华章科技
ELSEVIER 爱思唯尔

信息安全技术丛书

Kali
渗透测试技术实战

[美] James Broad Andrew Bindner 著
IDF实验室 译

Hacking with Kali
Practical Penetration Testing Techniques

- 国际著名信息安全专家亲笔撰写，IDF实验室成员倾情翻译，著译双馨。
- 全面而系统讲解Kali渗透测试的各种技术细节和方法，包含丰富示例，为快速掌握Kali渗透测试技术提供翔实的指导。

机械工业出版社
China Machine Press

信息安全
技术丛书

Kali
渗透测试技术实战

Hacking with Kali
Practical Penetration Testing Techniques

[美] James Broad　Andrew Bindner　著
IDF实验室　译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Kali 渗透测试技术实战 /（美）布鲁德（Broad, J.），（美）宾得（Bindner, A.）著；IDF 实验室译 . —北京：机械工业出版社，2014.9
（信息安全技术丛书）
书名原文：Hacking with Kali: Practical Penetration Testing Techniques

ISBN 978-7-111-47320-6

I. K… II. ①布… ②宾… ③ I… III. Linux 操作系统 IV. TP316.89

中国版本图书馆 CIP 数据核字（2014）第 158926 号

本书版权登记号：图字：01-2014-1843

Kali 渗透测试技术实战

[美] James Broad 等著

出版发行：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：吴 怡 责任校对：董纪丽
印 刷：北京市荣盛彩色印刷有限公司 版 次：2014 年 9 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：11.75
书 号：ISBN 978-7-111-47320-6 定 价：59.00 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

推荐阅读

黑客大曝光：Web应用程序安全（原书第3版）

作者：（美）Joel Scambray 等 译者：姚军 等 ISBN：978-7-111-35662-2 定价：65.00元

黑客大曝光：恶意软件和Rootkit安全

作者：（美）Michael A. Davis 等 译者：姚军 等 ISBN：978-7-111-34034-8 定价：55.00元

黑客大曝光：无线网络安全（原书第2版）

作者：（美）Johnny Cache 等 译者：李瑞民 等 ISBN：978-7-111-37248-6 定价：69.00元

C++反汇编与逆向分析技术揭秘

作者：钱林松 等 ISBN：978-7-111-35633-2 定价：69.00元

网络扫描技术揭秘：原理、实践与扫描器的实现

作者：李瑞民 ISBN：978-7-111-36532-7 定价：79.00元

BackTrack 4：利用渗透测试保证系统安全

作者：Shakeel Ali 等 译者：陈雪斌 等 ISBN：978-7-111-36643-0 定价：59.00元

Windows PE权威指南

作者：威利 ISBN：978-7-111-35418-5 定价：89.00元

内核漏洞的利用与防范

作者：Enrico Perla 等 译者：吴世忠 等 ISBN：978-7-111-37429-9 定价：79.00元

Java加密与解密的艺术

作者：梁栋 ISBN：978-7-111-29762-8 定价：69.00元

云计算安全与隐私

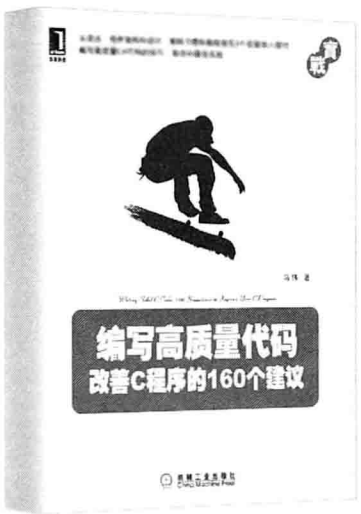
作者：Tim Mather 等 译者：刘戈舟 等 ISBN：978-7-111-34525-1 定价：65.00元

安全之美

作者：Andy Oram 等 译者：徐波 等 ISBN：978-7-111-33477-4 定价：65.00元

推荐阅读

从语法、应用架构、工具、框架、编码风格和编程思想等多角度探讨编写高质量代码的最佳实践，为进阶修炼提供绝佳指导！



推荐阅读

并行程序设计导论（英文版）

作者：Peter S. Pacheco ISBN：978-7-111-35828-2 定价：65.00元

并行程序设计原理

作者：Larry Snyder 等 ISBN：978-7-111-27075-1 定价：45.00元

Visual C++并行编程实战

作者：Colin Campbell 等 ISBN：978-7-111-38806-7 定价：59.00元

GPU高性能编程CUDA实战

作者：Jason Sanders 等 ISBN：978-7-111-32679-3 定价：39.00元

Java并发编程实战

作者：Brian Goetz 等 ISBN：978-7-111-37004-8 定价：69.00元

基于模式的工程：软件开发过程中的模式使用指南

作者：Lee Ackerman 等 ISBN：978-7-111-39811-0 定价：69.00元

深入理解软件构造系统：原理与最佳实践

作者：Peter Smith ISBN：978-7-111-38226-3 定价：89.00元

软件架构师的12项修炼

作者：Dave Hendricksen ISBN：978-7-111-37860-0 定价：59.00元

软件设计的艺术道

作者：Terry Winograd 等 ISBN：978-7-111-34741-5 定价：45.00元

The Translator's Words 译 者 序

“工具善其事，必先利其器”，当 BackTrack 系统基于电子取证和渗透测试的设计而逐渐成为信息安全人员炙手可热的 Linux 发行版本后，其功能更强大，系统操作更简洁，运行更稳定，最后一个版本是 BackTrack 5。已然熟悉和习惯了 BackTrack 系统的渗透测试人员完全没有必要因为 Kali 的出现而忧心忡忡，实际上 Kali Linux 在设计之初原本的命名是 BackTrack 6，只是再基于 Ubuntu 发行版进行修改以达到 Offensive Security 团队的设计目标显得工程尤为庞大，因此更替 Debian 作为基础系统后的 BackTrack 系统重新命名为 Kali Linux，即官方所称的“BackTrack Reborn”（BT 重生）。

相比其他的系统工具书籍，本书的内容不仅包括基础的 Kali Linux 安装、配置，而且涵盖信息安全爱好者和从业人员所关心的渗透测试实验环境的搭建、渗透测试生命周期以及渗透测试评估报告和模板的内容。无论是刚刚接触渗透测试的爱好者，还是从事信息安全行业的老手，相信都可以从中学到或了解到自己以往未知或未意识到的操作技能和渗透测试经验，毕竟本书作者 James Broad 拥有超过 20 年的一线 IT 从业经验。

值得注意的是，本书作者作为一名信息安全专家曾经为包括美国国防、执法机构、情报机构、金融和医疗保险行业提供过信息安全服务。而自 2013 年斯诺登事件后，从国家层面到企业层面都越来越重视信息安全及其在信息化发展中的重要性，以至于未来十年被很多人称为“信息安全的黄金十年”，本书的面世和引入虽不至于达到“师夷长技以制夷”，但至少可以在越加严峻的信息安全形势下，为诸多信息安全爱好者、从业者的成长与蜕变起到提点、引路的作用。

本书的翻译由 @IDF 实验室（www.idf.cn）成员裴伟伟、童进、封畅、李秀烈、张世会、成明遥共同完成，徐文博亦参与了部分审校工作。IDF 实验室一直致力于安全知识普及、安全人才培养、国际技术交流和黑客文化演绎，能够参与本书的翻译得益于 IDF 实验室联合创

始人万涛（@黑客老鹰）和机械工业出版社吴怡编辑的努力，同时感谢在翻译过程中吴怡编辑的耐心交流和经验提点。

由于本书内容涉及渗透测试的各个方面，一些术语尚无确切译法，我们保留了英文。部分章节翻译难度较大，加之参与翻译工作的各位 IDF 实验室成员水平有限，译文中如存在不当之处也在所难免。我们真诚地希望读者不吝赐教，如有任何的意见和建议请发邮件给我们：idf@idf.cn，我们将不胜感激。

IDF 实验室　裴伟伟（做个好人）

2014 年 5 月 23 日

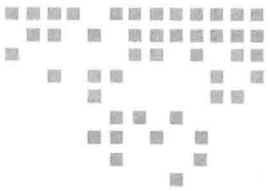
Acknowledgements 致　谢

我想把这本书献给我的家人：我的姐姐们 Lisa、Teresa、Mary，是她们一直在那里默默地支持我。感谢我的妻子 Dee 还有我的孩子 Micheal 和 Tremara，是你们给了我继续学习和成长的动力。还献给我的朋友们：Amber 和 Adam、Vince 和 Annette、Darla、Travis 和 Kim、Steve 和 Sharon，太多了无法在这里一一列出，不论是新朋友还是老朋友，是你们让我的生活变得更加精彩。

谢谢大家！

生命不息，奋斗不止——Jeff Olson

目　录 *Contents*



第 1 章 Chapter 1

引　言

章节信息

- 本书的读者群
- 本书图片、图表和屏幕截图
- 常用术语
- Kali Linux 发展史

本书要点

本书通过指导读者使用现今流行的最先进的 Live 版操作系统 Kali Linux，引领读者贯穿渗透测试整个生命周期。在简短介绍后，本章将详述如何寻找、下载、安装并定制 Kali Linux。接下来简要介绍 Linux 的基本配置和设置，以保证读者能理解基本命令和设置。本书剩余部分用于介绍渗透测试的生命周期——侦察、扫描、渗透、维持访问和报告等阶段。Kali Linux 的发行版带有成百上千种不同的工具，而本书在介绍渗透测试生命周期时将仅涉及对应生命周期阶段最常用的工具。报告阶段会详细介绍如何生成报告，包括将渗透测试结果呈现给管理层和领导的报告，还包括开始渗透测试前的授权合同（ROE）模板。

1.1　本书的读者群

专业技术人员

计算机专业领域的技术人员，通过了解渗透测试人员的工作过程，能够获取更多经验。

专业技术人员将会进一步理解渗透测试人员使用到的基本概念和技术，这些知识能让他们的信息系统更安全。这些领域包括但不限于服务器管理员、网络管理员、数据库管理员和桌面支持人员。

某些希望转型为专业渗透测试人员的专业技术人员通过阅读本书，可以获得大量渗透测试方面的知识。由于专业技术人员对各领域的知识有深入把握，在成为渗透测试人员时会具有独特的优势。在服务器管理方面拥有大量知识的人员会比渗透测试人员更适合测试服务器的安全配置。在其他专业领域的人员也是如此。

本书将会向专业技术人员介绍渗透测试领域以及渗透测试人员的常用工具。通过学习下面章节的例子和指令，专业人员将可以转型为渗透测试人员。

安全工程师

安全工程师的目标是努力使开发和维护的系统更加安全，如果理解了渗透测试的思维观念和生命周期，将会获得大量的知识，这将有利于总结提炼所开发和支持系统的安全特征。

信息安全和信息工程专业的学生

理解渗透测试领域，有助于学生深入了解当今报酬最高、最令人沮丧、最专业的信息技术领域之一：渗透测试。尽早接触渗透测试，可使学生确定把渗透测试方向作为职业是一个好的选择。

本书不适合的人群

本书不会为攻击美国国家安全局（NSA）或者本地银行分行提供技能和经验，也建议你不要去尝试。本书也不是为拥有多年渗透测试经验和深入掌握 BackTrack/Kali Linux 中工具原理的专业人员准备的。任何人都不能违法，本书引导更多的人接触渗透测试，是为了追求更安全的信息系统。

1.2 本书中的图片、表格和屏幕截图

本书中的图表是为了提供更坚实的理解，这是对文字描述的基本概念和技术的图解说明。

贯穿全书的屏幕截图用于说明将在 Kali Linux 环境中执行的命令和动作，也用于进一步阐明所述主题。根据 Kali Linux 的配置和版本的不同，这些屏幕截图与本地显示可能会有少许不同。这不影响渗透测试的基础学习，即使有影响，也应该是轻微的。

1.3 关于渗透测试

渗透测试是令人激动和内容丰富的领域，本章只是一个引言。渗透测试，或者更简洁地

说渗透，是一套技术过程和方法论，是技术专家模拟黑客的动作和技术去尝试利用网络或信息系统。本书将会带领读者沿着渗透测试人员的步骤一步步地跟进：形成对目标的理解，分析目标，并试着渗透。本书用一章总结了报告撰写和其他文档，这些文档用于向组织领导层表述渗透测试团队的活动以及发现的系统缺陷。最后一章包括一个规范化的授权协议（ROE）模板，应该在渗透测试开展前进行标准化并经过审批。仅对授权的系统实施渗透测试以及严格按照审批的授权文件（ROE）需求进行渗透，这点很重要。

1.4 渗透测试生命周期

在实践中有众多不同的渗透测试生命周期模型。目前为止，最受认可的是 EC-Council Certified Ethical Hacker（EC C|EH，伦理黑客认证）定义和使用的方法和生命周期。整个过程包含五个阶段：侦察、扫描、获取访问、维持访问以及清除痕迹[1]。本书将遵循 Patrick Engebretson 发行的《The Basics of Hacking and Penetration Testing》一书中渗透测试生命周期的修订版。这个过程采用了 C|EH 使用的基本阶段但是不包括最后阶段：清除痕迹。从本书中删除这个阶段是特意为之，因为最终阶段的许多技术在更深入的书中有出色的解释。

1.5 常见的术语

当提及渗透测试时，有很多常用术语需要讨论。不同的专业、技术领域，甚至是同一团队成员对该领域术语的理解都会稍有不同。因此，本书将使用下面的术语和相关定义：

渗透测试

渗透测试是测试人员在具体和授权的指导原则下尝试规避信息系统的防护措施所使用的方法、过程和规程，包括突破系统集成的安全特性。这种测试与技术评估、管理、操作设置和系统控制有关。通常情况下，仅评估信息系统建立时的安全性。目标网络系统管理员和技术人员或许不知道渗透测试正在进行。

红客团队

红客团队在方法和技术上模拟潜在对手。它们通常比渗透测试团队要大，范围也更广。渗透测试本身就是红客团队活动的一个子集，但是这些活动测试了一个组织安全部分的其他功能。红客团队通常采用安全技术、社会工程技术和物理方式攻击一个组织，通常使用与黑帽黑客同样的技术测试一个组织或者信息系统针对黑客攻击行为的防护措施。红客团队除了渗透测试外，他们还会执行社会工程攻击，包括网络钓鱼和鱼叉式网络钓鱼，还有可能发动物理攻击，包括翻垃圾桶或者物理开锁等方式获得所需要的信息。在大多数情况下，