清华大学计算机安全译丛

PEARSON
Prentice
Hall

网络防御与安全对策

Network Defense and Countermeasures

原理与实践
Principles and Practices

Chuck Easttom 著
张长富 等 译

PEARSON
Education

清华大学出版社

清华大学计算机安全译丛

PEARSON
Prentice
Hall

网络防御与安全对策

Network Defense and Countermeasures 原理与实践 Principles and Practices

Chuck Easttom 著
张长富 等 译

清华大学出版社
北京

EISBN: 0-13-171126-1

北京市版权局著作权合同登记号 图字: 01-2007-5193 号

图书在版编目(CIP)数据

网络防御与安全对策——原理与实践/(美)伊斯特姆(Easttom, C.)著;张长富等译. —北京: 清华大学出版社,2008.10
书名原文: Network Defense and Countermeasures: Principles and Practices
ISBN 978-7-302-17777-7

Ⅰ. 网… Ⅱ. ①伊… ②张… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 077838 号

责任编辑: 龙啟铭 李玮琪
责任校对: 徐俊伟
责任印制: 王秀菊

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: 010-62772015, 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 刷 者: 北京鑫海金澳胶印有限公司
装 订 者: 三河市溧源装订厂
经 销: 全国新华书店
开 本: 185×230 **印 张**: 21.75 **字 数**: 525 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: 43.00 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:026830-01

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
- 安全策略与过程：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

本书采用教科书形式、以理论基础与实际应用结合的方法，全面介绍了与网络安全相关的各种内容，覆盖了防御对策、攻击形式以及与计算机安全相关的策略，填补了其他一些安全图书某些内容缺失的空白。

本书以平易近人的语言详细阐述了防火墙、入侵检测系统、加密基础、操作系统加固、抵御病毒/木马/间谍软件攻击以及安全策略和安全标准的实际应用。为了巩固学习的知识，在本书每一章的末尾，都给出了多项选择题、练习、项目和一个案例研究，为学生提供了动手实践和深入理解本章内容的机会。

本书适合于作为学习网络安全的教材，也是网络管理员、安全专业人员以及安全审计专业人员日常工作的手边手册。

参加本书翻译工作的人员包括：张长富、蔡建章、李匀、张建安、邓铁洪、徐君、杨莹、李强、李勇、蒋恩骏、杨文保、苏辛、周成兴、魏敬安、朱建波、徐志平、赵杰辉、傅祎、郭碧莲、郭洵、洪晓煜、黄宣达、江松波、柯渝、赖曲芳、廖阳、刘文红、贺军等，张福林先生对本书中的一些关键段落和疑难之处作出了详细的解释和指导，在此深表感谢。限于译者水平，错误和遗漏之处，敬请读者批评指导。

前言

今天 IT 行业最热门的课题是计算机安全。新闻中充满了关于黑客攻击、病毒和身份窃贼的报道。安全的基础是保护机构的网络。本书提供了网络防御的全面介绍，向读者介绍了网络安全威胁和保护网络的方法。第 3～5 章专门介绍了防火墙和入侵检测系统，第 6 章提供了加密的基础知识。将对网络的攻击、用于确保安全的设备和技术以及像加密这样的概念结合起来的信息为读者提供了有关网络防御的坚实、内容广泛的方法。

本书提供了理论基础与实际应用的结合。每一章的末尾都给出了多项选择题、练习题、项目题和一个案例研究。成功学完本教材，包括每章末尾的材料，读者应该能够深入地理解网络安全。本书向读者提供了额外的资源，它们扩充了相应章节提供的内容。

读者

本书适合于对网络运行（包括基本术语、协议和设备）有了基本了解的读者。读者不需要拥有比初步计算机课程要求的更多的数学背景知识。

本书概述

本书将带你穿越错综复杂的保护网络、避免攻击的迷宫。第 1 章“网络安全引论”简要介绍网络安全领域，第 2 章“攻击类型”解释了对网络的威胁，包括拒绝服务攻击、缓冲区溢出攻击以及病毒。

第 3 章“防火墙基础”、第 4 章“防火墙实际应用”、第 5 章“入侵检测系统”和第 7 章“虚拟专用网”，详细叙述了各种安全技术，包括防火墙、入侵检测系统以及 VPN。这些项目是网络安全的核心，因此本书的一个重要部分就是专注于确保读者全面理解隐藏在它们背后的概念以及实际的应用。在每一案例中，都包括了给定网络下选择恰当技术的实际指导。

第 6 章“加密”提供了加密的坚实基础。这个主题很关键，原因在于，计算机系统本质上就是一个用于存储、传输和操纵数据的设备。无论网络如何安全，如果它传输的数据不安全的话，就存在相当大的危险。

第 8 章“操作系统加固”讲授操作系统的加固方法。第 9 章“防御病毒攻击”和第 10 章“防御木马、间谍软件、广告软件的攻击”，为读者提供了特殊的

防御策略和技术来抵御最常见的网络威胁。第 11 章“安全策略”向读者提供了安全策略的概貌。

第 12 章“评估系统”向读者讲授了如何评估网络安全，这包括检查策略的指导原则以及网络评估工具概览。第 13 章“安全标准”给出了常用安全标准的概览，比如 Orange Book（橙皮书）和 Common Criteria（通用评估准则）。本章也讨论了各种安全模型，比如 Bell-Lapadula。

第 14 章“基于计算机的间谍和恐怖主义”讨论了基于计算机的间谍和恐怖主义，这是计算机安全社团日益关心的两个主题，也是很多书经常忽略的两个主题。

为了帮助读者获得更我的知识，我们在书中使用如下约定：

练习：有关练习

这些内容说明如何理解书中介绍的概念，并在工作中加以应用。

提示：有关提示

这里提供超出本书范围的相关主题信息。

警告：有关警告

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。

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。
- PowerPint 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。强在原搜索和排序功能，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。

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 拥有 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。Chuck 的业余时间还是达拉斯地区学院的兼职教师，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，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

质量保证

我们愿意把我们的感谢奉献给质量保证小组，感谢他们对细节的关注和努力，从而确保了本书的质量。

技术编辑

Ken Dewey

Computer Information Technology（计算机信息技术系），Rose State College（罗斯州立学院）

Lance Parks

Computer Information Technology（计算机信息技术系），Cosumnes River College（Cosumnes River 学院）

校阅人

Jaime B. Sainz

Computer Science（计算机科学系），Sierra College（Sierra 学院）

Kathleen Murray

Computer Networking（计算机网络系），Los Medanos Community College（Los Medanos 社区学院）

Linda Woll

Computer Science（计算机科学系），Montgomery County Community College（蒙哥马利郡社区学院）

致谢

虽然只有一个名字出现在这本书的封面上，但仅有一个人是不可能完成这部著作的。我借此机会感谢参与本书出版的少数几个人。首先要感谢的是，Prentice Hall 的编辑人员在这本书上做出了极大的努力。没有他们，这个项目就不可能完成。我还要感谢我的妻子 Misty 和我的儿子 AJ，感谢他们毫不动摇的支持。无论什么时候，当我在做一个项目时，他们的耐心和理解是该项目成功的关键。没有这样的支持，不管是这本书还是其他任何工作都是不可能完成的。

目录