HZ BOOKS
华章科技

信息安全
技术丛书

Metasploit
渗透测试
魔鬼训练营

诸葛建伟 陈力波 孙松柏 王珩 田繁 等著

Penetration Testing Devil Training Camp
Based on Metasploit

- 首本中文原创Metasploit渗透测试著作，国内信息安全领域布道者和资深Metasploit渗透测试专家领衔撰写，极具权威性。
- 以实践为导向，详细讲解了Metasploit渗透测试的技术、流程、方法和技巧，深刻阐释了渗透测试平台背后蕴含的思想。

机械工业出版社
China Machine Press

Metasploit
渗透测试
魔鬼训练营

Penetration Testing Devil Training Camp
Based on Metasploit

诸葛建伟 陈力波 孙松柏 王珩 田繁 李聪 魏克 代恒 著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Metasploit 渗透测试魔鬼训练营 / 诸葛建伟等著 . —北京：机械工业出版社，2013.8

ISBN 978-7-111-43499-3

I. M… II. 诸… III. 计算机网络－安全技术－应用软件 IV. TP393.08

中国版本图书馆 CIP 数据核字（2013）第 176568 号

本书是 Metasploit 渗透测试领域难得的经典佳作，由国内信息安全领域的资深 Metasploit 渗透测试专家领衔撰写。内容系统、广泛、有深度，不仅详细讲解了 Metasploit 渗透测试的技术、流程、方法和技巧，而且深刻揭示了渗透测试平台背后蕴含的思想。

书中虚拟了两家安全公司，所有内容都围绕这两家安全公司在多个角度的多次“对战”展开，颇具趣味性和可读性。很多知识点都配有案例解析，更重要的是每章还有精心设计的“魔鬼训练营实践作业”，充分体现了“实践，实践，再实践”的宗旨。

本书采用了第二人称的独特视角，让读者跟随“你”一起参加魔鬼训练营，并经历一次极具挑战性的渗透测试任务考验。你的渗透测试之旅包括 10 段精彩的旅程。

全书共 10 章。第 1 章对渗透测试和 Metasploit 进行了系统介绍，首先介绍了渗透测试的分类、方法、流程、过程环节等，然后介绍了 Metasploit 的功能、结构和基本的使用方法。第 2 章详细演示了渗透测试实验环境的搭建。第 3 章讲解了情报收集技术。第 4 章讲解了 Web 应用渗透技术。第 5 章讲解了网络服务的渗透攻击技术。第 6 章讲解了客户端的渗透攻击技术。第 7 章讲解了社会工程学的技术框架和若干个社会工程学攻击案例。第 8 章讲解了针对笔记本电脑、智能手机等各种类型移动设备的渗透测试技术。第 9 章讲解了 Metasploit 中功能最为强大的攻击载荷模块 Meterpreter 的原理与应用。第 10 章，魔鬼训练营活动大结局，本章发起了一个“黑客夺旗竞赛”实战项目，目的是进一步提高读者的实战能力。

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：白 宇

藁城市京瑞印刷有限公司印刷

2013 年 9 月第 1 版第 1 次印刷

186mm×240mm · 31 印张

标准书号：ISBN 978-7-111-43499-3

定 价：89.00 元

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 投稿热线：（010）88379604

购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

前　言

当我开始动笔撰写本书前言的时候，仿佛在眼前看到了“万里长征”的胜利曙光。从2011年4月开始策划本书至近日完稿，我与其他几位作者一起经历了长达两年的艰难创作历程；而如果从2005年开始进行网络攻防技术方向的博士研究（第一次接触Metasploit）时算起，我已经伴随Metasploit走过了8年的成长路程。时至今日，当我能以第一作者的身份为国内第一本Metasploit渗透测试技术原创书籍撰写前言时，当我作为参与者基于这款历久弥新的开源框架性平台软件为国内读者介绍精彩纷呈的渗透测试技术时，内心是相当的激动。

渗透技术原本像是武林江湖中的武功秘籍一样隐秘，是行走网际空间的各色黑客“养家糊口”和“安身立命”的本事。早至如凯文·米特尼克[⊖]出于好奇兴趣在实战中修炼出强大渗透技能的第一批电话飞客与网络黑客，近至牟取非法利益而从事地下黑色产业链的“黑帽子黑客”以及为了国家利益而为各国政府或军方效力的“国家队黑客”，通常都对渗透技能守口如瓶，或是只在一个利益共同体中进行交流。然而“白帽子黑客”打破了这种旧有格局，在取得授权的先决前提下对目标进行渗透实践，并在黑客社区中分享渗透技术与开源工具，于是渗透测试便成为安全业界热点关注的技术手段，也造就了渗透测试师这一充满挑战与激情的新职业。

在促进渗透测试技术发展的“白帽子黑客”中，HD Moore无疑是最光芒四射的80后新星。2003年他的Metasploit开源渗透测试框架软件刚发布，便在2004年的Defcon黑客大会上

⊖ 米特尼克自传《线上幽灵——世界头号通缉黑客传奇》由诸葛建伟等翻译，并于2013年中期正式与读者见面，敬请期待观摩这位全球黑客社区偶像级人物的传奇人生经历吧。

引起轰动性效应，并以黑马姿态冲进 SecTools 的五强之列。在开源社区其他黑客的共同帮助下，经过 Metasploit v3 的全新架构与重写，以及 Metasploit v4 的全面扩展之后，Metasploit 成为一款覆盖渗透测试全过程的框架软件，而且已经被安全社区接受，成为一个开放的漏洞研究与渗透代码开发公共平台，在 2013 年荣登 SecTools 排行榜的榜眼。

Metasploit 所具有的强大功能与集成渗透能力，以及社区中分享的大量渗透攻击模块资源，足以让 Metasploit 成为渗透测试“神器”，但是其价值不仅仅在于作为一款渗透工具，事实上，在一些实际的渗透测试场景中，仅依靠 Metasploit 的现有能力，往往得不到很好的测试效果。作为渗透测试师，不应满足于掌握对各种优秀渗透测试软件的使用，而应对优秀渗透测试平台背后所蕴含的技术、方法、流程甚至思想进行深入研究，通过不断实践与广泛交流，不断地提升自己的能力与行业修养，只有这样才能适应这份挑战性职业的需求。

在渗透测试这个高深莫测、与时俱进的技术领域中，本书作者们深知修炼的道行尚浅，虽在本书策划期间已翻译并出版了《Metasploit 渗透测试技术指南》一书，并在科研项目、商业与公益性渗透测试以及黑客 CTF 竞赛中有过一些实战经验，但要达到对渗透测试技术“炉火纯青”的目标还有很长的路要走。但我们仍然鼓起勇气殚精竭虑地撰写出本书，以期望能为同样在修炼渗透测试技能的同道中人提供系统性的参考；也希望能够抛砖引玉，使国内业界“大牛”能够在渗透测试技术领域撰写出更多大作与大家分享。

本书策划时还有姐妹篇《Metasploit 漏洞分析利用特训班》（暂定名），因为作者们自知精力和技术修养尚不够充分，决定无限期挂起，待进一步积累经验并提升能力再予以考虑，欢迎感兴趣的技术高手加盟创作团队。

读者对象

本书的读者群主要包括：

- 网络与系统安全领域的技术爱好者与学生
- 渗透测试、漏洞分析研究与网络安全管理方面的从业人员
- 开设信息安全、网络安全与执法等相关专业的高等院校本科生及研究生
- 期望在信息安全领域就业的技术人员
- 想成为一位自由职业渗透测试师的人
- 以渗透技术行走于网际江湖的人

如何阅读和使用本书

学习与修炼渗透测试技术的唯一方法就是“实践，实践，再实践”，而为了让读者更好地践行这一原则，本书独特地采用了第二人称视角，让读者作为这次虚拟渗透测试之旅的

主角，而让我们跟随“你”一起参加魔鬼训练营，并经历一次极具挑战性的渗透测试任务考验。你的渗透测试之旅包括如下十段精彩的旅程。

❑ 第 1 章　魔鬼训练营——初识 Metasploit

我们将引领你进入渗透测试师的魔鬼训练营，你将了解到底什么是渗透测试，并熟悉渗透测试的过程环节；你也将接触到渗透测试中最为关键的安全漏洞与渗透攻击代码，并知晓从哪里可以搜索和获取这些宝贵资源；你还会见识到渗透测试之神器——Metasploit，回顾这匹“黑马王子”的发展历程，剖析其体系框架与内部结构，并学会如何初步使用这一神器进行简单的渗透攻击。

❑ 第 2 章　赛宁 VS. 定 V——渗透测试实验环境

本章将揭晓你在渗透测试修炼之旅中肩负的任务与挑战，同时帮助你建立起修炼渗透测试技术的实验环境。正所谓“磨刀不误砍柴工”，你的劳动付出将会给你带来更大价值的回报。

❑ 第 3 章　揭开“战争迷雾”——情报搜集技术

作为一名即时战略游戏的资深玩家，你非常清楚情报搜集对于对抗性游戏竞技的重要性，在渗透测试中亦是如此。你将应用在魔鬼训练营中学到的外围信息情报搜集技术、网络扫描与查点技术，以及网络漏洞扫描技术来探查目标环境，从而揭开笼罩在目标周边的“战争迷雾”。

❑ 第 4 章　突破定 V 门户——Web 应用渗透技术

定 V 公司门户网站是你实施渗透攻击的首站，这是考验 Web 应用渗透技术的时候。你能应用魔鬼训练营中传授的 Web 应用漏洞扫描探测技术来找出攻击点，并通过 SQL 注入、跨站脚本攻击、命令注入、文件包含与文件上传攻击技术突破定 V 门户网站吗？让我们拭目以待吧。

❑ 第 5 章　定 V 门大敞，哥要进内网——网络服务渗透攻击

在突破门户网站之后，你在定 V 公司 DMZ 区建立了渗透的前哨站，在侵入内网之前，你接到的任务是攻陷 DMZ 区所有的服务器。面对 Oracle 数据库服务、神秘的工业控制软件服务以及 Ubuntu Samba 网络服务，你在魔鬼训练营中学习实践的栈溢出和堆溢出等内存攻击技术是否过关了呢？

❑ 第 6 章　定 V 网络主宰者——客户端渗透攻击

随着你在定 V 网络中的深入，你要成功渗透攻击目标所需的技术难度也在逐步提升。对于常用的浏览器与 Office 应用软件，你在魔鬼训练营中学习了客户端渗透攻击技术，并实践了针对“Use-After-Free”漏洞的堆喷射利用和 ROP 攻击技术，以及针对栈溢出漏洞的

SEH 链伪造攻击技术。在定 V 内网中，你再次遭遇了神秘的工业控制软件，以及使用非常普遍的 Adobe PDF 阅读器，你能利用浏览器插件与应用软件文件格式中存在的漏洞，成为定 V 网络的主宰者吗？

❑ 第 7 章　甜言蜜语背后的危险——社会工程学

如果你的渗透测试之旅没有社会工程学的陪伴，那么终将留下无限的遗憾。在魔鬼训练营中，你了解到了社会工程学的前世今生，也接触到了社会工程学大师总结的技术框架。那么面对定 V 公司一众人等，你将如何设计，并结合哪些技术手段将他们玩弄于股掌之中呢？

❑ 第 8 章　刀无形、剑无影——移动环境渗透测试

无线 Wi-Fi 网络与 BYOD 自带设备无疑是近年企业移动信息化的热点，殊不知也将为企业的网络安全引入一个薄弱点。你制订了一个“刀剑无形”的移动环境渗透计划，在定 V 公司旁边破解无线 Wi-Fi 网络口令并接入网络，攻击并控制他们的无线 AP，然后对连入无线网的笔记本电脑和 BYOD 设备进行入侵，你能完成这一完美计划吗？

❑ 第 9 章　俘获定 V 之心——强大的 Meterpreter

通过各种技术深度渗透定 V 公司网络之后，该到“俘获定 V 之心”的时候了。强大的攻击载荷 Meterpreter 为你提供了丰富的主机控制功能，也为你收割定 V 网络中的业务数据提供了灵活可扩展的后渗透攻击模块支持，而现在的问题是：你能否用好这个强大工具，来为你的渗透测试任务画上一个圆满的句号？

❑ 第 10 章　群狼出山——黑客夺旗竞赛实战

在你圆满地完成渗透测试任务挑战之时，团队也成功地搞定了一个渗透测试的大项目。团队的另类狂欢活动——参加黑客夺旗竞赛，相信作为一名崭露头角的渗透测试工程师，你也会在这种比拼智力与技能的竞技活动中，找到属于你的那一份热情与欢乐。

❑ 附录 A　如何撰写渗透测试报告

借鉴渗透测试执行标准，为你提供一份如何撰写渗透测试报告的模板，让你能够在完成渗透测试之旅后，提交一份出彩的“游记”！

❑ 附录 B　参考与进一步阅读

本书只是你渗透测试人生旅途的一站，如果要成为一名真正的渗透测试师，需要站在前人的肩膀上，博采众长，并在实践过程中不断提升技能和创新技术。

勘误和支持

本书第 1 章由诸葛建伟撰写，第 2 章由诸葛建伟、田繁共同撰写，第 3 章由王珩撰写，

第 4 章由孙松柏撰写，第 5、6 章由陈力波、代恒撰写，第 7 章由魏克、诸葛建伟共同撰写，第 8 章由田繁、诸葛建伟共同撰写，第 9 章由李聪撰写，第 10 章由诸葛建伟、王珩、孙松柏、陈力波共同撰写，附录 A 由诸葛建伟撰写。全书由诸葛建伟总体策划、组织编写并进行全面细致的审校与润色。本书涉及技术面宽泛，参与撰写的作者人数较多，写作风格与技术能力上存在一些差异，书中难免会出现错误或者表达不准确的地方，恳请读者朋友们批评指正。

此外需要说明的是，本书中的故事场景与人物纯粹虚构，而以第二人称视角描述也可能会让一些读者产生被“说教”的不好感觉，为了本书的独特设计，我们选择承担这种风险，也在这里预先致以歉意。本书所采用的渗透攻击案例都是出于技术讲解与培训的目的，由于图书策划、协同创作与出版的周期较长，在追求最新技术潮流的读者眼中肯定会有时效性不强的问题，也请予以理解。我们在选择案例时并不是以时效性作为首要考虑因素，更关注如何更好地结合实践案例，为读者循序渐进地学习掌握各种渗透测试技术提供最大的帮助。而一旦建立起相关的技能，相信读者朋友们就可以自主地通过网络和其他途径，跟踪研究分析最新的渗透测试技术与实例。

我们将在 http://netsec.ccert.edu.cn/hacking/book/ 链接提供本书的勘误表，如果你遇到任何问题，也可以通过新浪微博直接 @ 清华诸葛建伟，我们将尽量在线上为读者提供最满意的解答。书中涉及的全部源代码文件可以从华章网站（www.hzbook.com）下载，也可以在 http://netsec.ccert.edu.cn/hacking/book/ 链接下载，此链接还会提供搭建本书实验环境所需的虚拟机镜像云盘下载链接。如果你有更多的宝贵意见，也欢迎在新浪微博上 @ 清华诸葛建伟，期待能够得到你们的真挚反馈。

诸葛建伟（@ 清华诸葛建伟）

清华园

致　　谢

诸葛建伟（@ 清华诸葛建伟）

首先要感谢 Metasploit 项目的创始人 HD Moore，以及参与 Metasploit 团队开发与贡献的所有白帽子黑客们，是你们为开源世界带来了一颗瑰宝。

感谢参与本书创作的所有伙伴们——陈力波、孙松柏、王珩、田繁、李聪、魏克和代恒，你们的坚持与共同努力促成了这本书的顺利出版。感谢王若愚、刘跃、方极等同学为本书做出的一些支持工作，以及提出的宝贵意见。感谢蓝莲花（Blue-Lotus）CTF 战队的每一位成员，和你们一起共同拼搏的每一次竞赛都是我的美好记忆。

感谢机械工业出版社华章公司的编辑杨福川老师，他为本书提供一个很好的出版机会，帮助我们将心血之作奉献给更多感兴趣的读者朋友们。感谢编辑白宇，她尽心尽责地审读了本书的全部内容，并对文字与图书结构进行了精心修改，保证了图书的出版质量。

最后感谢我的父母、岳父母、爱人和我即将出世的亲爱宝贝，你们给予我精神、情感与生活上的巨大支持，让我一直追寻心中的梦想，而我亏欠你们太多太多……

陈力波

首先要感谢 Metasploit 的开发、维护团队，得益于你们的高超技能和共享精神，渗透测试人员才能有如此利器。还记得第一次使用时，在浏览器中弹出 MSF 命令行时的兴奋和诧异；所有开源的漏洞测试代码更是直接将我带入渗透测试的底层，不仅知其然，更是知

其所以然！

感谢导师诸葛建伟博士，您对 Metasploit 的理解和认识将我快速地带入渗透测试的核心领域，并对我研究生时期的科研工作起到了莫大的帮助；您始终如一的坚持和推动是这本书得以顺利完成的最大动力；您对增强国内网络安全界软实力的努力激励着我更专注地创作，并在网络安全这个领域继续前行！

感谢同窗好友 luke、聪哥，Blue-Lotus 的 kelwin、fish 等同学，你们对未知的迫切渴望、学习的一贯热情、人生的执著追求已然改变了我许多，在生命的这个阶段能遇见你们是我莫大的幸运！

最后要感谢远在他乡的父母和两地分隔的妻子，你们对我的理解和包容常常使我羞愧难当；你们的鼓励是我一路前行的精神力量……

孙松柏（@lukesun629）

首先要感谢我的导师诸葛建伟博士，没有他坚定信念和心细的协调这本书无论如何也不能够完成。国内研究 Metasploit 的团队非常的多，但是我的导师诸葛建伟博士在 Metasploit 的诞生伊始就给予这个软件极大的关注，他带领的学生和承研的各种安全研究、渗透测试项目中都离不开 Metasploit 的影子，他可以说是国内理解 Metasploit 渗透测试平台最深刻的人之一。我也是在他的影响和指导下逐步对 Metasploit 有了更进一步的认识。

感谢本书创作过程中陪伴我的所有伙伴们，他们是我研究生阶段的同学，以及三年的同寝室友。三年来，波波和聪哥从生活到学习都对我影响颇多，是我研究生经历中无法忘却的记忆。感谢 Blue-Lotus 成员中的每一个兄弟，怀念我们一起奋战 CTF 竞赛的日日夜夜，从你们身上我学到了许多知识和做人的道理。

最后要感谢我的父母，感谢你们在遥远的家乡给予我默默的支持和鼓励，你们永远是我最大的精神支柱，祝愿你们健康、平安。

王珩（@evan-css）

感谢我的导师诸葛建伟博士，你严谨求实、勤奋创新的科研作风让我非常钦佩，生活中你的正直和包容也深深地影响了我。感谢参与本书创作的每一位同学和朋友，与你们的交流让我受益匪浅。

感谢我的妻子，虽然你的工作很忙，但你默默地承担了家里的琐事，让我能够专心投入本书的写作。感谢我的母亲，你永远为我付出，却从没要求我的回报。感谢上幼儿园的儿子，聪明乖巧的你给我注入了很多灵感。

田繁

首先要感谢我的导师诸葛建伟老师，您对于学术的专注以及对学生负责的态度值得我永远学习，您充沛的精力和积极的工作态度更令人钦佩。感谢本书的所有作者，大家的共同努力才有了这本书的面世。感谢 Blue-Lotus 战队的所有成员，虽然每次参赛我只是“打酱油”的，但是你们的出色发挥让我深感自豪。还要感谢实验室其他同学，和你们在一起的实习生涯使我收获颇多，你们每个人的优点都值得我学习的地方。

感谢所有同班同学，有你们同行，三年的研究生的生活显得格外精彩，尤其要感谢包子、月月、村长、铁哥、石吴老板、大拿等同学，更忘不了翻铁门的日子。

感谢我的父母一直以来对我的支持，希望我的小侄子能战胜身体上的痛苦，坚强地书写自己的人生。

李聪

感谢导师诸葛建伟博士，你严谨的学风和认真负责的工作态度一直是我学习的榜样。感谢同寝室的松柏和波波同学，你们的关心、帮助和包容让我终生难忘。感谢我的父母，是你们给了我健康的身体和聪明的头脑。感谢我温柔贤惠的妻子，这十几年来与我同甘共苦，借此机会对你说，我爱你！

魏克

首先在此感谢诸葛建伟博士和本书创作团队的所有伙伴，在诸葛建伟博士的耐心指导和协调组织下各位尽心尽力完成了本书创作。感谢田繁、王珩、孙松柏、陈力波和代恒，每一次讨论你们都让我深受启发，获益匪浅。感谢诸葛建伟老师和参加 CTF 竞赛团队的所有成员，你们的聪明才智和勤奋努力使得我们每年的 CTF 竞赛排名都稳步向前。

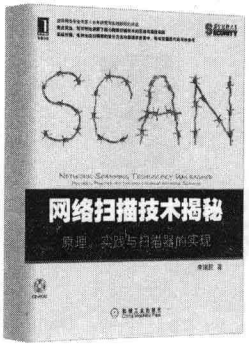
感谢我的家人，每次都是你们给予我最坚定的支持和鼓励。

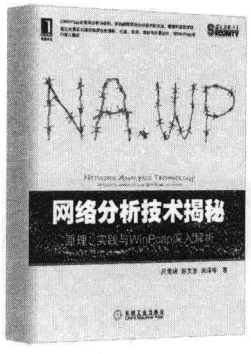
最后我要把最美好和诚挚的祝愿，献给我的父母家人，献给我的兄弟姐妹，献给我们团队中的每一个人。

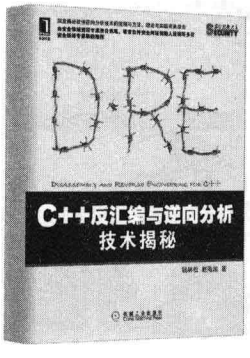
代恒

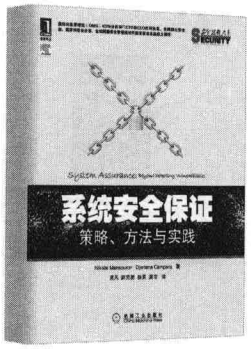
小学时曾经学习过牛顿是“站在巨人肩膀上”，学历慢慢提高，对这种看法感受越来越多。如今，每当利用 Metasploit 做渗透测试、漏洞分析、编写测试脚本，我都会暗自感谢 HD Moore 和无数人走到前面，搭建了一个如此强大的平台，让我们也能够“站在巨人肩膀上”。在此还要感谢诸葛建伟老师的指导和帮助，感谢参加创作的各位朋友，我们是最棒的。

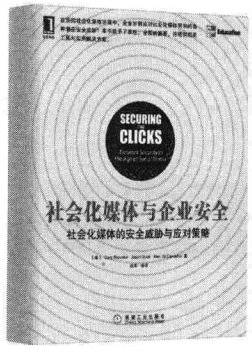
推荐阅读

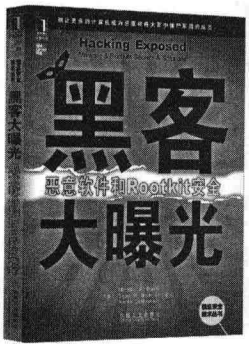

SCAN
网络扫描技术揭秘
原理、实践与扫描器的实现

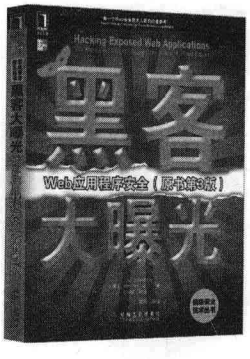

NA.WP
网络分析技术揭秘

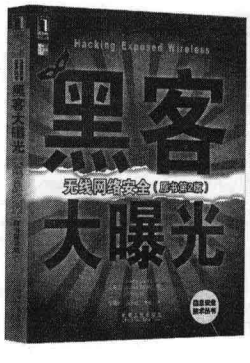

D·RE
C++反汇编与逆向分析
技术揭秘


系统安全保证
策略、方法与实践

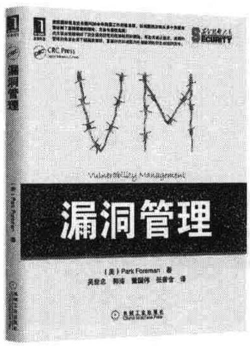

SECURING CLICKS
社会化媒体与企业安全
社会化媒体的安全威胁与应对策略

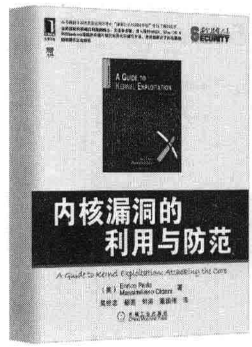

Hacking Exposed
黑客大曝光
恶意软件和Rootkit安全

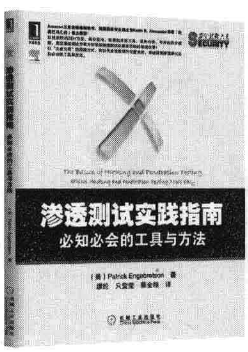

Hacking Exposed Web Applications
黑客大曝光
Web应用程序安全（原书第3版）

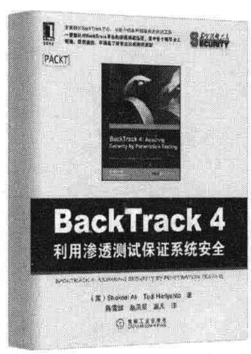

Hacking Exposed Wireless
黑客大曝光
无线网络安全（原书第2版）

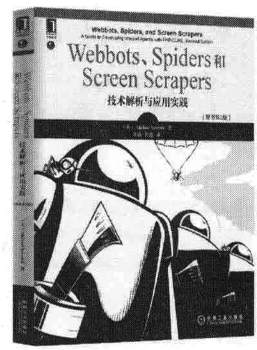
推荐阅读


VM
Vulnerability Management
漏洞管理
(美) Park Foreman 著

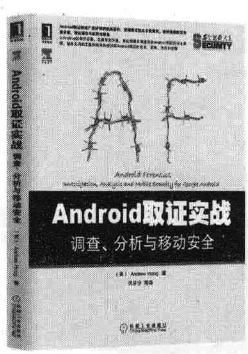

内核漏洞的
利用与防范
A Guide to Kernel Exploitation: Attacking the Core

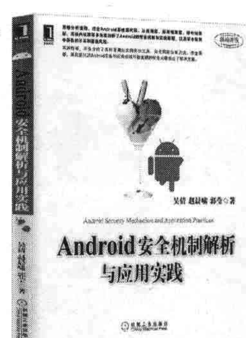

渗透测试实践指南
必知必会的工具与方法
(美) Patrick Engebretson 著


PACKT
BackTrack 4
利用渗透测试保证系统安全


Webbots、Spiders和
Screen Scrapers
技术解析与应用实践


iOSF
iOS取证实战
调查、分析与移动安全


AF
Android Forensics
Android取证实战
调查、分析与移动安全


Android安全机制解析
与应用实践

目　录