Broadview
www.broadview.com.cn

PRENTICE HALL

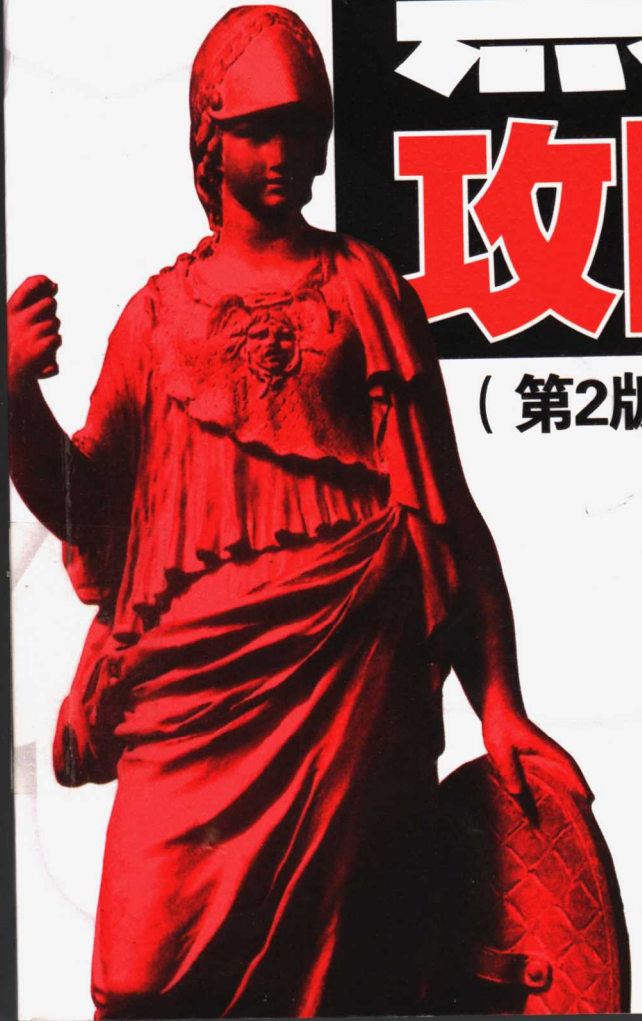
安全技术大系

COUNTER HACK RELOADED:
A STEP-BY-STEP GUIDE TO COMPUTER ATTACKS AND EFFECTIVE DEFENSES(SECOND EDITION)

黑客攻防演习

（第2版）

[美] Ed Skoudis Tom Liston 著
龚玲 张云涛 郝黎明 李敏 译



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

PRENTICE HALL

安全技术大系

COUNTER HACK RELOADED:

A STEP-BY-STEP GUIDE TO COMPUTER ATTACKS AND EFFECTIVE DEFENSES(SECOND EDITION)

黑客攻防演习

（第2版）

[美] Ed Skoudis Tom Liston 著
龚玲 张云涛 郝黎明 李敏 译

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

内 容 简 介

本书主要分为三个部分：第一部分是技术概述部分。作者阐述了网络攻防技术中的基础知识，从而可以了解攻击者是如何攻击系统的，以及了解攻击者入侵系统所采用的基本技术。在掌握该部分技术内容后，读者将能顺利地理解本书第二部分的内容，也即本书的重点部分。在这部分，作者深入浅出地介绍了当前常用的攻防技术，并详细地介绍了攻击的具体步骤，包括侦察、扫描、获取访问权限、维持访问以及掩盖踪迹等，并详细介绍了在每个攻击阶段中所使用的工具和技术手段，以及相应的防御方法。最后，本书对相关技术进行了总结，并对未来的攻防技术的发展趋势进行了预测，从而使读者能够做到未雨绸缪、及时跟上时代的步伐。

本书是一本有关黑客攻击和防御黑客的网络攻防方面的专著，可以帮助系统管理员、安全人员和网络管理员，以及其他从事网络安全的工作人员学习攻击者如何工作的，以及防御自己的系统免受攻击所用技术，以加固他们的系统，抵御各种攻击。

版权贸易合同登记号 图字：01-2006-3325

图书在版编目（CIP）数据

黑客攻防演习：第 2 版 /（美）思克迪斯（Skoudis, E.）等著；龚玲等译. —北京：电子工业出版社，2007.6
（安全技术大系）
书名原文：Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses (Second Edition)
ISBN 978-7-121-04426-7

I. 黑… II. ①思… ②龚… 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（2007）第 070984 号

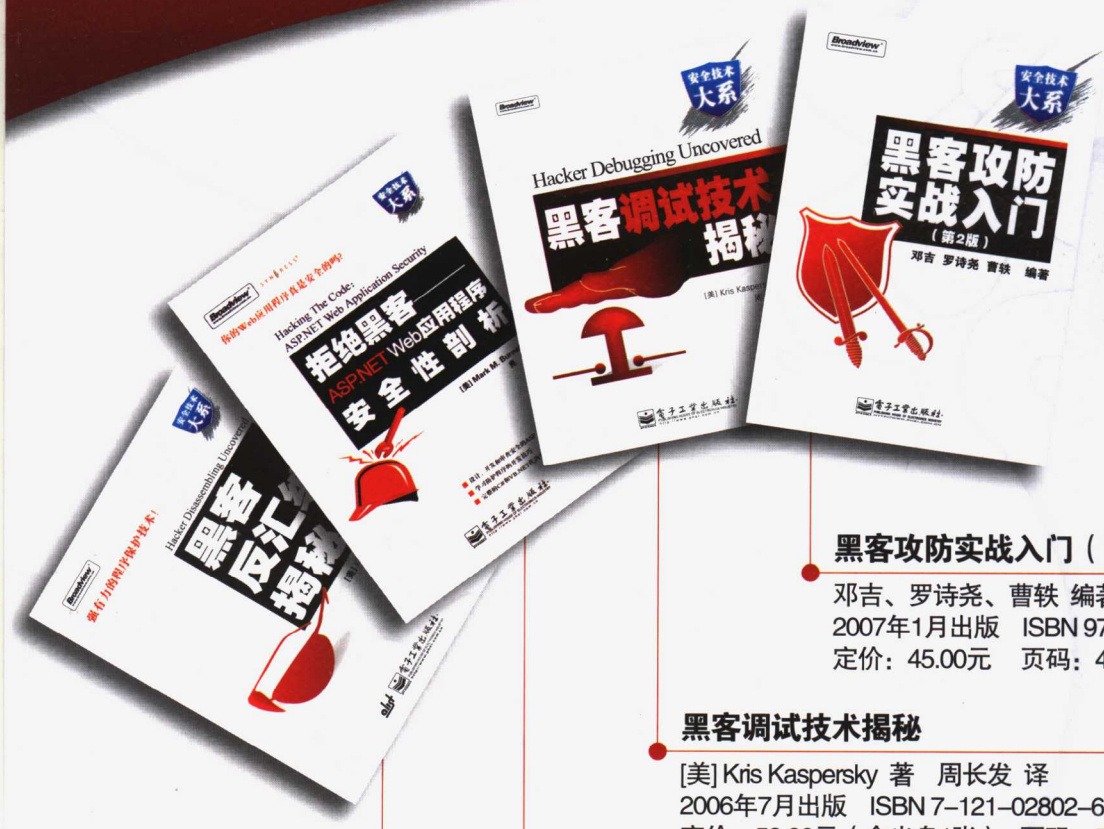
责任编辑：孙学瑛
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：34.5　字数：689 千字
印　　次：2007 年 6 月第 1 次印刷
印　　数：5000 册　　定价：69.00 元

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。

黑客攻防大演练



黑客攻防实战入门（第2版）

邓吉、罗诗尧、曹轶 编著
2007年1月出版　ISBN 978-7-121-03709-2
定价：45.00元　页码：400页

黑客调试技术揭秘

[美] Kris Kaspersky 著　周长发 译
2006年7月出版　ISBN 7-121-02802-6
定价：59.00元（含光盘1张）　页码：517页

拒绝黑客——APS.NET Web应用程序安全性剖析

[美] Mark M. Burnett 著　良忠 译
2005年2月出版　ISBN 7-121-00405-4
定价：48.00元　页码：353页

黑客反汇编揭秘

[美] Kris Kaspersky 著　谭明金 译
2004年10月出版　ISBN 7-121-00206-X
定价：59.00元　页码：532页

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn
Broadview®
www.broadview.com.cn

发行热线：88254020　门市热线：88254043　通信地址：北京市万寿路173信箱　发行部

中国计算机网络安全应急年会
暨中国互联网协会网络安全工作年会

CNCERT/CC

每年一度的中国计算机网络安全应急年会（简称CNCERT年会）

为国内外科研、教育、学术界、电信、金融等企业界和政府相关部门提供一个全面交流的机会，在广泛的领域展示最新的研究成果和具有挑战性的实践与经历，促进跨学科的研究发现和分享新思考，积极参与国际互联网领域的合作、交流，促进中国互联网的健康发展。CNCERT年会一般包括以下领域的内容：

- 在安全事件防御、检测和响应方面的先进技术；
- 在计算机与网络安全工具方面的最新进展；
- 交流计算机安全事件响应领域的观点、经验和解决方案

2007中国计算机网络安全应急年会（第4届）简介

主办单位

国家计算机网络应急技术处理协调中心

中国互联网协会网络与信息安全工作委员会

协办单位

中国通信学会通信安全技术委员会

承办单位

电子工业出版社

大会网址 http://2007.cert.org.cn

2007年4月5日至7日，由国家计算机网络应急技术处理协调中心（简称CNCERT/CC）主办、电子工业出版社承办的“2007中国计算机网络安全应急年会”在江苏无锡召开。

本届年会以“服务信息社会，共建和谐网络”为主旨，围绕奥运安全保障、电子政务、网上金融和公共互联网安全等热门话题展开专题研讨。年会开幕式上，信息产业部蒋耀平副部长做了题为“服务信息社会、共建和谐网络”的主题发言；方滨兴院士做了题为“网络安全需求与863的技术对策”的主题报告；信息产业部电信管理局赵志国副局长做了题为“加强行业监管、保障网络安全”的报告；会议还专门邀请了国际奥组委及承担悉尼奥运会、雅典奥运会信息安全保障工作的技术专家，以及北京市奥组委技术部贾胜文副部长参加本届年会并做主题发言。国内相关政府部门、科研机构和企事业单位的200余位专业人士参加了本届年会。

信息产业部蒋耀平副部长做
“服务信息社会、共建合谐网络”的报告

方滨兴院士做
“网络安全需求与863的技术对策”的报告

2008中国计算机网络安全应急年会——诚邀您的参与

会议地点

中国深圳

会议时间

2008年3月下旬

2008年会内容

（1）您定专题：请告诉我们您所关心的话题。
（2）您定培训：请告诉我们您所感兴趣网络安全方面的培训。
（3）您的论文：本届年会将征集网络安全方面的论文，欢迎您投稿。
（4）您来交流：请告诉我们您所期待交流的专家及想了解的产品。
（5）您提建议：欢迎您的任何建议和意见，我们将根据您的建议调整会议内容。

请在第一时间将您的联系方式发送给联系人，以便我们随时向您提供会议相关进展情况。

联系人：

毕　宁（承办单位）：010-88254368，13120323280，bn@phei.com.cn，
bining2008@sina.com，　MSN：cert_cn@163.com

大会网站：

更多内容请登录：**http://2008.cert.org.cn**

对《反击黑客》的赞誉

“我终于明白了！我过去听说过 rootkit、缓冲区溢出和空闲扫描这些词，但一点不明白它们的意思。我向其他人请教，他们也不知道这些东西是如何工作的，或者至少他们不能以我能明白的方式解释。《黑客攻防演习》对这些工具给出了我所见过的最清晰的解释。谢谢！”

——Stephen Northcutt，CEO，SANS 学院

“Ed Skoudis 是一位罕见的专家，他了解各种系统的内在机理以及各种最新的攻防技术，而且能恰如其分地解释所有事情。《黑客攻防演习》第 1 版就是一本令读者陶醉的书。该书讲述的技术非常有意思并且阐述得非常清晰。……不过，有关攻击的书终将过时，因此在《黑客攻防演习》的第 2 版中，作者重写和更新了大量内容。本书出色地描述了该领域的概况。”

——摘自 Radia Perlman 为本书写的前言；
Radia Perlman 也是“计算机网络和安全”系列丛书的编辑，
“*Interconnections*”一书的作者，
Network Security: Private Communications in a Public World 的合著者

“多好的合作关系啊！在以一种清晰而有趣的方式解释最具有挑战性的安全概念时，Ed Skoudis 和 Tom Liston 显示了不可思议的才能。《黑客攻防演习》对于那些想要提高防御技能并理解计算机攻击机制的人来说是必不可少的。”

——Lenny Zeltser，“*Malware: Fighting Malicious Code*”一书的合著者

“Ed Skoudis 又成功了！在这个新版本中，Ed 将一个非凡的工作提升到更高的层次！对每个与计算机和计算机安全相关的人来说，本书是‘必须拥有’和‘必须阅读’的。”

——Harlan Carvey，CISSP，“*Windows Forensics and Incident Recovery*”一书的作者

“除了拥有渊博的网络安全知识和深刻的洞察力之外，Ed Skoudis 真正的过人之处在于，他具有以一种可理解的方式展示复杂问题的能力。本书虽然一开始似乎有一堆令人绝望的缩写词，但逐渐就变得让人轻松和熟悉。本书是理解攻击策略、攻击工具和防御的最佳资料。”

——William Stearns，www.stearns.org 的网络安全专家

“每个从事互联网安全工作的人都必须拥有本书。它包含了所有内容，从基本原则到在线攻击方法和反攻击策略的细节，写得非常吸引人。”

——Warwick Ford，“*Secure Electronic Commerce*”一书的合著者

作 者 简 介

Ed Skoudis 是位于华盛顿地区的网络安全顾问公司“Intelguardians Network Intelligence，LLC”的创始人和高级安全顾问。他的专长包括黑客攻击和防御、信息安全行业和计算机隐私问题。他为财富 500 强公司进行过无数的安全评估，设计信息安全管理模式和组织实施团队，并为金融、高科技、医疗卫生和其他行业的客户的计算机攻击进行应急响应。Ed 为美国参议院演示过黑客技术，他经常是黑客工具和防御相关问题的发言人。除了本书，Ed 还是“*Malware: Fighting Malicious Code*”（Prentice Hall, 2004）一书的合著者。他获得过 2004 年度和 2005 年度 Windows 服务器安全的微软 MVP 奖，他是 Honeynet 项目[①]的毕业生。在成立 Intelguardians 公司之前，Ed 曾在国际网络服务（INS），Predictive Systems，Global Integrity，SAIC 和贝尔通信研究所（Bellcore）担任安全顾问。

Tom Liston 是位于华盛顿地区的网络安全顾问公司“Intelguardians Network Intelligence，LLC”的高级分析师。他是流行的开放源代码网络工具 LaBrea 的创作者，为此他成为 2002 年度“*eWeek*”杂志和“*PC Magazine*”杂志评选的“基础设施（i3）革新奖”的决赛选手。他是系统网络安全（SANS）协会的“互联网风暴中心”的管理者之一，在那里，他每天处理最前沿的安全问题，并且是“Follow the Bouncing Malware”系列热门文章的作者。Liston 先生居住在富饶的大都市伊利诺伊州的 Johnsburg，他有 4 个漂亮的孩子（他们要求在这里被提及）：Mary，Maggie，Erin 和 Victoria。

---

① Honeynet 项目是一个由 30 余名安全专业组织成员组成，专门致力于了解黑帽子团体使用的工具、策略和动机以及共享他们所掌握的知识的项目。这个组织使用他们自己的资源来收集这方面的信息，其中最主要的方法是通过使用 Honeynet 来收集信息。——译者注

译 者 序

随着网络在企业活动和社会生活中占据越来越重要的位置，对网络和信息安全的需求也日益迫切。当我们的生活和社会越来越依赖于互联的计算机时，攻击也变得越来越流行和有破坏性。正因为如此，我们需要深入地了解各类攻防技术，“师夷长技以制夷”。

本书是一本有关黑客攻击和防御黑客的网络攻防方面的专著，可以帮助系统管理员、安全人员和网络管理员加固他们的系统，抵御各种攻击。作者曾在6年前编写了本书的第1版，并受到读者的广泛欢迎。然而，自第1版出版以来，计算机攻防世界已经发生了很大的变化，因此作者在新版本中更新了大量的内容，加入了第1版以后出现的新的攻击方法和相关工具，从而使读者可以了解到最新的攻击技术和发展趋势，并能在实际工作中应用这些最新的防御策略。

本书主要分为3个部分。第1部分是技术概述。作者阐述了网络攻防技术中的基础知识，从而使读者了解攻击者是如何攻击系统的，了解攻击者入侵系统所采用的基本技术。在掌握该部分技术内容后，读者就能顺利地理解本书第2部分的内容，也即本书的重点部分。在这部分，作者深入浅出地介绍了当前常用的攻防技术；详细地介绍了攻击的具体步骤，包括侦察、扫描、获取访问权限、维持访问以及掩盖踪迹等；还详细介绍了在每个攻击阶段中所使用的工具和技术手段，以及相应的防御方法。最后，本书对相关技术进行了总结，并对未来攻防技术的发展趋势进行了预测，从而使读者能够未雨绸缪，及时跟上时代的步伐。

本书的翻译和审校工作由龚玲、张云涛、郝黎明和李敏共同完成。全书包括13章，其中龚玲完成了1~4章、10~13章、前言和序言的初稿，郝黎明完成了5~8章的初稿，李敏完成了8~9章的初稿，张云涛对所有初稿进行了修订并完成最终定稿。此外，郑韶华、冯赟、黄嘉维和王锐也参与了许多有益的辅助工作，译者在此对他们的工作表示衷心的感谢。

网络攻防、黑客技术是当前计算机技术的热点之一，各种新技术、新工具层出不穷，其中许多术语尚无固定译法。此外，由于译者水平有限，译文中的不当之处在所难免，恳请同行和各位读者朋友不吝赐教。如果您能将意见和建议发往 *yuntao_zhang@hotmail.com*，我们将不胜感激。

译者

2006年8月于上海交通大学

前　言

没有互联网的世界已经淡出人们的记忆。现在我们对于在互联网上的各种活动已经习以为常，例如查看自己的银行账户和医疗记录、接受网络驾驶导航、网上聊天以及网上购物等。而许多公司离开互联网也无法生存，因为互联网已成为公司和客户之间的联系纽带。

但是互联网并非只是帮助企业联系客户、医生浏览病人的医疗记录、或朋友们相互联络，它也使攻击者能访问用户的系统以及用户所要访问的系统。

许多系统在创建初期通常是不设防的。有些系统在大学里使用，以便诚实的研究者们共享信息。有些系统在家庭使用，供单个用户做文字处理或玩游戏。伴随着互联网的诞生，以攻击系统为乐，或为表达某种政治观点而攻击系统的情况也随之出现了，其发展如此迅速，以至于人们都来不及完善这些系统。在防御者和攻击者之间将有一场旷日持久的马拉松战争。

放弃是很容易的事情，只要宣称这种情况毫无希望，就可以到佛蒙特州养兔子去了。但是正当我们的出路似乎只能是饲养数千只兔子时，具有无穷活力、热情和乐观精神的 Ed Skoudis 出现了。

Ed 是一位罕见的专家，他了解各种系统的内在机理以及各种最新的攻防技术，而且能恰如其分地解释所有事情。《黑客攻防演习》第 1 版就是一本令读者陶醉的书。该书讲述的技术非常有意思并且阐述得非常清晰。当然，书中的内容也是令人恐慌的，但是 Ed 的乐观精神贯穿本书，让我们多少安心一些。

不过，有关攻击的书终将过时，因此在《黑客攻防演习》的第 2 版中，作者重写和更新了大量内容。本书出色地描述了该领域的概况。（如读者需深入了解恶意代码的细节，强烈推荐 Ed 的另一本书“*Malware*” [Prentice Hall, 2004]。）

遗憾的是，在这场攻防大战中，一直都是道高一尺、魔高一丈。正如 Red Queen 在“*Through the Looking Glass*”一书中所说：“现在你可看到，即使竭尽全力也只能和入侵者打个平手。”这非常令人沮丧，但至少《黑客攻防演习》这本书可以让我们学到需要掌握的知识，从而尽力而为。

——丛书编辑 Radia Perlman

2005 年 9 月

新版《黑客攻防演习》序

时值午夜，我的航班刚刚降落，航班服务员就通知我们可以打开手机了。我的手机一开，就立刻嗡嗡叫了起来，这是我最近结识的一个报社记者打来的紧急电话。他快速地解释说他获得了一份恐怖分子写的宣言，这个恐怖分子在几个月前发动了一些相当恐怖的袭击，数百名无辜的人在袭击中丧生。该记者已经请专业人士翻译了这份宣言，这样他就可以请人来分析。在这份长达 30 页的文档中，这个极其邪恶的家伙迫切要求他的追随者们改变斗争策略。为了扩大他们的武力恐怖行动，现在他们计划增加计算机攻击，以便最大程度地影响那些反对恐怖主义活动的国家。该记者希望我能从技术上分析这份宣言的可行性，判断该宣言仅是烟雾弹，还是要真正需要关注的事件。

我到了旅馆房间后，快速从邮箱中收下这份宣言的拷贝。这份文档令我非常震惊。虽然在技术上并没有什么高深之处，但是它确实击中了要害。宣言的作者强调，通过使用计算机攻击来破坏敌人的经济状态，恐怖组织可以提高声望和影响力，并制造更多的恐怖行动。在讲述了其相当可怕的“动机”之后，宣言开始描述如何使用不同类型的攻击来达到恐怖主义的目的。虽然作者并没有涉及技术细节，但确实给出了大量有关计算机攻击的技术参考资料，要求他忠实的追随者努力学习异教徒的技术，从而可以进行破坏。

第二天我接到了另一个电话，这次是我的一个律师朋友打来的。他说一个计算机黑客攻入了一家公司的网络并偷窃了数百万个信用卡号码。因为攻击者偷窃了存放在计算机服务器上的整套磁条数据，这个坏家伙就可以制作相当逼真的假信用卡，并在黑市上销售。我的律师朋友希望我能调查这次偷窃行为的细节，用通俗易懂的语言来解释窃贼是如何得手的。我仔细研究了这个案例，分析坏家伙的行动步骤。我很不安地注意到，在这起重大的犯罪案例中，罪犯采用了一些相当地道的攻击技术。

在紧接着分析那些案例的日子中，我重新阅读了大约 5 年前我写的《黑客攻防演习》一书中的序。尽管它描述的是针对一个 ISP 的真实攻击，但当时仍有一种好玩的感觉。当时最大的担忧是一些 Web 站点被黑，以及我密友的老板抓狂。这些固然值得关注，却还不是世界末日。虽然在计算机攻击中有许多事情都发生了变化，但我发现一点也没有向好的方向发展。5 年前，我们面临威胁，但它通常表现为青少年在无聊时的取乐。当时我们确实面临一些厉害的罪犯，但是我们的工作也有一些乐趣。当前，随着有组织

的犯罪出现以及，是的，甚至恐怖分子掌握了计算机攻击技术，事情就变得更加困难和险恶。诚然，技术发展了，但是对我们的威胁自然也增加了。

为了强调这个问题，你不妨现在将一台未打补丁的计算机连到互联网上，估计平均不到 20 分钟，这台计算机就会完全崩溃。在不同的时候，这个存活期限会有所波动，有时甚至不到 10 分钟。在一些很好的补丁发布并很快应用后，该时限偶尔会突然提高到 30 分钟以上。但是，即使是最大的数字也是令人气馁的。在具有高度入侵威胁的情况下，现在比以往任何时候都更重要的是，计算机专家（系统管理员、网络管理员和安全人员），甚至是外行，都必须了解坏家伙们是如何进行攻击的，并具备如何进行防御的知识。如果我们不了解坏家伙们的策略，不知道如何挫败他们，他们会不断地侵入我们的计算机，造成严重破坏。他们知道如何进行攻击，并且一直在学习更多的知识。我们这些防御者也必须同样地武装起来。相对于原书，新版《黑客攻防演习》更新了大量的内容，这其中有许多是计算机攻击技术在过去 5 年中的新发展。但是，本书依然保留了原书的版式和目标：以循序渐进的方式描述攻击是如何发起的，并使用经过时间考验的实际中真正使用的技术来演示如何防御每个攻击。

最后提一点：即使我们面对的攻击变得越来越邪恶，也不要灰心丧气。面对攻击时，消沉或惊恐的态度会使你泄气和更加迟钝，从而降低防御能力。若要具有战斗力，就必须记住，我们所做的信息安全工作本质上是有趣的，甚至是开心的。极其重要的一点是，在面对这些不断升级的威胁时，我们必须勤奋。同时，我们必须努力保持积极的态度，打个漂亮仗，使我们的系统更加安全。

第 1 版的序

我的手机响了。我睡眼朦胧地瞥了一眼闹钟。哎哟！是元旦凌晨 4 点呀。不用说，那晚我睡得很少。

我拿起电话，立刻听到密友 Fred 狂躁的声音。Fred 是一家中型互联网服务提供商的安全管理员，他经常打电话向我咨询各种安全问题。

“我们在狂欢时被‘黑’了！”Fred 大叫，声音在早晨的这个时间显得格外响亮。

我揉揉眼睛，试图弄清一些事情。

“你怎么知道他们入侵了？他们做了些什么？”我问道。

Fred 回答：“他们篡改了一些 Web 页面。这太糟了，Ed。我的老板会大发脾气的！”

我问：“他们怎么入侵的？你有没有检查日志？”

Fred 结结巴巴地说：“唔，我们没有做很多日志，因为它会降低性能。我只从几台机器上获得一些日志。另外，在有日志的那些系统上，攻击者清除了日志文件。”

“你有没有在机器上安装你们操作系统厂商最新的安全补丁？”我问，试图更多地了解 Fred 采取的有关安全措施。

Fred 犹豫地回答：“我们每 3 个月安装一次安全补丁。我们最后一次安装补丁是……唔……两个半月之前。”

我挠了挠隐隐作痛的脑袋，说：“上周发布了两个比较重要的缓冲区溢出攻击。你可能碰上了它们。他们有没有安装一些 rootkit[①]？你有没有检查系统重要文件的一致性？

“你知道，我正计划安装类似 Tripwire 这样的软件，但是尚未实施。”Fred 承认。

我轻轻叹了口气，说：“好吧。保持冷静。我马上过去，这样我们可以开始分析机器的情况。”

你肯定不想碰到类似 Fred 这样的情况，我也希望减少在元旦凌晨 4 点接到电话的次数。虽然我为了保护他的名誉，在这里没有公开他的真实名字，但这种情况确实发生过。Fred 的组织没有实施基本的安全控制，当攻击者到来时就不得不付出代价。以我的经验，许多组织都会发现他们同样没有准备好进行信息安全工作。

但是在实际工作中，仅仅实施这些基本的安全措施还远远不够。即使实施了 Fred 故事中所讨论的所有措施，仍有许多其他的方法和技巧可用于防御系统。当然，你可能打上安全补丁，使用文件一致性检查工具，并做充分的日志，但是你最近有没有搜寻不安全的调制解调器？或者，为了防止目前流行的、破坏力很大的嗅探攻击，你有没有考虑在关键网段的交换机上激活端口级安全？为防止当前最普遍的攻击类型之一——基于堆栈的缓冲区溢出，有没有考虑过实施不可执行栈？有没有准备好应付内核级 rootkit？如果想深入了解这些主题或更多的内容，请继续往下读。

正如将在本书中看到的，每天都在发生着威力日益增加的计算机攻击。为建立良好的防御，必须理解对手的攻击技术。在我作为系统渗透测试人员、突发事件响应组成员，以及信息安全设计师的生涯中，我见过许多类型的攻击，从无知的孩子发起的简单扫描到地下犯罪组织发起的有效攻击。本书主要讲述这些在实际攻击中最常见和最危险的部分，同时提出具体的建议，指导读者如何主动避免对手带来的这些麻烦。我们将详细分析计算机攻击者的活动过程，研究攻击过程中的每一个步骤，从而可以深入地实施防御。

本书适用于系统管理员、网络管理员、安全专家，以及想要了解计算机攻击者是如

---

① rootkit 是一种比普通木马后门更为阴险的木马后门，主要通过替换系统文件来达到目的。这样就会更加隐蔽，使检测变得比较困难。一个典型 rootkit 包括：以太网嗅探器程序，用于获得网络上传输的用户名和密码等信息；特洛伊木马程序，为攻击者提供后门；隐藏攻击者目录和进程的程序；还包括一些日志清理工具，攻击者用其删除 wtmp、utmp 和 lastlog 等日志文件中有关攻击者行踪的条目。——译者注

何实施攻击以及如何能阻止他们的人员。本书列出的攻击和防御技术适用于当前使用计算机和网络的所有各种组织，包括从小型到巨型的企业和服务提供商。

攻击者在互相共享如何攻击基础设施的信息方面做得很好。他们相互之间很有效地散发受害者的信息，并显得相当冷酷。我希望通过共享一些本书中实用的建议来改变现状，这些建议是有关如何使得计算机系统免遭坏家伙们破坏的。通过应用本书中论述的防御技术，用户可以极大地提高计算机的安全性，可能明年的元旦我们就都能睡个好觉。

致谢

我惊奇地发现，写一本书的新版本甚至比写第 1 版还要困难！决定保留什么去掉什么是非常困难的，但我们进行了很好的权衡。来自评阅者的各种很好的建议，大大帮助了我对本书的修订。偏重技术的评阅者希望在技术细节上更深入些，而不太偏重技术的评论家希望有更多的指导信息和背景知识。他们提出了有关在背景材料和技术细节之间平衡的极好信息，我非常感谢所有这些信息。

特别是 Radia Perlman，她在本书的撰写过程中起了很大的作用。是她最初产生了写这本书的想法，最后推动我开始写。她还在写作过程中指导我，并提供大量的支持和极好的技术反馈。非常感谢 Radia，网络界的伟大女王！

Prentice Hall 的 Catherine Nolan 在催促我完成本书的整个过程中起到了至关重要的作用。她很严厉但又很友善，通过 E-mail 激励我每日保持一定的进度。

Prentice Hall 的 Mary Franz 是个令人深受鼓舞的朋友，她帮助完成了修订版的启动工作。没有 Mary 就没有本书的存在。虽然现在她转向了其他行业，但我很想念她。

此外，感谢 Prentice Hall 的所有人，有他们的支持才能使本书顺利完成，尤其是 Julie Nahil 和 Teresa Horton，她们指导了整个编辑过程，并提出了许多有用的建议。

还要感谢 Harlan Carvey，Kevin Fu，Mike Ressler 和 Warwick Ford，他们阅读本书并给出非常有用的评论。此外，Denise Mickelsen 在组织本书的评阅工作中发挥了很大的作用。

感谢 Tom Liston，一个伟大的朋友，他更新了第 4，8 和 11 章。没有 Tom 在这些章节的出色工作，我不能确定我们是否能完成本书。非常感谢！

SANS 学院的 Allan Paller 和 Stephen Northcutt 在推动我形成自己的陈述和写作风格方面做了大量的工作。我非常感激他们，在如何以有趣、富含信息的和专业的方式表达原理方面，他们给予了很多建议。

此外，感谢本书所述工具的创作者。尽管一小部分工具开发者有着险恶用心，但绝大多数开发者主要是为了帮助人们在攻击者行动之前找到安全缺陷。尽管你可能不赞同

他们的动机，但是设计这些工具和攻击策略的过程中，他们所表现出的技能和奉献精神是出色的，不应被轻视。

在过去的 10 年中上我课的学生提供了大量的信息。反馈表中一个很小的意见经常会导致教学材料的大改动，这大大提高了一致性，并增加了论述中用到的材料和本书的价值。感谢所有在过去的岁月中给予贡献的人们！

但最重要的是，我要特别感谢我那出色的妻子 Josephine，以及我们的孩子们 Jessica 和 Joshua，在整个过程中，他们给予我帮助和理解。当我日以继夜地写稿时，他们给予我不能置信的支持，给予我超出我应得的自由和理解。这不容易，但令人开心……现在终于完成了。

目　录