，逐步提高读者的使用能力，巩固学习技能。

另外，本书注重实践、强调实用。大量的练习，由简单到复杂，完全覆盖了网络安全应用的各个方面涉及的知识内容。辅助功能讲解的练习（in Practice）以及课后练习中的大量选择题（测试读者对知识的理解程度）、练习题（围绕章节中出现的个别概念设计的简要、引导性的课程项目）、工程题（综合一章内若干知识点的较长、引导性的课程项目）和案例研究（运用该章中的知识点来解决问题的实际场景），可以在理论知识的学习基础上边学边练，通过实际操作理解各种功能的实际应用。针对各种练习，书中提供了详细的操作步骤，注意事项，初学者以及具有一定基础的中级读者，只要按照步骤一步步学习，都能完成实例练习，并通过技巧的提示达到举一反三的目的，在较短的时间内快速掌握知识应用的精髓。

本书主要由贺民翻译，参加翻译的还有韦笑、王雷、李志云、李晓春、陈安华、孙宏、赵成璧、侯佳宜、许伟、戴文雅、于樊鹏、刘朋、王嘉佳、李腾、邓卫、邓凡平、陈磊、李建锋、樊旭平、唐玮、周京平、李强、赵东辉、吴江华、孙燕、周刚、高强等人。虽然竭尽所能，但由于水平有限，错误和疏漏之处，烦请读者批评指正。

前言

本书是一本入门书籍，从总体上介绍了信息安全领域的各个方面，描述了黑客如何定位系统、获取信息并用之攻击系统。通过对本书的学习，读者可以了解如何利用密码工具以及网络扫描工具防护自身系统；同时，本书还介绍了安全侵入的细节，但要注意，本书不是一本入侵手册，不是写给黑客的。本书通过解释说明、定义和各种例子，来深入讲解数据、计算机以及网络防护的重要性，而且还介绍了各种防护重要信息的安全措施所采取的操作步骤。

最后，本书主要以 Windows 系统环境为例来介绍安全知识，但其中的原理和概念是普遍适用的。之所以选择 Windows，是因为其应用范围广泛，受攻击的几率也比较大。

读者对象

本书主要面向希望扎实了解计算机安全概念的读者。本书虽然是一本基础丛书，但要求读者是熟练的计算机用户，能够使用计算机工作或学习，并熟练使用电子邮件和 Web 浏览器，了解基本的术语如 RAM 和 USB 等。读者应该具备基本的计算机知识，但不需要系统学习计算机课程。

计算机科学、计算机信息系统专业之外的读者也会发现本书十分有用，特别是相关法律工作者和电子商务人员。

本书主要内容

本书概要地介绍了网络犯罪和计算机安全。第 1 章详细介绍了网络犯罪和计算机安全，并详细阐述了网络犯罪的严重性以及学习系统防护的必要性。第 1 章还介绍了基本的计算机安全知识，包括威胁分类、常见攻击类型、一些术语和范例等，以及在法律许可范围内的安全框架。在第 1 章最后描述了一些安全资源，并在后面的练习中实践了一些工具的用法。

第 2 章介绍的内容是网络安全最重要的几个方面之一：网络操作的实际工作经验。计算机经验比较丰富的读者可以快速浏览本章，系统地复习一下这些知识。初学者通过对本章的学习将能够了解到基本的网络模型及其工作机制，在后面的练习中可以动手使用 IPconfig、tracert、ping 等工具，以便

加强对网络的理解，并学会如何防护网络安全。

第 3 章介绍了一些评估系统脆弱性的工具（黑客经常使用这些工具），并讲述了网络安全管理者如何利用这些工具评估系统的安全性，以免受到攻击；还提供了一些实践内容以使读者了解最常用的端口扫描工具的用法，并在实践中加深学习。

第 4～5 章主要介绍各种黑客攻击类型。第 4 章讲述拒绝服务，重点介绍了 SYN 泛洪、Smurf 攻击和分布式拒绝服务攻击；同时还通过一些真实的拒绝服务攻击案例来说明此类攻击所造成后果的严重性，以及如何应对。第 5 章介绍了恶意软件、病毒、特洛伊木马、缓冲区溢出攻击、间谍软件等，也通过一些真实例子来揭示这些威胁所在，并说明如何利用检测和清除工具，如 Norton、McAfee 来进行防护。

学完本书前面的内容，读者已经了解了各种系统面临的威胁以及防护、检测、清除这些威胁的措施。第 6 章主要介绍系统评估与防护基础，第 7 章讲解加密，这两章的内容跳出各种攻击，从更为宽广的视角来审视计算机安全管理。在第 6 章，读者将会了解到各种安全防护基础知识：脆弱性探测、设置策略、咨询顾问、防护个人工作站以及服务器、安全浏览网站。第 7 章介绍了加密，包括加密的历史和现代密码学方法。这两章拓展了读者在安全管理领域的视角，至少能够使读者有能力提出正确的问题，为深入学习打下基础。

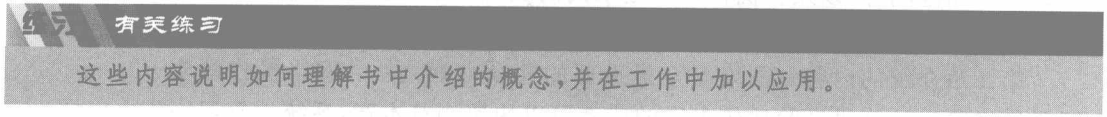
第 8～10 章介绍了 Internet 上的各种犯罪形式。第 8 章介绍了 Internet 欺骗和网络犯罪，讨论了身份盗用、网络侵犯。第 9 章介绍了网络工业间谍，第 10 章介绍了网络恐怖袭击和信息战。第 11 章讲解网络侦查，继续前 3 章的内容，描述了黑客如何利用 Internet 信息实施犯罪，并解释各种网络犯罪的原理，以便读者掌握如何应对各种犯罪并进行防护。每一章都有一些真实的案例用以说明各种犯罪方法，以加强读者对网络安全重要性的认识。

第 12 章的内容涉及计算机安全软硬件，深入到计算机安全的技术层面，介绍了各种与安全相关的软硬件，其中一些在前面的章节里已提到过。本章的目的就是使读者更为深入地理解病毒扫描器、防火墙、入侵检测系统和反间谍软件。本章的内容对于即将从事计算机安全工作的读者来说是非常有用的。

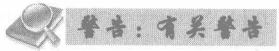
附录中是一些附加内容，提供了各种有用的网站链接资源、安全清单模板、术语表和参考资料。

本书约定

为了帮助读者获得更多的知识，我们在书中使用如下约定：



这里提供超出本书范围的相关主题信息。



警告在边栏出现，它们标志着非常重要的信息，需要牢记。这些信息与正文内容密切相关。

有边框和编号的代码段，可以从本书配套网站上下载（www. prenhall. com/security）。

新术语的出现，使用斜体字，加粗的形式表示。

这个图标表示可以在本书配套网站（www. prenhall. com/security）找到更多信息。

教师和学生资源

教师资源仅提供给教师，需要这些资料的老师请与 longqm@tup. tsinghua. edu. cn 联系。它包含：

- 教师手册：提供教学提示、每章导言、教学目标、教学建议以及章末习题的答案。
- PowerPoint 幻灯片演示：每章课件，用于教学。
- 题库：用 Prentice Hall 的 TestGen 软件可以使用这个 TestGen 兼容的题库文件。该软件在 www. prenhall. com/testgen 网站上可以免费下载。TestGen 是试题生成器，可以以适合不同教学情形的各种形式打印。该程序提供许多选项，可以组织和显示题库和测验。它具有内置的随机数字以及文本生成器，通过计算可以创建试题的多个版本，所提供的测试题可能比题库问题更多。强大的搜索和排序功能，使用户能够轻松找到试题，以需要的方式安排它们。

本书配套网站

www. prehall. com/security 是本书配套网站，这是一个 Pearson 学习工具，可以为学生和教师提供在线支持。其内容主要包括如下几方面。

- 交互式学习指南。这是基于 Web 的交互式测试，学生可以在这里方便地进行在线测试，自行检测是否掌握了本书的相关知识。
- 附加的 Web 工程和资源，练习每章所学的基本概念。
- 认证信息（来自附录 A）、有用 Web 资源的链接（来自附录 B）和策略以及检查列表的模板（来自附录 C）。

作者简介

Chuck Easttom 在 IT 行业具有多年的实践经验，随后有 3 年时间，在一家技术学院教授计算机科学，包括计算机安全课程。后来，他又离开学术界，转向 IT 业，在美国得克萨斯州的达拉斯的一家公司担任 IT 经理。除了日常事务之外，他还负责计算机安全。他编写过 7 本有关程序设计、Web 开发和 Linux 的图书。Chuck 曾荣获 20 多个不同的证书，包括

CIW 安全分析师(Security Analyst)、MCSE、MCSA、MCDBA、MCAD、Server＋和其他证书。在 ComTIA(Computer Technology Industry Association,计算机技术协会),他作为相关科目的专家,曾制定和修订 4 种认证考试,包括 Security＋认证的初始创建。业余时间,Chuck 还在达拉斯地区学院任兼职教师,教授各种课程,包括计算机安全。他时常还作计算机安全的咨询工作。

Chuck 经常作为计算机团体的客座演讲人,主要讨论安全问题。他的联系方式如下。

网站:www. chuckeasttom. com

电子邮件:chucjeasttom@yahoo. com

目录