李华峰　商艳红　高伟　毕红静　著

Kali Linux 2

网络渗透测试实践指南

从专业的视角
对网络的安全性
进行评估

详尽的内容引导
读者快速掌握
Kali Linux 2

真实的案例帮你
顺利开启网络安全
渗透之旅

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

Kali Linux 2

网络渗透测试

Kali Linux 2

网络渗透测试实践指南

李华峰　商艳红　高伟　毕红静　著

人民邮电出版社
北京

图书在版编目（CIP）数据

Kali Linux 2网络渗透测试实践指南 / 李华峰等著
. -- 北京 : 人民邮电出版社, 2018.5
ISBN 978-7-115-48033-0

Ⅰ. ①K… Ⅱ. ①李… Ⅲ. ①Linux操作系统－安全技术－指南 Ⅳ. ①TP316.85-62

中国版本图书馆CIP数据核字(2018)第043912号

内 容 提 要

Kali 是世界渗透测试行业公认的优秀的网络安全审计工具集合，它可以通过对设备的探测来审计其安全性，而且功能完备，几乎包含了目前所有的热门工具。

本书由资深的网络安全领域的教师编写完成，全书共 16 章，内容围绕如何使用 Kali 这款网络安全审计工具集合展开。本书涉及网络安全渗透测试的相关理论和工具、Kali Linux 2 使用基础、被动扫描、主动扫描、漏洞扫描、远程控制、渗透攻击、Armitage、社会工程学工具、BeEF-XSS 渗透框架、漏洞渗透模块的编写、网络数据的嗅探与欺骗、身份认证攻击、无线安全渗透测试、拒绝服务攻击、渗透测试报告的编写等内容。

本书面向网络安全渗透测试人员、运维工程师、网络管理人员、网络安全设备设计人员、网络安全软件开发人员、安全课程培训人员、高校网络安全专业方向的学生等。读者将从书中学习到实用的案例和操作技巧，更好地运用 Kali Linux 2 的工具和功能。

◆ 著　　李华峰　商艳红　高　伟　毕红静
责任编辑　胡俊英
责任印制　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市祥达印刷包装有限公司印刷

◆ 开本：800×1000　1/16
印张：24
字数：451 千字　　2018 年 5 月第 1 版
印数：1－2 400 册　　2018 年 5 月河北第 1 次印刷

定价：79.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

技术审校者简介

陈虹

这是一位天赋极佳的前端设计师，她在本书的编写过程中，从艺术的角度提出了很多重要且准确的建议。可以这样说，正是由于她的努力和智慧才保证了本书的顺利完成。

张珺、孟一珍

此二人有着丰富的 Web 开发经验，他们共同完成了本书 Web 相关部分的内容审校和修订工作。

赵宇

这是一位少有的同时精通 JAVA 语言和汇编语言的编码者，他协助完成了本书软件调试和漏洞渗透部分的内容审校和修订工作。

李爽

长期从事网络设计方面的工作，相关经验非常丰富，目前正在主讲 MPLS 与 VPN 方面的高级网络课程，她完成了本书网络相关部分的内容审校和修订工作。

序言：如何正确地运用网络攻防技术

我们暂且不谈 Kali，先来谈谈黑客。

长期以来，黑客在人们心目中都是一个神秘的职业。但是，在人们心目中这个职业为社会带来的好像更多的是负面的影响，因为只要一提到黑客，就会和攻击、泄密和破坏这些词汇联系到一起。然而事实确实如此吗？在现实生活中普通人很难见到从事这个职业的人，不过在影视作品中出现的黑客往往具备两个特点：足够聪明，喜欢单干。其实在现实生活中，黑客的年龄从十几岁到几十岁不等，他们从事着各种各样的职业，他们可能精通从编写病毒到漏洞测试的各种技能中的某一项。

虽然近年来，我们经常可以看到“某天才黑客被大企业以天价年薪招安”的新闻，但是绝大多数的黑客却并没有这么好的机会，他们的才华很难得到社会的肯定，要么没有企业接纳他们，要么企业接纳他们之后没有合适的岗位。所以很多拥有天赋的黑客选择了铤而走险，利用自己的技术走上了违法的道路。

就在不久前，我的一个大学同学创办的公司推出了一款新的行业软件。这款软件的前景十分光明，一时间几乎垄断了某省份该类软件的全部市场份额。可是好景不长，就在这款软件投入部署不久，研发部门收到了一封匿名邮件。这封邮件清楚地指出了该软件存在漏洞，并且这个漏洞会导致全部数据库信息的泄露。匿名邮件发送人开出了一个并不很高的价格，只要支付费用，就不会公布这个漏洞，并会提供修复的信息。

这件事情后来成为了我课堂上的一个经典案例，除了用来对这个类型漏洞进行分析之外，也用来帮助学习网络攻击这门课程的学生进行职业生涯规划。网络攻击是计算机专业中一个比较另类的课程，在这门课上讲述每一种技术，每一种工具，甚至每一个思路好像都不是为了建设，而是为了破坏。这些黑客技术就像是一件件武器，掌握了这些武器的人又该去做些什么呢，这些黑客技术能否用在正途上呢？

这个问题的答案很肯定。现在随着网络安全越来越受到各方面的重视，一个新兴的职业正在蓬勃发展起来，那就是网络安全渗透测试。在国外，出现了很多专门提供这个服务的企业；在国内，虽然起步较晚，但是前景却非常广阔。

网络安全渗透测试严格的定义应该是一种针对目标网络进行安全检测的评估。通常这种测试由专业的网络安全渗透测试专家完成，目的是发现目标网络存在的漏洞以及安全机制方面的隐患并提出改善方法。从事网络安全渗透测试的专业人员会采用和黑客相同的方式对目标进行入侵，这样就可以检测网络现有的安全机制是否足以抵挡恶意的攻击。

网络安全渗透测试专家将会像黑客一样思考，在别有用心的人之前找出目标的问题，

提前采取预防手段。

但是一个出色的黑客并不一定就是一个合格的网络安全渗透测试专家。因为很多黑客只掌握了众多技术中的一种，他们在某一个领域出类拔萃，但是可能对另一个领域毫无所知。而网络安全渗透测试专家必须掌握全面的知识。

本书讲解了大量的网络安全渗透测试的实例，希望能为各位有志于从事这个行业的读者提供一些帮助。祝各位成为网络安全渗透测试方面的优秀人才，为我国的网络安全与信息安全事业作出贡献。

李华峰

2018 年 1 月于唐山

致谢

多年前，我曾经领略了传奇黑客工具 BO2K 的神奇，对这款工具的创造者——“死牛之祭”（The Cult of the Dead Cow，CDC）也是极为仰慕。不过在许多年之后，我才知晓“死牛之祭”并非是一个人，而是一个团体。“死牛之祭”由很多人组成，有趣的是，他们中有的人完全不懂密码学，有的人又不怎么了解软件调试技术，但是他们中的每个人都有自己独特的技能。单独来看这些人中的每一个，可能都不是一个理想的黑客，但是当他们聚在一起的时候，却又变成了一股全世界都不能忽视的力量。

在本书的编写过程中，我曾经一度感到十分迷茫，网络安全渗透测试需要极为全面的知识和技能。因为现实中的网络安全渗透测试用“千里之堤，溃于蚁穴”来形容是再为贴切不过了，任何一个方面出错，都会影响到整个测试的成功与否。现在既然要系统地讲解网络安全渗透测试，那么如何能将各种渗透测试的技能都完整而又准确的介绍出来，这是一个十分严峻的挑战。受到“死牛之祭”的启发，我想为什么不去建立一个技能全面的团队呢？好吧，事实上我真的这样去做了。幸运的是，在短短的时间里，一些有着丰富经验的老手们纷纷加入了本书的编写和审校团队。十分感谢他们的参与和热情！本书的完成包含着你们辛勤的付出。感谢人民邮电出版社的胡俊英编辑，在本书的编写过程中始终支持我的写作，正是她的鼓励和帮助，我才能顺利完成全部书稿。

前言

时至今日，网络安全问题已经成为社会热点中的热点。随着近年来网络和计算机的安全越来越受重视，渗透测试技术已经成为网络安全研究的核心问题。而渗透测试的成功与否又取决于对目标信息的掌握情况，这就要求渗透测试者必须精通网络安全审计技术。尤其是对网络的保护者来说，精通网络安全审计技术，意味着可以先于攻击者发现网络和计算机的漏洞，从而有效地避免来自于企业内部和外部的威胁。因此无论是安全渗透测试人员、网络管理人员、网络安全设备和安全软件开发人员的工作都包含了网络安全审计技术。目前，国内的网络安全正处于起步阶段，大家所使用的工具多种多样，缺乏先进、专业、完善的学习资料，基本上都是依靠摸索学习。

而 Kali 是世界渗透测试行业公认的优秀的网络安全审计工具集合，它可以通过对设备的探测来审计它的安全性，而且功能极为完备，几乎包含了目前所有的热门工具。Kali 的强大功能是毋庸置疑的，它几乎是必备工具，你几乎可以在任何经典的网络安全图书中找到它的名字，甚至可以在大量的影视作品（例如最新的《黑客兵团》等）中看到 Kali 的身影。现在，国内对于 Kali 的研究也越来越热。近年来正是国内网络安全飞速发展的阶段，Kali 这个曾经只有顶尖高手才会涉及的工具，也逐步走入了普通网络安全工作人员的“寻常百姓家”，从而受到了广大网络安全从业人员的喜爱。假以时日，它势必将成为国内流行的网络安全审计工具。本人从 2009 年开始正式涉足网络渗透领域，对于 Kali 的使用，花费了大量的时间和精力进行研究，尤其是阅读了大量国外的相关文献。在本书中将会分享自己学习 Kali 的使用经验、方法，并对其精心汇总，希望可以减少其他 Kali 学习者的学习成本。

本书将 Kali 应用实例与网络原理相结合进行讲解，不仅讲述 Kali 的实际应用方法，还将从内部原理的角度来分析 Kali 实现网络安全审计的技术，实现了将各种网络协议、各种数据包格式等知识与 Kali 的实践应用相结合，真正做到理论与实践相结合。

读者对象

本书的读者对象如下：

- 网络安全渗透测试人员
- 运维工程师
- 网络管理员和企业网管
- 计算机相关专业的学生

- 网络安全设备设计与安全软件开发人员
- 安全课程培训人员

如何阅读本书

本书的结构是按照渗透测试的流程来展开编写的，全书内容共分为 16 章。

第 1 章 “网络安全渗透测试的相关理论和工具”，这一章对什么是网络安全渗透测试，以及如何开展网络安全渗透测试进行了介绍。

第 2 章 “Kali Linux 2 使用基础”详细地讲解了 Kali Linux 2 的安装和使用。

第 3 章 “被动扫描技术”，被动扫描是整个渗透测试过程中极为重要的一个阶段。这一章介绍了间接扫描中优秀的 3 种工具，分别是 Maltego、Recon-NG、ZoomEye。

第 4 章 “主动扫描”以 Nmap 为工具，详细地介绍了主动扫描的各种方法。

第 5 章 “漏洞扫描”介绍了在漏洞扫描阶段需要完成的任务。

第 6 章 “远程控制”以 Android 和 Windows 作为目标平台，通过实例介绍了 Metasploit 框架中提供的优秀工具 Meterpreter。

第 7 章 “渗透攻击”以网络安全渗透测试工具 Metasploit 的正式介绍作为开头，然后以实例的形式开始介绍 Metasploit 框架的使用方法。

第 8 章 “Armitage”引入了 Metasploit 的图形化操作界面——Armitage，这是一款由 Java 开发的工具。

第 9 章 “社会工程学工具”，在这一章中介绍了 Kali Linux 2 中社会工程学工具包的基本使用方法，工具包 social-engineer-toolkit 提供了大量成熟的社会工程学攻击方式，随后就其中最为经典的几种方式进行了介绍，

第 10 章 “BeEF-XSS 渗透框架的使用”介绍了一个新的渗透测试方法 XSS（跨站脚本攻击），这是一种令人防不胜防的渗透方式，用户往往只是访问了恶意攻击者建立的网站就会被渗透。

第 11 章 “漏洞渗透模块的编写”针对一个特定漏洞进行渗透模块开发，这是一个存在于 FreeFloat FTP Server 软件中的栈溢出类型漏洞。

第 12 章 “网络数据的嗅探与欺骗”介绍了如何在网络中进行嗅探和欺骗，这是极为有效的一种攻击方式。

第 13 章 “身份认证攻击”介绍了一些网络渗透中常见的密码破解方式。

第 14 章 “无线安全渗透测试”总结了无线网络的各种渗透方式。

第 15 章 “拒绝服务攻击”，按照 TCP/IP 协议的结构，依次介绍了数据链路层、网络

层、传输层和应用层中的协议漏洞，并讲解了如何利用这些漏洞来发起拒绝服务攻击。

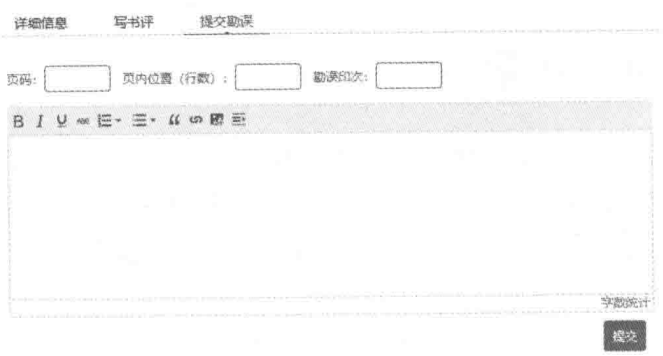
第 16 章 “渗透测试报告的编写”介绍了渗透测试报告的编写规范及包含的内容，并介绍了 Kali Linux 2 中最为优秀的测试报告编写工具 Dradis 的使用方法。

大家可以根据自己的需求选择阅读侧重点，不过还是希望能够按照顺序来阅读，这样不仅可以对渗透测试有一个清晰的认识，还可以对渗透测试中的技术有一个简单的对比。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免还会存在差错。欢迎您将发现的问题告诉我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区主页 https://www.epubit.com/，搜索到本书页面，点击 “提交勘误”，相应输入信息，最后单击“提交”按钮即可。之后本书的作者和编辑会对您提交的勘误进行审核。确认并接受后，您将获赠异步社区的 100 积分。积分可用于在社区兑换优惠券，以及兑换样书或奖品之用。



扫码关注本书

请扫描下方二维码关注本书，即可在异步社区微信服务号中看到本书和进一步的服务信息。

与我们联系

我们的联系邮箱是 contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请发邮件到此邮箱，邮件标题中请注明本书书名。

如果您有兴趣出版图书、录制教学视频，或参与图书翻译、技术审校等工作，可以发邮件，或者到异步社区在线提交投稿：

www.epubit.com/selfpublish/submission

如果您是学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，请发邮件联系我们。

如果您在网上发现有针对异步图书的各种形式的盗版行为，包括图书或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的举动是对作者权利的保护，我们也由此才能继续为您带来有价值的内容。

关于异步社区和异步图书

异步社区是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务，社区创办于 2015 年 8 月，提供超过 1000 种图书、近 1000 种电子书，以及众多技术文章和视频课程。更多详情请访问异步社区官网 https://www.epubit.com。

异步图书是由异步社区编辑团队策划出版的精品 IT 专业图书品牌，依托于人民邮电出版社近 30 年的计算机图书出版积累和专业编辑团队，在封面上印有异步图书的 LOGO。我们的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

关于异步社区和异步图书

异步社区是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务，社区创办于 2015 年 8 月，提供超过 1000 种图书、近 1000 种电子书，以及众多技术文章和视频课程。更多详情请访问异步社区官网 https://www.epubit.com。

异步图书是由异步社区编辑团队策划出版的精品 IT 专业图书品牌，依托于人民邮电

出版社近 30 年的计算机图书出版积累和专业编辑团队，在封面上印有异步图书的 LOGO。我们的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

社区二维码	服务号二维码
	

目录