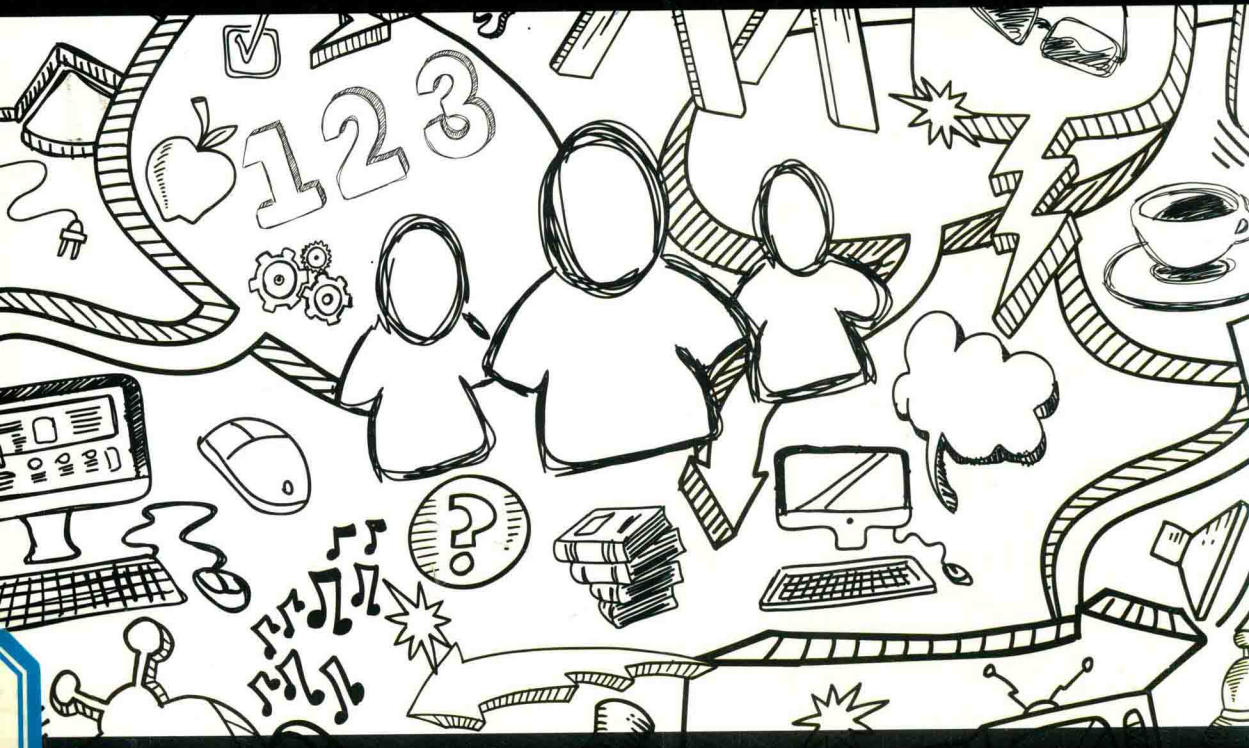
Broadview
www.broadview.com.cn

安全技术大系

官方团队写作 阵容强大 内容上乘

Kali Linux 大揭秘

深入掌握渗透测试平台



Kali Linux Revealed

Mastering the Penetration Testing Distribution

[美] Raphael Hertzog Jim O'Gorman Mati Aharoni 著
诸葛建伟 王珩 刘跃 梁智溢 译

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

Kali Linux 大揭秘

深入掌握渗透测试平台

Kali Linux Revealed

Mastering the Penetration Testing Distribution

[美] Raphael Hertzog Jim O'Gorman Mati Aharoni 著
诸葛建伟 王珩 刘跃 梁智溢 译

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

内 容 简 介

Kali Linux 是设计用于数字取证和渗透测试的操作系统。本书是官方出版的唯一著作，适合新手入门。

在本书中，重点介绍了 Kali Linux 平台本身，并详细论述了如何来理解和最大限度地使用 Kali。本书首先引导读者了解 Kali Linux 的功能和基础知识，并解释了基本的 Linux 命令和概念。然后介绍了最常见的 Kali Linux 安装方案，并探讨了如何配置、分析和保护 Kali Linux。随后介绍了强大的 Debian 软件包管理器，在这部分中，介绍了如何安装和配置软件包，如何更新和升级 Kali 安装，以及如何创建自定义软件包，并介绍了如何在大型企业网络中部署自定义安装。最后，进入到高级主题，介绍了内核编译、自定义 ISO 创建、工业强度加密，以及如何安装加密杀死开关来保护敏感信息等内容。

无论你是老将还是新手，本书都是你学习 Kali Linux 的最佳选择。

版权贸易合同登记号　图字：01-2018-0971

图书在版编目（CIP）数据

Kali Linux 大揭秘：深入掌握渗透测试平台 /（美）拉斐尔·赫佐格（Raphael Hertzog），（美）吉姆·奥戈曼（Jim O'Gorman），（美）马蒂·艾哈尼（Mati Aharoni）著；诸葛建伟等译. —北京：电子工业出版社，2018.8
（安全技术大系）
书名原文：Kali Linux Revealed: Mastering the Penetration Testing Distribution
ISBN 978-7-121-34313-1

Ⅰ. ①K… Ⅱ. ①拉… ②吉… ③马… ④诸… Ⅲ. ①Linux 操作系统－安全技术 Ⅳ. ①TP316.85

中国版本图书馆 CIP 数据核字(2018)第 115548 号

责任编辑：刘　皎
印　　刷：三河市良远印务有限公司
装　　订：三河市良远印务有限公司
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：18.5　字数：390 千字
版　　次：2018 年 8 月第 1 版
印　　次：2018 年 8 月第 1 次印刷
定　　价：89.00 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）88254888，88258888。

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。

本书咨询联系方式：010-51260888-819，faq@phei.com.cn。

推荐序一

应诸葛建伟先生之邀，为其翻译的《Kali Linux 大揭秘：深入掌握渗透测试平台》一书作序。OWASP 作为国际权威应用安全的研究机构，在 Web 安全方面的研究，是国内外信息安全机构在应用安全研究方面的主要参考依据。本人作为 OWASP 中国北京的主要负责人，很荣幸地拜读了本书的整个目录和全部章节，最大的感受就是本书贴合实际需求、生动详实，案例充分。

本书从渗透测试的实战出发，增加了诸多新增工具的介绍，完整地填补了目前市面上相关书籍内容上的空白：现在市面上的许多安全书籍，都是只介绍结果，考虑过程的并不多。本书从实践出发，本着务实的精神，对环境搭建一直到渗透测试的全阶段，以及主流工具的使用，都做了详尽的介绍，示例丰富，是每位信息安全的从业人员、在校学生不可多得的一本使用大全。你完全可以依照本书的案例来学习，并有效地贴近企业需求，做到有的放矢。

从本书的编写风格就可以看出作者技术功底扎实、写作思路清晰、讲解由浅入深、举例生动详实，非常值得一读！

陈　亮
OWASP 中国

推荐序二

你可能还没意识到你所拥有的美好事物。

在 1998 年，我还是一位初出茅庐的黑客，创建了最早的一个职业白帽黑客团队。当时团队成员们还都是一群孩子，梦想着自己未来的工作，能够拿着不错的薪水，去入侵这个星球上最安全的计算机系统、网络甚至建筑。

这听起来很“性感”，但现实却是，我们需要把生活中的绝大部分时间花在和电脑键盘相处上，用行业中的一些数字工具来武装自己。我们挥舞着四处采集到的程序，绘制网络地图并定位目标，然后扫描、渗透目标并进一步拓展。在某些情况下，我们中的一员（经常是 Jim Chapple）会编写一些定制化工具来做一些很酷的事情，比如说扫描一个 A 类的网络（在当时可没有其他现成工具能够搞定这件事），但绝大多数时候我们只是使用和修改黑客社区中已开发好的工具。在那些还没有 Google 的日子里，我们频繁地刷 BugTraq、AstaLaVista、Packet Storm、w00w00、SecurityFocus、X-Force 以及其他资源，来研究并建立起我们自己的军火库。

因为我们在每次行动中的时间有限，我们必须追求速度，这意味着我们不会花很多时间来拨弄各种工具。所以我们必须要学习最核心工具的里里外外，然后让其他辅助工具只是处于待命状态。于是我们必须良好地组织我们的工具，文档化并进行测试，以便在实战中不要给我们带来意外。如果不能成功渗透，那么我们将在客户面前丢脸，而他们也会轻视我们所提出的建议。

正因为如此，我花了非常多的时间来对工具进行分类编目，当一个工具被发布或更新时，我会完整地走完一个流程，查看它是否可以在攻击平台上正常运行，以及是否值得安装运行。我还必须更新依赖这一工具的所有脚本，编写相关文档并进行测试，包括相对于前一版本有了何种变化。然后我会组织所有的工具，根据它们在执行一次安全评估时的目的和作用，将它们放置到不同的目录里。我会为特定工具编写包装脚本，将一些工具链接在一起，并将所有工具关联在一起，刻录成一张 CD 盘，当客户不让我们带入攻击机器或者移动介质到他们实验室的时候，我们将带着这个 CD 盘进入隔离的敏感区域。这一过程是非常让人头疼的，但也是必须的。我们知道，如果合适地应用我们的技能和专业经验，保持良好的组织

性，并高效工作，我们有入侵任何网络的能力。尽管在渗透测试中从不失手是我们的驱动力，但是我们提供给客户的是一种专业入侵网络的渗透服务，而客户会增加各种限制，并通过金钱回报引导渗透的主要目标到他们最为关键但可能疏于防范的信息安全流程中。

我们花了好几年的时间来磨练我们的技能和专业度，但如果没有良好的组织和高效率，我们不会像现在这样成功。如果我们没有尽心去调校所需的工具，我们可能已经失败了。这是我花那么多时间研究、编撰文档、测试与分类工具的根本原因。在 21 世纪到来之后，这很快发展成为一份压力巨大的全职工作。由于 Internet 的发展，攻击面的全球性爆发，以及攻击工具的种类和数量的指数级增长，维护这些工具所需的工作量也随之剧增。

从 2004 年开始，Internet 已经不仅仅是商务活动的基石，也成为了一个社交平台。计算机已经变成人人都能负担得起的东西，而且更加友好，无所不在。存储技术已经从 M 字节扩展到 G 字节，以太网的速率从每秒几百 KB 快速发展到每秒数十 MB，Internet 连接变得越来越快，也更加便宜。电子商务已经非常流行，而社交媒体如 Facebook（2004 年）、Twitter（2006 年）已经上线，Google 变得更加成熟，可以让每个人（包括罪犯）在互联网上找到几乎任何东西。

研究对于我们这样的团队变得至关重要，因为我们必须能够跟上新型攻击和工具集发展的脚步。我们对更多计算机犯罪事件进行响应，在必要的取证工作中我们需要仔细追查潜在的证据。而自生型 CD 的概念意味着我们可以在被攻陷的机器上执行实时取证，而不会对证据造成任何破坏。现在我们这个小团队必须要管理攻击工具、取证工具和在敏感区域使用工具发行版，我们必须跟上所有最新攻击技术和利用方法学的发展。我们必须这么做，因为你知道我们是受雇来进行渗透测试的，所以都是高标准要求。而事情变得有些超出控制，在最近一段时间，我们在实战中花费的时间少了，而在研究、打磨工具和计划方面投入更多的时间。

在这场对抗中我们并不孤独，在 2004 年，Mati“Muts”Aharoni，一位黑客和安全专家，发布了“WHoppiX”（White Hat Knoppix），一个被宣传为“终极版渗透测试 Live CD”的自生 Linux CD，其中包含了“来自 SecurityFocus、Packet Storm 和 kotik 的所有渗透利用脚本，Metasploit 框架 2.2 版，以及更多其他软件”。记得在下载 WHoppiX 时，我在想这是很棒的东西，我也下载了其他一些自生 CD，想象假使我之前陷入困境的一些局面，这些自生 CD 可以在实战中帮上我们。但是我当时并没有计划在真正实战工作中依赖 WHoppiX 和其他 CD。我并不相信它们中的任何一个能够满足我的大部分需求，没有一个对我的工作流来说感觉是对的，而且它们也不是完全的、可安装的发行版。在我下载的时候，它们已经过时了。一个过时的工具集对于我们所在的行业就是“死神降临”。我只是简单地将这些 CD 镜像添加到军火库里，尽管它们的大小相对较大，然后还是继续着那令人头疼的过程来维护我们实际使用的工具集。

尽管在当时我对它持保留意见，但 WHoppiX 及其后续者在我们的行业和社区中都造成了巨大的影响，或许也超出了 Muts 本人的预期。

在 2005 年，WHoppiX 进化成了 WHAX，一个扩展并更新后的工具集，基于“最模块化的 SLAX（Slackware）自生 CD”。Muts 和来自黑客社区的一个迅速发展的志愿者团队看起来已经意识到了，无论他们如何具有远见，仍然无法预期到我们这个行业的所有发展和波动，而 CD 的用户们在实战中也有多种差异化需求。而且 Muts 和他的团队显然也已经在实战中使用 WHAX，他们似乎也努力让它变得更加好用，这件事对于我是非常受鼓舞的。

到了 2006 年，Muts、Max Moser 和他们的团队将 Auditor Security Linux 和 WHAX 合并到单一发行版中，称为 BackTrack。基于 SLAX，BackTrack 继续向前发展，增加了更多的工具，更多的框架，扩展语言支持，多种无线协议支持，整合一个对专业用户和新手用户都适用的菜单结构，以及重度修改了内核。BackTrack 成为领先的安全发行版，但是像我这样的很多人仍然把它作为“实际使用工具集”的一个备份。

在 2009 年初，Muts 和他的团队已经将 BackTrack 扩展至 BackTrack 4，这是一个明显的变化。今天，Muts 将此作为了全职工作，BackTrack 已经不再是一个自生 CD，而是一个基于 Ubuntu 充分发展的发行版，并充分利用了 Ubuntu 的软件仓库。这种变化以一个显著的革新作为标志：也就是 BackTrack 4 拥有系统更新机制。用 Muts 自己的话说：“当和我们的 BackTrack 的软件仓库同步时，你可以在安全工具发布后很快就获得更新。”这真的是一个转折点，BackTrack 团队已经真正理解了渗透测试者、取证分析师和该行业其他从业者所面对的挑战，他们的工作可以帮助我们节省很多时间，并为我们提供了一个坚实的基础，使得我们直接进入实战状态，将更多的时间花在真正重要且有趣的事情上。结果是，社区反响热烈，众多用户群集到论坛和 wiki 上，并热情参与到开发团队中。BackTrack 确实是一个社区化的贡献，而 Muts 仍在其中引领着。

BackTrack 4 最终成为工业界最强的渗透测试平台，而我，还有很多像我这样的人终于可以松一口气了。我们对 Muts 和他团队所承受的“痛苦”有着切身体会，因为我们也曾经亲身经历过。而结果是，我们中的很多人开始使用 BackTrack 作为工作的首要基础平台。是的，我们仍然会拨弄一些工具，编写我们自己的代码，以及开发我们自己的漏洞利用工具和技术，我们开展研究和实验，但是我们不再在收集、更新和组织工具上花费很多时间了。

BackTrack 4 R1 和 R2 是 2010 年进一步修订的版本，之后又在 2011 年自底向上重新构建了 Back Track 5——仍然基于 Ubuntu，但跟上每个发布的脚步。Back Track 在当时已经是一个极为成功的项目，需要英雄的志愿者团队和社区的努力，同时也需要一些资助。Muts 在 2006 年开始创立 Offensive Security 公司，该公司不仅仅提供全球领先的培训和渗透测试服务，还为保持 Back Track 的开发进程提供坚实后盾，保证 Back Track 的开源和免费使用。

Back Track 在 2012 年继续发展和改进（先后发布 R1、R2 和 R3 版本），其维护着 Ubuntu 的核心并增加了数以百计的新工具，包括物理和硬件利用工具、VMware 支持、许多无线和硬件驱动，以及大量的稳定性改进和缺陷修复。然而，在 R3 版本发布之后，Back Track 的开发变得相对缓慢，甚至有点神秘地静默。

当时在坊间有一些猜测，一些人以为 Back Track 变了，把它的灵魂出售给了一家无情邪恶的企业主而获得丰厚回报。Offensive Security 也在那几年里发展成为最受尊敬的网络安全培训机构之一以及行业中的一家思想引领者，某些人揣测这家公司的成功是建立在吞并大量 Back Track 关键开发者的基础上。然而，事实并非如此。

2013 年，Kali Linux 1.0 发布，从发布公告中可以看到，经过一年沉默的开发过程，Offensive Security 自豪地宣布，发布 Kali Linux，并且它是公开可用的，这是最先进、鲁棒和稳定的渗透测试发行版，Kali 是比 Back Track 更加成熟、安全和适合企业应用的版本。

Kali Linux 于 Back Track 并不是“新瓶装旧酒”，其移植了超过 600 个完全重打包后的工具，这显然是一个令人称奇的工具集，但还不仅仅只是这些。Kali 是从 Debian 的内核核心基础上，从头开始构建的，这对于一些还不了解情况的人而言，看起来并不是个大工程，但是懂行的人知道这需要做大量底层的工作。做了这些重打包的工作后，Kali 用户可以下载每一个工具的源码包，可以按需求修改并重构工具，而只需要敲几行代码和命令。和目前其他主流操作系统发行版不同的是，Kali Linux 同 Debian 软件仓库每天进行四次同步，这意味着 Kali 用户可以及时获取软件包更新和安全补丁。Kali 开发者全身心投入到许多工具上游版本的打磨、打包和维护上，才使得用户可以始终保持在业界前沿。感谢 Debian 的根基，Kali 用户可以从软件仓库直接引导一个安装或者 ISO 镜像，这也打开了完全定制化 Kali 安装版之门，你可以通过预设文件进行自动化和定制的大规模的企业化部署。为了实现定制目标，Kali 用户可以修改桌面环境，变更菜单项，改变图标文件，甚至改变窗口环境。由于做了大量的 ARM 开发工作，使得 Kali Linux 可以在大范围硬件平台上安装，包括无线 AP、单片机系统（例如树莓派、ODROID、BeagleBone、CubieBoard 等），以及基于 ARM 的 Chromebook 计算机等。最后要提及的重要一点是，Kali Linux 支持无缝的小更新和重大升级，这意味着 Kali 的狂热者永远不需要在机器上重新安装定制化的 Kali Linux。

社区也注意到了 Kali 的发布，在最初的五天中，9 万名用户下载了 Kali 1.0 版本，而这仅仅是开端。在 2015 年，Kali 2.0 发布，紧随其后的是 2016 年的 rolling 版本发布。总结来说，如果 Kali 1.0 聚焦于构建一个稳固的基础设施，那么 Kali 2.0 则专注于提升用户体验并维护更新的软件包和工具仓库。而目前 Kali Linux 的版本是一种滚动更新的发行版，这标志着特定版本的终结。

现在用户可以持续地保持最新版本，并接收到开发者创建的更新和补丁。得益于上游软

件的版本标记系统，核心工具的更新更加频繁，也针对视障人士做了便捷性方面的改进，Linux 内核也被进行了更新和修补以扩展对无线 802.11 注入的支持范围。SDR（Software Defined Radio，软件定义无线电）和 NFC（Near-Field Communication，近场通信）工具增加了对安全测试新领域的支持，完全 Linux 加密磁盘安装和紧急状况自毁选项也变得可用。感谢 LVM、LUKS，增加了 USB 持久化选项，并允许基于 USB 的 Kali 安装保持重启后的系统改变，而无论 USB 盘是否加密。最后，最新版本的 Kali 为 NetHunter 打开了大门，NetHunter 成为一个运行在移动设备上的全球领先的开源操作系统，以 Kali Linux 和 Android 作为其基础。

Kali Linux 已经演化成为信息安全从业者首选的平台，而且真正成为了一个工业级别、全球领先、成熟、安全、适合企业使用的操作系统发行版。通过十多年的开发历程，Muts 和他的团队，以及来自黑客社区无法计数的全身心投入的志愿者，承担了组织我们工作环境的压力，把我们从大量工作、负担中释放出来，并提供了一个安全和可靠的基础平台，让我们聚焦在驱动工业界向前发展，让数字世界更安全的终极目标上。

围绕着 Kali Linux，一个令人惊奇的社区已经创建起来，每个月新版本的 Kali 被三四十万的用户下载，我们汇聚在 Kali 论坛和 Kali 的 IRC 频道中，我们汇集在 Kali Dojos 会议上，从开发者那里学习如何最好地利用 Kali。

Kali Linux 改变了信息安全的世界，让它变得更好，而 Muts 和他的团队帮我们节省了许多时间，让我们能够将更多时间和精力放在一起驱动工业界的向前发展上。

尽管 Kali 拥有惊人的接受度、支持度和流行度，它却从来没有发布一份官方的手册。好吧，现在这种状况已经改变了，我非常激动地和 Kali 开发团队，特别是 Mati Aharoni、Raphaël Hertzog、Devon Kearns 和 Jim O'Gorman，一起来提供这本指南，第一本关于 Kali Linux 的官方出版物，或许也是官方手册系列中的第一本。在这本书中，我们聚焦于 Kali Linux 平台本身，帮助你从最基础了解和使用 Kali。我们还不会深入到 Kali Linux 中的工具军火库中，但无论你是一位老兵还是一位新手，如果你准备深入探索 Kali Linux，本书是你最好的起点。无论你在这个游戏中已经玩了多长时间，阅读这本书，你将可以和正在发展的 Kali Linux 社区联结在一起，我们行业中最古老、最大、最有生气以及最活泼的社区之一。

我代表 Muts 和 Kali Linux 开发者团队的其他同仁，恭喜你踏上深入掌握 Kali Linux 的征程。

Johnny Long
2017 年 2 月

作 者 序

你所在的渗透测试团队定购的 16 台高性能笔记本电脑刚刚已经到货，而你被赋予设置好工作环境的任务，那就为明天一场驻场渗透测试做好准备吧。你安装好 Kali 系统并启动了其中一台电脑，以确认它是否可用。尽管 Kali 拥有最前沿的内核，但是网卡和鼠标仍然不工作，笔记本电脑中最新款的 NVIDIA 显卡和 GPU 也正在困惑地“注视”着你，因为缺少恰当安装的驱动程序。你很无奈。

在 Kali 的自生模式下，你快速地在一个终端中输入 lspci 命令，然后眯着眼睛盯着屏幕，当你滚动查看硬件列表：“PCI bridge、USB controller、SATA controller、Ethernet 和 Network controllers”，并通过 Google 快速搜索这些硬件相应的型号，以及 Kali 内核版本号的交叉索引时，发现这些最新款硬件的驱动还没有被集成到主线的内核代码中。

这对于你来说并不是难题。一个解决计划正在你的脑袋中成型，而这要归功于你几周前仔细研读过的《Kali Linux 大揭秘》这本书。你使用 Kali Live-Build 系统来创建一个定制 Kali ISO 镜像，将所需的驱动程序灌入安装盘里。另外，除了包含 NVIDIA 显卡驱动之外，还安装了用来发挥 GPU 性能并用于 hashcat 程序的 CUDA 库文件，它使得 GPU 可以在飞速破解哈希口令时发挥最大的功效。你甚至扔了一张带有微软 Logo 的定制桌面进去，来冒充正在使用 Windows 桌面工作的机器。

因为你这次安装的所有机器硬件配置是一致的，所以你可以在 ISO 镜像中增加一个预设的启动选项，这使得你可以从一个 U 盘启动并在没有任何用户干预的情况下安装好 Kali。让安装任务自动完成，并拥有一个全盘加密的系统。

棒极了！你现在已经按照你的需求，为你的机器硬件配置特别设计及优化更新了 Kali 系统版本，你节省了一整天的时间，任务完成！

我们其中的一些人需要从主流操作系统使用者身份中跳出，寻找更加干净、更具意义、更适合于我们工作方式的操作系统，而随着市场上硬件设备的膨胀式发展，上述这样的场景对我们而言变得越来越普遍。

对于投身于网络安全领域的我们更是如此，不管你将网络安全作为一种业余爱好、痴迷的兴趣，还是从事的行业。作为新手，我们经常发现被操作环境或操作系统所困，对于很多

新手而言，Kali 是他们进入 Linux 世界最早接触的系统。我在好几年前就认识到用户群体在这一转变中的困惑，并计划编写一本组织合理的入门引导书来帮助社区用户进入网络安全的世界，而不是一开始直接将所有 Linux 系统的复杂特性全部提供给他们。基于这样的考虑，《Kali Linux 大揭秘》这本书就诞生了。本书让所有通过 Kali Linux 进入网络安全领域的人都能受益。

现在这本书要面世了，然而我们很快意识到还有很多潜藏的“宝藏”有待发掘，因此在这本 Kali Linux 引导书之后，还有很多机会再去探索它更有趣但鲜为人知的特性，就像本书的书名一样，“Kali Linux 大揭秘”。

最后，我们对目前的结果非常开心，本书达到了我们的预期，我可以骄傲地说它已经超出了我们的预期。我们也意识到我们在不经意间扩展了本书的潜在读者群，它不仅仅是为网络安全领域的新手准备的，而且可以帮助一些有经验的渗透测试者提升与改进对 Kali Linux 的控制能力，使得他们可以解密 Kali Linux 发行版中我们准备的各种潜在特性。无论你面对的是一台机器，还是企业中上千台机器；无论是仅仅做配置上的微小修改，还是从内核级别开始完全定制并重建软件仓库；无论是仅仅触及 Debian 软件包管理系统的表层，还是深入探索，《Kali Linux 大揭秘》这本书都提供了路径图。

我代表自己和整个 Kali Linux 团队衷心祝愿，拥有这本导航手册在手，你能够拥有一个激动人心、充满快乐和收获的揭秘之旅！

Muts

2017 年 2 月

前　言

Kali Linux 是世界上最强大和最受欢迎的渗透测试平台，被网络安全领域的专家们广泛使用，其应用领域包括渗透测试、取证、逆向工程及漏洞评估。这是多年来我们精益求精和平台不断发展的结果，从一开始的 WHoppiX 到 WHAX，再到 BackTrack，最终发展到目前融入了 Debian GNU/Linux 以及充满活力的全球开源社区强大能力的完整渗透测试框架平台。

Kali Linux 并不是一个简单的工具集合，而是一个灵活的框架，专业渗透测试人员、安全从业者、学生和业余爱好者都可以根据自己的具体需求，来剪裁和定制它的功能。

为什么要写这本书

Kali Linux 不仅仅是一个在标准 Debian 发行版基础上安装了各种信息安全工具的集合，我们还针对它进行了很多预先的配置工作，以便让你能够立即启动和运行它。为了充分利用 Kali 的功能，你还应当深入了解强大的 Debian GNU/Linux 基础操作，以及学习如何将这些技能使用在你的应用场景中。

Kali 的确有很多用途，但它主要被设计用于渗透测试。本书的目的不仅在于帮助你轻松使用 Kali Linux，更在于提高你对系统的整体认识，使你的操作体验更加流畅，从而在你遇到时间紧迫的渗透测试任务时，无须浪费宝贵时间去安装新软件或者启用新的网络服务。在本书中，我们首先介绍了 Linux，然后更深入一步，介绍了 Kali Linux 的特别之处，以便你准确了解表象之下深层次的特性。

特别是当你时间紧任务重时，这些知识显得非常有价值。掌握这些更深层次的知识有助于你更好地设置 Kali，解决一些疑难问题，按照个人意愿更好地使用工具，分析工具的输出，或者在更大规模的测试场景中使用 Kali。

如果你渴望投身到充满智慧且令人着迷的网络安全领域，并且正好选择了 Kali Linux 作为主要操作平台，那么本书就是为你准备的。本书旨在帮助 Linux 新手以及 Kali 的现有用户加深对 Kali 基础知识的了解，那些已经使用 Kali 多年但希望更加系统深入学习 Kali 的读者，也能够通过本书扩大 Kali 的应用领域，填补之前对 Kali 认知的空白。

此外，本书还可以作为想考取 Kali Linux 认证专家资质读者们的学习大纲、技术参考以及学习指南。

本书的总体思路和结构

这本书的设计非常贴近实战，你从一开始阅读就可以动手去操作 Kali Linux，而不是阅读大量章节的理论介绍。本书对每个主题都以非常务实的方式来介绍，包含了许多样例和图示，以便使讲解更形象和具体。

在第 1 章“关于 Kali Linux”中，我们定义了一些基本术语，并解释了 Kali Linux 的用法。在第 2 章“Kali 入门”中，我们循序渐进地引导你下载 ISO 镜像并在计算机上运行 Kali Linux。第 3 章“Linux 基础”讲述了阅读本书需要了解的 Linux 基本知识，例如 Linux 系统架构、安装过程、文件系统层次结构、权限等重要概念。

至此，你已经使用 Kali Linux 作为自生系统有一段时间了。在第 4 章“安装 Kali Linux”中，将学习如何（在硬盘上）安装永久性的 Kali Linux。在第 5 章“配置 Kali Linux”中将学习如何按照喜好调整它。作为一个已入门的 Kali 用户，现在是熟悉 Kali 中一些重要资源的时候了，第 6 章“自助解决问题并获得帮助”提供了解决可能遇到的各种意外问题的方法。

在掌握了这些基础知识之后，将涉及更高级的主题。第 7 章“加固和监控 Kali Linux”提供了确保 Kali Linux 的安装能够满足你的安全要求的技巧。接下来，第 8 章“Debian 软件包管理”解释了如何充分发挥 Debian 软件包生态系统的潜力。而在第 9 章“高级用法”中，将学习如何创建完全定制的 Kali Linux ISO 镜像。如第 10 章“Kali Linux 企业级应用”中所述，当你在企业规模部署 Kali Linux 时，所有这些主题的内容都可能会用得上。

第 11 章“安全评估简介”使你将在本书中学到的所有知识与安全从业者日常工作联系起来，真正做到学以致用。最后一章，第 12 章展望未来的路。

Raphael Hertzog的致谢

我要感谢 Mati Aharoni！2012 年，当我还是数十名 Debian 顾问中的一员时，他与我联系，说想开发一个基于 Debian 的 BackTrack 替代版本。这就是我从事 Kali Linux 相关工作的开始，从那以后，我就喜欢上了我在 Kali 世界的旅程。

多年来，Kali Linux 越来越向 Debian GNU/Linux 靠近，特别是在基于 Debian 测试版分支的 Kali 滚动发行版之后。现在我的大部分工作，无论是基于 Kali 还是基于 Debian，都在为整个 Debian 生态系统做贡献，这正是我日复一日、年复一年继续下去的动力。

写这本书也是 Mati 给我的一个绝好机会。写书和 Kali 开发是完全不同的工作，但是具有相通的地方：都能够帮助他人并和他们一起分享我们在 Debian/Kali 操作系统领域的专业知识。基于我创作《Debian 管理员手册》的经验，希望我的文字能够帮助你迈出在快速发展的网络安全世界中的第一步。

我还要感谢所有对这本书做出过贡献的 Offensive Security 公司的伙伴们！Jim O'Gorman（一些章节的合著者）、Devon Kearns（评审员）、Ron Henry（技术编辑）、Joe Steinbach 和 Tony Cruse（项目经理）。同时也感谢 Johnny Long 参与撰写序言，并完成了整本书的评审。

Jim O'Gorman的致谢

我要感谢参与这个项目的所有伙伴！我的工作只是其中的一小部分。这本书很像 Kali Linux 本身，是一个由大家共同努力而使工作事半功倍的合作项目。特别感谢 Raphaël、Devon、Mati、Johnny 和 Ron，他们承担了绝大部分工作。没有他们，这本书不会问世。

Mati Aharoni的致谢

Kali Linux 第一个版本从发布到现在已经过去了好几年。从第一天起，我一直梦想着出版一本涵盖整个 Kali 操作系统的官方书籍。因此，我很荣幸能够把这本书奉献给公众。我衷心感谢参与这个项目的所有人，包括 Jim、Devon、Johnny 和 Ron。特别感谢 Raphael 做了本书绝大部分的繁重工作，并将珍贵的专业经验分享给我们的团队。

关于作者

Raphael Hertzog 拥有超过 20 年的 Debian 开发经验，并且是《Debian 管理员手册》的作者，他同时是 Kali 团队中的 Debian 权威。当他还没有进入 Kali 团队工作的时候，他通过自主创业的 Freexian 公司提供 Debian 专家咨询服务，帮助其他公司和个人创建 Debian 的派生定制化安装器和软件包管理系统，改进现有的软件包（bug 修补和增加新特性），等等。

Jim O'Gorman 是 Offensive Security 公司美国安全服务部的总经理，Jim 拥有超过十年在全球范围内对深度防御环境进行渗透测试的经验，此外 Jim 还是 Offensive Security 公司“使用 Kali Linux 进行渗透测试”认证培训的首席讲师。

Mati Aharoni 是信息安全界的一位老兵了，他活跃在安全社区已超过十年。Aharoni 创建了 Back Track 和 Kali 开源发行版，以及 Exploit DB 数据库项目，并创建了 Offensive Security，一家领先的信息安全公司，以工业界领先的安全证书认证和培训闻名于世。在漏洞利用代码开发与编目分类、渗透测试、Kali 开发和捣鼓硬件的过程中，Aharoni 享受着类似于传教士的角色，说服人们聆听关于 Kali Linux 的神奇。

目　录