披露黑客练功全过程
识破黑客入侵小伎俩
轻松实现从菜鸟到大虾
练就黑客终极必杀技

矛与盾
黑客攻防与脚本编程

36个知识点多媒体视频讲解
让你快速从入门到精通

武新华 陈艳艳 王英英 等编著

机械工业出版社
China Machine Press

矛与盾
黑客攻防与脚本编程

武新华 陈艳艳 王英英 等编著

机械工业出版社
China Machine Press

本书对每一个入侵步骤作详细的分析，以推断入侵者在每一个入侵步骤的目的以及所要完成的任务，并对入侵过程中常见问题作必要的说明与解答。全书共分为13章，主要包括黑客入门知识基础、黑客的攻击方式、Windows 系统编程与网站脚本、后门程序编程基础、高级系统后门编程技术、黑客程序的配置和数据包嗅探、编程攻击与防御实例、SQL 注入攻击与防范技术、数据库入侵与防范技术、Cookies 攻击与防范技术、网络上传漏洞的攻击与防范、恶意脚本入侵与防御、数据备份升级与恢复等内容。

本书内容丰富全面，图文并茂，深入浅出，面向广大网络爱好者，也适用于网络安全从业人员及网络管理者，同时可作为一本速查手册。

图书在版编目（CIP）数据

矛与盾——黑客攻防与脚本编程 / 武新华等编著. —北京：机械工业出版社，2010.1

ISBN 978-7-111-28574-8

Ⅰ. 矛… Ⅱ. 武… 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（2009）第 188878 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）
责任编辑：李东震
北京京师印务有限公司印刷
2010 年 1 月第 1 版第 1 次印刷
184mm×260mm · 22.5 印张
标准书号：ISBN 978-7-111-28574-8
　　ISBN 978-7-89451-258-1（光盘）
定价：48.00 元（附光盘）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；88361066
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）88379604
读者信箱：hzjsj@hzbook.com

前　言

本书本着防患于未然的主旨，着重而详细地介绍了各种黑客入侵网页的手段，概括绝大部分的攻击方式。本书虽然详细解说了每个攻击手法的原理与实际操作，但毕竟如何防范这些入侵才是本书的重点。想要开发安全的 PHP 应用程序，就赶快拿起这本书仔细地阅读吧!只有使读者在了解黑客攻击知识的基础上，能够最大限度地做到“知己知彼”，才有可能在遭受黑客攻击时尽量减少自己的损失。

下面简要介绍本书的特点、学习方法以及提供的服务。

本书内容

本书以配图、图释、标注、指引线框等丰富的图解手段，再辅以浅显易懂的语言，介绍了黑客攻击计算机的一般方法、步骤，以及所使用的工具。本书内容主要包括：黑客入门知识基础、黑客的攻击方式、Windows 系统编程与网站脚本、后门程序编程基础、高级系统后门编程技术、黑客程序的配置和数据包嗅探、编程攻击与防御实例、SQL 注入攻击与防范技术、数据库入侵与防范技术、Cookies 攻击与防范技术、网络上传漏洞的攻击与防范、恶意脚本入侵与防御、数据备份升级与恢复等内容。本书详细地讲述了防护黑客攻击的方法及黑客的攻击与防范技术，使读者在实际应用中碰到黑客攻击时，能够做到“胸有成竹”。

读者运用本书介绍的黑客攻击防守方法去了解黑客，进而防范黑客的攻击，使自己的网络更加安全。

本书几个具体网站例子，已经将具体信息提交给网站进行了修改。

增值服务

本书附赠的光盘提供了多种攻防实战的教学视频，汇集了众多高手的操作精华，通过增加读者对主流操作手法感性认识的方式，使读者实现高效学习。

此外，如发现本书中有需要改进之处，还可通过访问 http://www.newtop01.com 或 QQ: 274648972 与编者进行沟通，编者将衷心感谢提供建议的读者，并真心希望在和广大读者互动的过程中能得到提高。

组织方式

本书紧紧围绕“攻”、“防”两个不同的角度，在讲解黑客攻击手段的同时，介绍了相应的防范方法，图文并茂地再现了网络入侵与防御的全过程。

- 真正的以图来解释每一个知识点及操作实例，基础知识讲解、范例与练习结合，学习周期最短，阅读最轻松。

- 作者采用最为通俗易懂的图文解说，“理论+实战 图文+视频=让读者快速入门”，即使是电脑新手也能通读全书。
- 用任务驱动、情景教学的方式来介绍，在学习案例过程中可掌握知识点，学习目的性、指向性最强。最新黑客技术盘点，让读者实现“先下手为强”。

本书特色

本书以情景教学、案例驱动及任务进阶为鲜明特色，在书中可以看到一个个生动的情景案例。通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。

- 技术最新：当前最新技术，热点技术，常用相关工具软件都在本书有所涉及，有关黑客攻防技术、方法与思路，也做了重要讲解，并通过实例介绍综合技术的运用手段。
- 高效模式：完全站在实用角度介绍黑客攻防技术，突出了实用性和案例分析，全程图解模式可彻底克服攻防操作的学习障碍，学习起来省时、省力，易于上手。
- 内容合理：结合图解，标注和多媒体教学，精选入门读者最迫切需要掌握的知识点，构建一个实用、够用、完整的知识体系。
- 举一反三：详细分析每一个操作案例，力求通过一个知识点的讲解，以实现读者用更少时间尽快掌握黑客编程技术，让读者彻底理解和掌握类似场合的应对思路。

读者对象

本书作为一本面向广大网络爱好者的速查手册，适合如下读者学习使用：

- 电脑爱好者、提高者；
- 具备一定黑客知识基础和工具使用基础的读者；
- 网络管理人员；
- 喜欢研究黑客防御技术的网友；
- 大中专院校相关专业学生。

本书作者

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验，可带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。参与本书编写工作的有：冯世雄负责第 1 章，张晓新负责第 2 章，陈艳艳、李防负责第 3、4、5、6 章，王肖苗负责第 7 章，孙世宁负责第 8 章，杨平负责第 9 章，段玲华负责第 10 章，李伟负责第 11 章，王英英负责第 12 章，郑静负责第 13 章，最后由武新华通审全稿。我们虽满腔热情，但限于自己的水平，书中仍难免有疏漏之处，因此，还望读者本着共同探讨、共同进步的平和心态来阅读本书。作者心存谨敬，随时恭候您提出的宝贵意见。

最后，需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负，切记切记！

编　者

2009 年 11 月 8 日

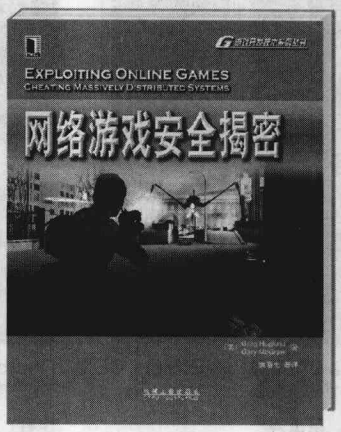
好书推荐

作者：Pedram Amini
书号：978-7-111-25755-4
定价：59.00元

作者：Chris Butler 等
书号：978-7-111-25507-9
定价：29.00元

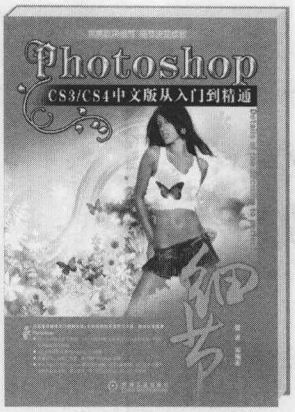
作者：Andy Walker
书号：978-7-111-26519-1
定价：49.00元

作者：David Rice
书号：978-7-111-25229-0
定价：39.00元



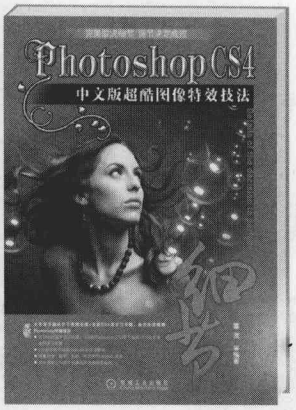
作者：Greg Hoglund 等
书号：978-7-111-25522-2
定价：45.00元

好书推荐



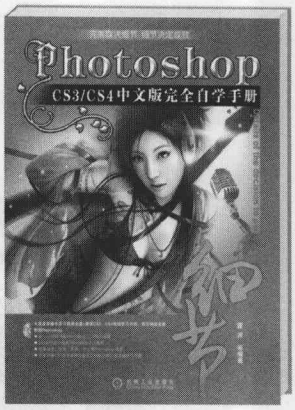
Photoshop CS3/CS4
中文版从入门到精通

作者：雷波
书号：978-7-111-26093-6
定价：89.00元



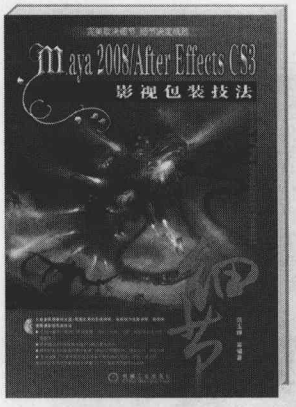
Photoshop CS4
中文版超酷图像特效技法

作者：雷剑
书号：978-7-111-26106-3
定价：79.80元



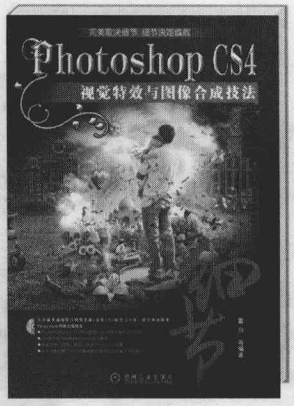
Photoshop CS3/CS4
中文版完全自学手册

作者：雷剑
书号：978-7-111-26092-9
定价：79.00元



Maya 2008/After Effects CS3
影视包装技法

作者：范玉婵
书号：978-7-111-26105-6
定价：88.00元



Photoshop CS4
视觉特效与图像合成技法

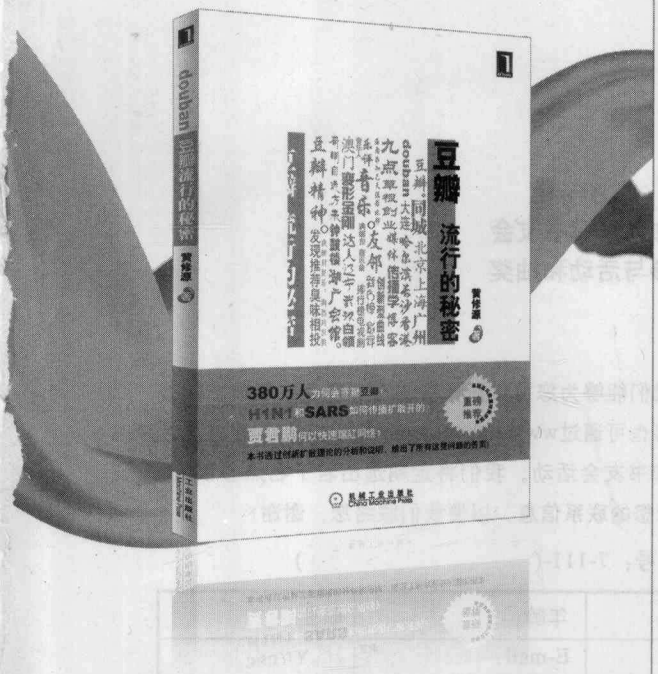
作者：雷剑
书号：978-7-111-26094-3
定价：79.00元

Photoshop
中文版数码照片处理技法精粹

作者：雷波
书号：978-7-111-24411-0
定价：69.80元

3ds maxVRay
室内效果图渲染技法

作者：范玉婵
书号：978-7-111-26135-3
定价：79.00元



《豆瓣，流行的秘密》

——传递爱和理想 一本正在漂流的图书

当你在KFC、麦当劳、星巴克甚至在地铁站里发现一本《豆瓣，流行的秘密》时，不要以为这是一本被丢弃的图书，请把它拣起来，这是一本正在全国漂流的图书，这本漂流的图书，它传播的不仅是一位年轻创业者的理想，也传承着一种阅读的文化。

看了这本书，也许不能让你的产品或网站突然流行起来，但至少，它能让你知道你的产品或网站为什么没能流行起来。下一次，也许你也能创造出一个大流行。

如果你想了解为什么很多网站吸引客户的秘诀，如果你想知道为什么长尾理论只会在互联网的产品中出现，那么我推荐你阅读这本书籍。它很短小，语言简单，例子很实际，它希望用简单的语言告诉你一件我已经发现的或许你还不知道的秘密，你可以在闲暇的周末泡杯咖啡，一边慢慢喝一边阅读它，我想这会是一个很充实的周末。

作者黄修源，正在和他的团队一起在实践很多书中所说的理论，番茄树正是他们正在运营的网站。2个月的时间从ALEXA的100多万名到24000名，没有花一分钱广告费，“其实我们只是在实践我写的书中的一些有意思的理论而已！”修源这样说。

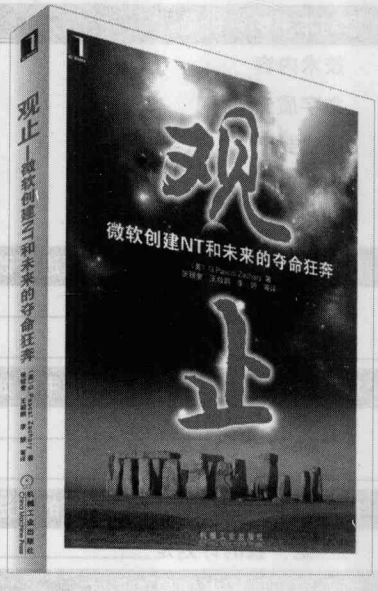
中国IT励志小说

一个月重印三次

让无数企业高管、IT开发者、创业者、高校学生彻夜啃读叹为观止！

作者是一位《华尔街杂志》的著名记者，文笔犀利，用词泼辣，豪放不羁，微软NT团队的几十个人物，在作者的笔下栩栩如生，作者直言不讳写出的他们的缺点，甚至于相貌、家庭、婚恋、事业，大卫·卡特勒是其中的灵魂人物，他是一位计算机的天才，汇编高手，但他的性格很暴躁，脾气倔犟，这也许就是我们传说中的鬼才吧，在昨天刚拿到书时，我并没有立即去看这本书，随手放在了桌边，晚上躺在床上顺手翻了一下，结果一发不可收拾，一直看到早晨5点多才睡觉，要不是顾及今天上班，估计我还会继续看下去。有人说在本书中仅看对卡特勒的描述就很值了，建议大家有空时也读读这本书，看看那些个性鲜明的人物他们的传奇故事，也许我们应该从中学到点什么。

——博客园知名博主　李会军



“在微软的成长过程中，一直伴随着对梦想的不懈追求。本书展现了微软的天才团队追梦过程里的精彩片断——他们付出了艰苦卓绝的努力，经历了犹疑、冲突和痛苦，但他们的成就今天仍然在影响世界。”

——微软全球副总裁 张亚勤

专业成就人生
立体服务大众

www.hzbook.com

填写读者调查表　加入华章书友会
获赠精彩技术书　参与活动和抽奖

尊敬的读者：

感谢您选择华章图书。为了聆听您的意见，以便我们能够为您提供更优秀的图书产品，敬请您抽出宝贵的时间填写本表，并按底部的地址邮寄给我们（您也可通过www.hzbook.com填写本表）。您将加入我们的“华章书友会”，及时获得新书资讯，免费参加书友会活动。我们将定期选出若干名热心读者，免费赠送我们出版的图书。请一定填写书名书号并留全您的联系信息，以便我们联络您，谢谢！

书名：　　书号：7-111-(　　)

姓名：	性别：☐男　☐女	年龄：	职业：
通信地址：		E-mail：	
电话：	手机：	邮编：	

1. 您是如何获知本书的：

☐朋友推荐　☐书店　☐图书目录　☐杂志、报纸、网络等　☐其他

2. 您从哪里购买本书：

☐新华书店　☐计算机专业书店　☐网上书店　☐其他

3. 您对本书的评价是：

技术内容	☐很好	☐一般	☐较差	☐理由_____
文字质量	☐很好	☐一般	☐较差	☐理由_____
版式封面	☐很好	☐一般	☐较差	☐理由_____
印装质量	☐很好	☐一般	☐较差	☐理由_____
图书定价	☐太高	☐合适	☐较低	☐理由_____

4. 您希望我们的图书在哪些方面进行改进？

_____

_____

5. 您最希望我们出版哪方面的图书？如果有英文版请写出书名。

_____

_____

6. 您有没有写作或翻译技术图书的想法？

☐是，我的计划是_____　☐否

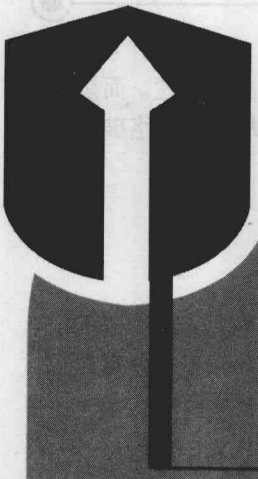
7. 您希望获取图书信息的形式：

☐邮件　☐信函　☐短信　☐其他_____

请寄：北京市西城区百万庄南街1号　机械工业出版社　华章公司　计算机图书策划部收

邮编：100037　电话：（010）88379512　传真：（010）68311602　E-mail: hzjsj@hzbook.com

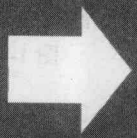
目 录



第 1 章　黑客攻防知识

重点提示

- 黑客基础知识
- 常见的网络协议
- 创建安全测试环境



随着互联网对人们日常生活影响的深入，网络的安全问题也引起了人们高度关注。而黑客则是网络世界中很神秘的一类人，他们有时会义务去维护网络的安全，有时却又以网络破坏者的形象出现。

1.1 黑客基础知识

要成为一名合格的黑客，就必须对操作系统相关的知识有充分地了解，包括进程、端口、服务、文件、文件系统、常用的 DOS 命令和注册表等。只有充分了解了这些知识，才可以提高攻击的成功几率。

1.1.1 进程、端口和服务

一般情况下，计算机中的进程、端口和服务都会给黑客可趁之机，所以在深入了解黑客常用的攻击手段之前，有必要对他们使用的相关基础知识有初步的了解。

1. 进程

进程是一个正在执行的程序。运行一个程序，就启动了一个进程。程序是静态的，进程是动态的。进程可以分为系统进程和用户进程两种。凡是用于完成操作系统的各种功能的进程就是系统进程，它们就是处于运行状态下的操作系统本身；用户进程就是所有由用户启动的进程。进程是操作系统进行资源分配的单位。

在 Windows 系统中按“Ctrl+Alt+Delete”组合键，即可打开【任务管理器】窗口。切换到“进程”选项卡，即可看到本机中开启的进程，如图 1-1 所示。如果想设置进程显示的内容，则选择【查看】→【选择列】菜单项，在【选择列】对话框中勾选相应的复选框，如图 1-2 所示。

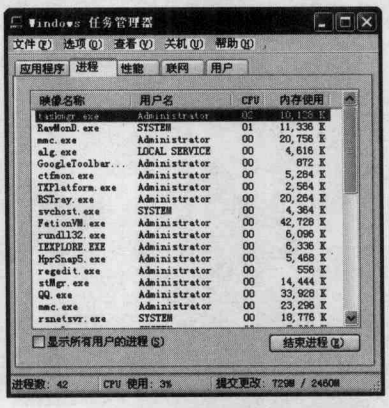


图 1-1 查看本机中开启的进程

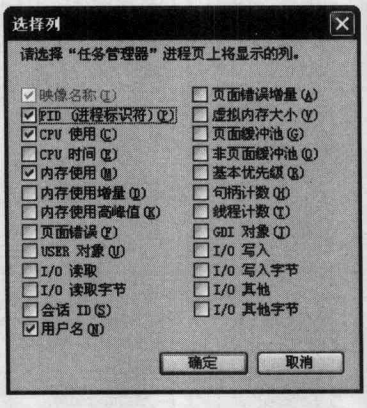


图 1-2 【选择列】对话框

2. 端口

计算机“端口”是计算机与外界通信的出入口。其中硬件领域的端口又称接口，如 USB 端口、串行端口等；而软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，包括一些数据结构和 I/O（基本输入/输出）缓冲区。

在网络技术中，端口有两种含义：一是物理意义上的端口，如集线器、交换机、路由器等