HZ BOOKS
华章IT

[PACKT] PUBLISHING

·网络空间安全技术丛书·

MASTERING KALI LINUX FOR ADVANCED PENETRATION TESTING

Second Edition

Kali Linux 高级渗透测试

（原书第2版）

[印度] 维杰·库马尔·维卢（Vijay Kumar Velu）著　蒋溢 马祥均 陈京浩 祝清意 孙天勇 罗文俊 译

- Kali Linux 渗透测试经典之作全新升级，全面、系统阐释 Kali Linux 网络渗透测试工具、方法和实践
- 从攻击者的角度来审视网络框架，详细介绍攻击者“杀链”采取的具体步骤，包含大量实例，并提供源码

机械工业出版社
China Machine Press

Kali Linux 高级渗透测试

（原书第2版）

MASTERING KALI LINUX FOR ADVANCED PENETRATION TESTING

Second Edition

[印度] 维杰·库马尔·维卢（Vijay Kumar Velu）著

蒋溢 马祥均 陈京浩 祝清意 孙天勇 罗文俊 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Kali Linux 高级渗透测试（原书第 2 版）/（印）维杰·库马尔·维卢（Vijay Kumar Velu）著；蒋溢等译 . —北京：机械工业出版社，2018.3
（网络空间安全技术丛书）
书名原文：Mastering Kali Linux for Advanced Penetration Testing, Second Edition

ISBN 978-7-111-59306-5

I. K… II. ①维… ②蒋… III. Linux 操作系统 - 安全技术 IV. TP316.85

中国版本图书馆 CIP 数据核字（2018）第 041464 号

本书版权登记号：图字 01-2017-7342

Kali Linux 高级渗透测试（原书第 2 版）

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：陈佳媛 责任校对：李秋荣
印 刷：北京市兆成印刷有限责任公司 版 次：2018 年 3 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：19.5
书 号：ISBN 978-7-111-59306-5 定 价：79.00 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）88379426 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzit@hzbook.com

华章IT
HZBOOKS | Information Technology

Foreword 推 荐 序

时隔一年，《Kali Linux 高级渗透测试》（原书第 2 版）这么快就跟读者见面了，不得不感叹网络空间安全技术的发展日新月异。

刚刚过去的 2017 年，勒索病毒 WannaCry 肆虐全球，各种“邮件门”、个人隐私泄露事件层出不穷，网络安全问题更加突出。也正是在 2017 年 6 月 1 日，我国首部网络安全法——《中华人民共和国网络安全法》正式实施，成为我国第一部规范网络空间秩序的基础性法律，该部法典从法律层面明确了网络安全保护的基本原则和要求，对于技术人员则需要从技术层面去研究实践如何提高网络攻击防御技术，提升网络系统的安全保护能力。渗透测试作为主动防御的一种重要手段，其重要性不言而喻。本书在第 1 版的基础上，增加了部分章节，更加全面、系统地介绍了 Kali Linux 在渗透测试中的高级应用，相信能够为国内从事空间网络安全的相关人员提供最前沿的技术参考。

本书由网络空间安全方面的教授和行业专家合作翻译，译者不但理论水平高，而且还拥有丰富的业务实践经验，尤其在渗透测试方面更是实干的权威行家。本书译文忠实原著，是一部高质量的学术译著。本书既可作为网络空间安全专业领域的研究开发人员、工程技术人员及高级技术主管的工具书，也可作为高校研究生和高年级本科生学习网络安全相关课程的参考书。

网络空间安全学科建设任重道远，学科的统一基础理论有待创立；心理学、管理学、经济学、社会学、安全熵、赛博学等因素对网络空间安全的影响有待深入探讨；借助科普提升普通大众的网络空间安全意识才刚刚开始；网络空间安全的各种攻防新手段、新思路永无止境。但愿此书能为此添砖加瓦；但愿已经（或即将）出版的《安全通论》《安全简史》《安全心理学》和《安全管理学》等，能为网络空间安全学科建设尽一点绵薄之力。

杨义先

2018 年 1 月

作者简介 *About the Author*

Vijay Kumar Velu 是一位充满激情的信息安全从业者、作者、演讲人和博主。他目前是马来西亚的 Big4 的副总监之一，拥有超过 11 年的 IT 行业经验，拥有渗透测试人员资格证书，专门为各种网络安全问题提供技术解决方案，包括简单的安全配置审查、网络威胁情报，以及事件响应等方面。Vijay 有多个安全职业头衔，包括 CEH（道德黑客）、EC 委员会安全分析师和计算机取证调查员。

Vijay 受邀在印度各种网络安全大会上发表过演讲，包括国家网络安全峰会（NCSS）、印度网络会议（InCyCon）、开放云会议（Open Cloud Conference）等；他还在印度各大商学院举办的重要信息安全培训会上做了多次客座讲座。

Vijay 还撰写了《Mobile Application Penetration Testing》一书，并且审校了 Packt 出版的《Learning Android Forensics》一书。

在信息安全界，Vijay 是吉隆坡云安全联盟（CSA）董事会成员，也是印度国家网络防御与研究中心（NCDRC）主席。工作之余，他喜欢演奏音乐和做慈善事业。

Vijay 是新技术的采用者，喜欢听任何疯狂的想法——所以，如果你有一个创意、产品或服务，不要犹豫，与他联系。

特别感谢我的母亲、姐姐、兄弟和父亲对我的信任，他们总是鼓励我做我喜欢的事，甚至疯狂的事。不能忘记感谢我的黑客朋友（Mega、Madhan、Sathish、Kumaresh、Parthi、Vardha）和我的同事 Rachel Martis 及 Reny Cheah 的支持。

感谢 Packt 出版社在本书的整个出版过程中提供的所有支持，对 Chandan 和 Deepti 表示特别的感谢！感谢他们完美的协调工作！

About the Reviewer 审校者简介

Amir Roknifard 是一名自学成才的网络安全解决方案架构师，专注于 Web 应用、网络和移动安全。他领导马来西亚 KPMG 的研究、开发和创新，并且爱好编码与程序开发，他喜欢花时间教导人们理解隐私和安全，即使是普通人也可以用知识来保护他们自己。他喜欢自动化，并为网络防御团队开发了一个综合平台，以便他们能轻松地工作：从需求票据表到最终报告。

Amir 已经完成了许多项目，包括政府、军队，以及无国界的公共部门，他为银行、金融机构、石油、天然气，以及电信公司工作。他也曾开展数小时的 IT 和信息安全专题讲座。

Amir 还创办了《 Academician Journal 》，旨在缩小学术界与信息安全行业之间的差距，试图找出这个差距发生的原因，分析和解决它们。他提出了可能解决未来问题的新思路并研究如何发展它们。所以，有类似想法的人总是乐于通过 @roknifard 分享他们的想法或者共同发表研究成果。

译者简介 *About the Translators*

蒋　溢　博士、正高级工程师、硕士生导师，重庆邮电大学计算机科学与技术学院副院长，重庆市移动互联网数据应用工程技术研究中心负责人，重庆高校“移动互联网大数据创新团队”带头人，重庆高校移动互联网大数据智能处理众创空间负责人。主要从事移动互联网网络安全、服务计算、海量数据处理与分析等领域研究。出版学术专著两部；获重庆市科技进步奖两项。

马祥均　从事网络安全十余年，精通计算机网络，擅长利用 OSI 七层模型审视和规划计算机与网络安全，对大数据和人工智能有一定研究。

陈京浩　副高级工程师，拥有 9 年网络安全领域从业经验，主要感兴趣的领域包括 Web 安全、网络设备安全及风险评估。

祝清意　博士，重庆邮电大学网络空间安全与信息法学院讲师，主要研究领域为网络安全动力学。

孙天勇　硕士，四川公众监理咨询有限公司高级工程师，从事通信及网络信息安全工作 15 年。

罗文俊　博士，重庆邮电大学网络空间安全与信息法学院教授，为研究生、本科生讲授信息安全课程。

Preface 前　言

本书致力于介绍如何使用 Kail Linux 对网络、系统、应用执行渗透测试。渗透测试可以模拟内部或外部的恶意攻击者对网络或系统进行的攻击。不同于漏洞评估，渗透测试包括漏洞利用阶段。因此，漏洞是存在的，而且如果不采取相应的措施将会有很大风险。

在本书中，“渗透测试人员”“攻击者”和“黑客”使用完全相同的技术及工具评估网络和数据系统的安全性。他们之间唯一的区别是他们的目标——数据网络的安全或数据的外泄。

简而言之，本书将带你踏上渗透测试者之旅：使用一些成熟的工具，在使用 Kali Linux 的网络上打败最新的防御，从选择最有效的工具，到网络安全快速响应，再到最重要的避免检测技术。

本书涵盖的内容

第 1 章介绍了贯穿全书的渗透测试方法的功能概要，确保全书遵循一致和全面的渗透测试方法。

第 2 章提供了一个背景，说明如何利用公共可用的资源和工具收集有关目标的信息，从而简化侦察和信息管理。

第 3 章向读者介绍可用于获取有关目标信息的隐秘方法，特别是识别可利用的漏洞的信息。

第 4 章教你掌握扫描网络及其设备的半自动化过程，接受所有侦察和漏洞信息，评估并创建一个指导渗透测试过程的地图。

第 5 章说明了如何能够物理地访问一个系统，或与管理人员进行交互，从而提供最成功的利用方法。

第 6 章简要介绍了无线技术，重点介绍了绕过安全防范进而危害这些网络的常用技术。

第 7 章简要概述了一个最复杂的交付阶段，以确保基于 Web 的应用暴露在公共网络上。

第 8 章从安全的角度介绍了最常用的远程访问技术，说明了可利用的弱点在哪里，以及如何在渗透测试中验证系统的安全性。

第 9 章着重介绍对最终用户系统上的应用程序的攻击，这些终端系统常常没有得到与组织的主干网络相同级别的保护。

第 10 章演示最常见的安全控制，找出克服这些控制的系统过程，并演示如何使用 Kali 工具集的工具。

第 11 章演示了攻击者发现和利用系统漏洞的方法。

第 12 章重点讨论直接的后利用活动和横向扩展，即利用被控制系统作为起点，“跳”到网络上的其他系统。

第 13 章演示了渗透测试人员如何拥有系统各方面的操作权限；更重要的是，获得一些访问权限，将允许测试人员控制网络上的所有系统。

第 14 章重点讨论现代攻击者如何使数据转移到攻击者的本地位置，以及隐藏攻击的证据。

学习本书需要准备什么

为了练习本书中出现的示例，需要虚拟化工具，例如 VMware 或者 VirtualBox。

需要下载和安装 Kali Linux 操作系统及工具套件。通过访问互联网来确保你的系统是最新的，并且安装了所有的工具。

不幸的是，不是 Kali Linux 系统上的所有工具都会呈现，因为工具太多了。本书的目标不是将所有的攻击和选项展现给读者，而是提供一个测试方法，这个方法可以为读者提供学习和掌握新工具的机会，经过一段时间后，将它们变为自己的经验和知识。

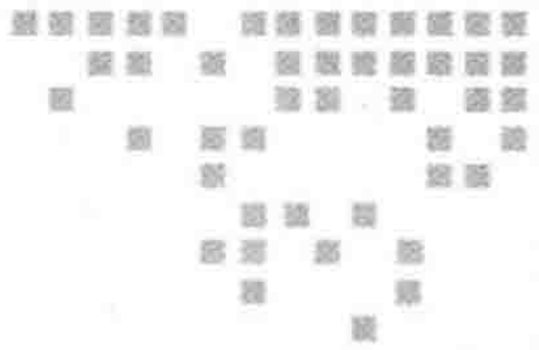
虽然本书中大多数示例是基于 Microsoft Windows 的，但是方法和大多数工具是可以转换到其他操作系统的，例如 Linux 和其他 UNIX 系统。

最后，本书应用 Kali 来完成攻击者的攻击流程，对目标系统进行攻击。你需要一个目标操作系统。本书的许多示例是基于 Microsoft Windows 7 和 Windows 2008 R2 的。

读者对象

如果你是一个渗透测试者、IT 专业人士，或安全顾问，想要通过使用 Kali Linux 的先进功能最大程度地完成网络测试任务，那么本书是为你准备的。之前有一些渗透测试 / 道德黑客的基础知识会帮助你充分利用本书。

Contents 目　录



第 1 章 Chapter 1

基于目标的渗透测试

“这个世上只有两种人，黑客和被黑客攻击的人。”

所有事情都是围绕一个目标来实现的。因此，在本章中，我们将讨论基于目标的渗透测试的重要性；并且描述一些在没有目标的情况下，漏洞扫描、渗透测试和红队练习的经典失败案例。本章还对安全测试做了一个总结，介绍了如何搭建实验室环境，重点讨论了如何自定义 Kali 以支持渗透测试的一些高级内容。阅读完本章，你将了解到以下内容：

- 安全测试的概述
- 漏洞扫描、渗透测试和红队练习的经典失败案例
- 更新和组织 Kali
- 使用 BASH 脚本自定义 Kali
- 设置定义的目标
- 构建运行环境

1.1 安全测试的概念

世界各地的每个家庭，每个个体、公共企业或私人企业在网络空间中都存在各种顾虑，例如数据丢失、恶意软件和网络恐怖主义等。这些都围绕一个概念——保护。如果你问 100 位不同的安全顾问：“什么是安全测试?”可能会听到不同的回答。其中最简单的解释为：安全测试是一个过程，用于验证信息资产或系统是否受到保护，并且验证保护功能是否按照预期效果执行。