HZ BOOKS
华章IT

[PACKT]
PUBLISHING

信息安全
技术丛书

资深网络安全专家撰写，全面、系统阐释Kali Linux网络渗透测试工具、方法和最佳实践

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

Kali Linux 高级渗透测试

[加] 罗伯特 W. 贝格斯（Robert W. Beggs）著
蒋溢 马祥均 陈京浩 罗文俊 祝清意 译

MASTERING KALI LINUX FOR ADVANCED PENETRATION TESTING

机械工业出版社
China Machine Press

信息安全
技术丛书

Kali Linux
高级渗透测试

[加] 罗伯特 W. 贝格斯（Robert W. Beggs）著
蒋溢 马祥均 陈京浩 罗文俊 祝清意 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 /（加）贝格斯（Beggs，R. W.）著；蒋溢等译 . —北京：机械工业出版社，2016.5
（信息安全技术丛书）
书名原文：Mastering Kali Linux for Advanced Penetration Testing

ISBN 978-7-111-53639-0

I. K… II. ①贝… ②蒋… III. Linux 操作系统 – 安全技术 IV. TP316.89

中国版本图书馆 CIP 数据核字（2016）第 085977 号

本书版权登记号：图字：01-2015-7679

Kali Linux 高级渗透测试

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：殷　虹
印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2016 年 5 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：15.25
书　　号：ISBN 978-7-111-53639-0　　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）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

Forword 推荐序

随着“网络空间安全”被国务院学位委员会正式批准为国家一级学科，特别是随着北京邮电大学等高校正式获批该一级学科博士点，网络空间安全人才的培养将掀起一个新高潮：网络空间安全学院将如雨后春笋般，在许多高校成立；安全专业的本科生、硕士生和博士生等人员规模将大幅度提高；更多的精英人才进入网络空间安全领域，从事产学研等活动；网络空间安全保障体系的整体布局将更加全面、合理，比如，将有更多的力量部署于主动防御领域等。

主动防御的“杀手锏”之一，便是本书的主题：渗透测试。而它也是网络空间安全教育方面的弱项。虽然我们知道渗透测试很重要，知道它可以评估网络系统的安全措施及策略是否有效，知道用它可以发现并预防潜在的安全风险，知道它有很高的应用价值，但是，据我所知好像很少有高校全面、系统地开设过渗透测试方面的课程，通常只是零星地提及过相关的技术和思路。我希望，也坚信这种局面会很快改变，因此，及时引进国际上有关渗透测试方面的高水平专著就显得尤为重要了。当然，无论是翻译还是撰写渗透测试方面的书籍，都不是件容易的事，因为它不但需要精湛的文字翻译技巧，更需要对渗透测试的相关技术和理念有深入的理解，还需要有丰富的实践动手经验等。

Kali Linux 是迄今为止，国际知名度很高，各方评价也很好的少有的计算机安全检测系统。它集成了大量精心挑选的渗透测试和安全审计工具。本书全面、系统且深入地介绍了 Kali Linux 在渗透测试中的高级应用，堪称渗透测试方面的经典之作，是国际影响很大、权威性很高的专著。希望本书的翻译出版，能够为国内从事空间网络安全和对抗的人员提供国际前沿的技术指南。

本书由网络空间安全方面的教授和专家合作翻译，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，对某些难点进行了反复推敲，是一部高质量的学术译著。本书可作为网络空间安全专业领域的研究开发人员、工程技术人员及高层技术主管的参考书。希望也能够尽快成为相关高校博士生、硕士生和高年级大学生的参考书。

杨义先

2016 年 3 月

About the Author 作者简介

罗伯特 W. 贝格斯（Robert W. Beggs）是 Digitial Defence 公司的创始人和首席执行官，该公司专门从事信息安全事件的预防和处理。他拥有超过 15 年的安全业务技术管理经验，涉及有线和无线网络的渗透测试、事件响应、数据取证等内容。

罗伯特是一个资深的信息安全传播者，并且是多伦多地区安全大会（Toronto Area Security Klatch，TASK）的联合创始人之一，在北美多伦多地区安全大会是众所周知的、最大的独立 – 供应商安全用户群。他是部门安全会议（SecTor Security Conference）咨询委员会的成员，以及其他几个安全学术委员会的成员。他是一个热心的安全培训教师，他在加拿大几所大学教授研究生、本科生和继续教育学生的信息安全课程。

罗伯特拥有女王大学的计算机科学与技术 MBA 学位，同时是一个认证信息系统安全专家。

首先，最重要的是，感谢 Kali Linux 的开发者和支持者。经过共同的努力，他们创造了一种保护网络和数据安全的最重要工具。感谢 Packt 出版社的编辑和审稿人的支持，感谢他们在写作本书的过程中给予我无止境的包容。我保证接下来将以更快速度工作！

我还要感谢布瑞恩 · 伯恩（Brian Bourne）和 TASK 的其他成员。他们给了我一个令人难以置信的机会，与最好的安全极客社区学习和分享知识。

在本书的写作过程中，我的家人给了我源源不断的动力和支持。谢谢莎拉、亚历克斯和安妮卡。

最后，特别感谢我的母亲和父亲（我不记得何时学会了阅读），在他们的鼓励下，我养成了读书的习惯。

谢谢。

审校者简介 *About the Reviewers*

Terry P. Cutler 是网络安全专家，IT 安全和数据防御公司——Digital Locksmiths 公司的联合创始人和首席技术官，该公司位于加拿大的蒙特利尔。他们保护小企业、大型机构、家庭和个人免受网络罪犯的伤害，据估计每天约有 150 万人在遭受网络犯罪的伤害。

他擅长于为政府、企业、商家和消费者，预测、评估与防范安全漏洞。自 2005 年起，他曾在 2500 名现场观众、世界上成千上万的直播观众和录制的视频的观众面前，表演一个黑客利用假的 LinkedIn 请求入侵几乎任何一家公司。

自 2006 年起，Terry 已经为孩子、父母、执法机关提供互联网安全。他认为预防、街头宣传和亲子沟通是防止孩子被绑架或沦落为激进与冒险牺牲品的最有效的方法。给孩子们保护自我的知识和实践技能与教他们读和写同等重要。在网站 http://www.TheCourseOnInternetSafety.com 上，可以找到更多的相关内容。

他经常在媒体发表关于家庭和个人每一天必须面对的真实网络危险的内容，包括网络犯罪、网络间谍、安全故障、网络诈骗等。他是一位公认的变革型领导者、解决问题者、值得信赖的顾问，是一个能促进各级组织共同积极合作、协同工作的真正人才。

Terry 从 2011 年开始全职经营 Digital Locksmiths 公司，在 2011 年之前，Terry 供职于一家软件巨头——Novell。他加入这一全球性的软件公司，该公司专业提供企业操作系统和身份、安全和系统管理解决方案，为公司在全世界多达 45 000 个用户和 600 台服务器的优质客户提供技术支持。

感谢罗伯特在 2004 年作为导师，慷慨地引导我在这个行业工作，其中历尽艰辛、躲避陷阱。

现在，我已经成长为一名行业专家，我很荣幸能够与罗伯特及其他的读者分享一些自己的经验。

特别感谢我的家人，我的妻子 Franca，我的儿子 David 和 Matthew，感谢他们在过去几年中的支持、鼓励、耐心、包容和无条件的爱。

Danang Heriyadi 是印尼的一位计算机安全研究员，专门从事逆向工程和软件开发，拥有超过五年的实践经验。

Danang 目前在 Hatsecure 公司工作，是高级开发（Advanced Exploit）与 Shellcode 开发（Shellcode Development）的教员。作为一位研究者，他喜欢通过他在 Fuzzerbyte（http://www.fuzzerbyte.com）的博客分享 IT 安全知识。

感谢父母给了我生命；没有他们，就不会有今天的我；我的女朋友每一天用微笑和爱支持我；还有我的朋友们，对他们的谢意我无以言表。

Tajinder Singh Kalsi 是 Virscent Tehnologies 公司的联合创始人和技术专家，在 IT 领域拥有超过六年的工作经验。Tajinder 以 Wipro 技术助理开启了他的职业生涯，接着他成为一名 IT 顾问和培训师。截至目前，Tajinder 在印度各地的学院举办的研讨会主题包括信息安全、Android 应用程序开发、网站开发和云计算等；他的工作已经覆盖了超过 120 所学院及 9000 多名学生。除了培训之外，Tajinder 还有一个博客（www.virscent.com /blog），他在博客上解释各种黑客技巧。Tajinder 之前曾审阅了由 Joseph Muniz 和 Aamir Lakhani 编著，Packt 出版社出版的《*Web Penetration Testing with Kali Linux*》一书。

可以在 Facebook 的 www.facebook.com/tajinder.kalsi.tj 页面上找到 Tajinder，也可以在他的个人主页 www.tajinderkalsi.com 上关注他。

感谢 Packt 出版社的团队通过我的博客联系我，并且再次给我这个机会。还要感谢我的家人和亲密的朋友，感谢他们在我完成这个项目的工作期间给我的所有支持。

Amit Pandurang Karpe 是 FireEye 公司的员工，FireEye 是一个跨国信息安全公司，Amit 是服务亚太地区客户的支持工程师。Amit 与他的妻子 Swatee 和儿子 Sparsh 住在新加坡。Amit 从大学时代开始就一直活跃在开源社区，特别是 Pune，在那里他组织了各种活动使社区充满活力，如 PLUG、TechPune、IT-Milan、Embedded Nirvana 等。Amit 写的技术博文参见 http://www.amitkarpe.com。

Amit 曾经与 Dai Xuewu 博士、Qin Fei 博士合著了《*Rapid BeagleBoard Prototyping with MATLAB and Simulink*》，由 Packt 出版社出版。目前，他正致力于完成两本著作《*Building Virtual Pentesting Labs for Advanced Penetration Testing*，*Kevin Cardwel*》和《*Kali Linux CTF Blueprints*，*Cam Buchanan*》。

感谢开源社区，没有开源社区，我不可能成功。特别感谢 Kali Linux 背后的梦想家，他们坚持开放源代码并且主动提供各种实例。同时，感谢社区成员和信息安全专家，他们做了大量的工作，促使 Kali Linux 成功。

感谢 Packt 出版社的团队、编辑和项目协调员，他们坚持做正确的事情，才使我能以最好的工作状态完成工作。

感谢 Pune Linux Users Group（PLUG）、Embedded Nirvana 组和 VSS 的朋友们，基于他们的支持我才能胜任这个项目。感谢在这一领域帮助过我的所有人，他们都是我的良师益友——Vijay Gokhale 博士、Sunil Dhadve、Sudhanwa Jogalekar、Bharathi Subramanian、Mohammed Khasim 和 Niyam Bhushan。

最后，感谢我的家人，我的父母、我的兄弟、我的儿子、我的妻子 Swatee，没有他们一直以来的支持，我不可能全身心投入这个项目。

Ashish Pandurang Karpe 是 CompuCom-CSI Systems India 公司的系统支持专员。Ashish 从大学开始就一直活跃在开源社区，在那里他能够组织各种活动使社区充满活力，如 PLUG 和 VITLUG。

首先要感谢开源社区，没有他们的帮助，我不可能在这里。其次要感谢我的家人，他们是 Anuradha（母亲）、Pandurang（父亲）、Sparsh（侄子）、Amit（兄弟）和 Swatee（嫂子）。我要感谢 Packt 出版社的团队、编辑和项目协调员，他们坚持做正确的事情，才使我能以最好的工作状态完成工作。

感谢 Pune GNU/Linux Users Group（PLUG）。也感谢我的导师——Vijay Gokhale 博士，他在这个领域帮助并指导我前行。

Kunal Sehgal 从 2006 年在加拿大乔治亚学院学习网络安全开始，他就一直从事 IT 安全行业方面的工作。Kunal 一直与各种金融机构合作。这不仅表明 Kunal 具有关键安全岗位的经

验，还证明他在这一领域是一位有价值的专家。你可以在 KunSeh.com 找到他。

Kunal 目前负责欧洲最大的一个银行在亚太地区的 IT 安全运维项目。Kunal 在各种不同的安全方向上都积累了丰富的经验，从漏洞评估到安全治理，从风险评估到安全监控。在专业领域他总会更新最新动态，Kunal 出版著作、举办讲习班、写博客，所有工作都为促进 IT 安全。Kunal 还持有多个证书，包括 OSCP、CISSP、TCNA、CISM、CCSK、Security+、Cisco Router Security、ISO 27001 LA 和 ITIL。

我是 Backtrack 项目（现在的 Kail）的大力支持者，首先，感谢他们的核心团队。值得一提的是，感谢那些无名人士，没有他们的训练和关注，我不可能迷恋 Kail。在个人方面，感谢我的家人（父母、兄弟、妻子），他们给予我无尽的支持和信任。我承认，我忽略了他们，沉浸在网络世界里。

前　言 Preface

本书致力于介绍如何使用 Kali Linux 对网络执行渗透测试。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。

在这本书中，“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。

大多数的测试人员和攻击者遵循一个非正式的、开源的或专门定义的测试方法，指导测试过程。下面的一些方法有其固有的优势：

- 测试过程的部分方法可以自动生成（例如，测试人员可以经常使用 ping 扫描发现潜在的目标；因此，这可以作为脚本利用），鼓励测试人员把重点放在发现和利用漏洞的技术创新上。
- 结果是可重复的，允许反复比较，交叉验证测试的结果，确定随着时间的推移，目标的安全性是否有所改善。
- 定义的方法在时间和人员的要求方面是可见的，鼓励成本控制并使成本最小化。
- 测试方法已经预先获得客户批准，在对网络或数据造成任何损害时测试人员免责。

正式的方法包括以下著名的例子：

- Kevin Orrey 的渗透测试框架：这种方法为测试人员提供一个渗透测试的序列步骤，以及工具的超链接和相关命令。更多信息请参见 www.vulnerabilityassessment.co.uk。
- 信息系统安全评估框架（Information Systems Security Assessment Framework，ISSAF）：这个综合性指南的目标是单一的网络测试，更多信息请参见 www.oissg.org。
- NIST SP 800-115，信息安全测试和评估技术手册：完成于 2008 年，这种四步走的方法

已经有些过时。然而，它确实为渗透测试提供了一个很好的基本步骤总结。更多信息请参见 http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf。

- 开源安全测试方法手册（Open Source Security Testing Methodology Manual，OSSTMM）：这个最老的方法之一，并且最新版本试图量化确定的风险。更多详细内容参见 www.osstmm.org。
- 开放 Web 应用安全工程（Open Web Application Security Project，OWASP）：该工程主要关注了基于 Web 应用的 10 个最常见的漏洞。更多信息请关注 www.owasp.org。
- 渗透测试执行标准（Penetration Testing Execution Standard，PTES）：积极维护，这种方法能完整并且精确地反映恶意者的行为。更多信息请关注 www.pentest-standard.org。
- 攻击（Web）测试框架（Offensive（Web）Testing Framework，OWTF）：在 2012 年提出，结合了 OWASP 方法和更完整、严格的 PTES 方法，这是一个非常有前途的研究方向。更多详细信息请关注 https://github.com/7a/owtf。

但是，使用一个结构化的渗透测试方法可能会导致测试过程陷入泥潭：

- 模型中很少考虑为什么要进行渗透测试，或哪些数据是业务的关键数据，并且需要保护。缺少这至关重要的一步，渗透测试无法抓住重点。
- 很多渗透测试人员不愿遵循现成的模型方法，他们担心模型会阻碍他们进行网络渗透的创造力。
- 渗透测试不能反映恶意攻击者的实际活动。通常，客户希望看到你能不能在一个特定的系统中获得管理上的访问权（“你可以打开这个盒子吗?”）。然而，攻击者可能会重点关注复制关键数据的方式——不需要底层接入，或引起拒绝服务。

为了解决形式化测试方法所固有的局限性，它们必须被整合在一个框架中，从一个攻击者的角度看这个网络框架，这就是“杀链”(kill chain)。

渗透测试的“杀链”方案

在 2009 年，Lockheed Martin CERT 的 Mike Cloppert 介绍了这个概念，现在被称为“攻击者杀链”（attacker kill chain）。当攻击者攻击网络时，“杀链”包含攻击者采取的步骤。“杀链”不总是以一个线性流呈现，因为一些步骤可能会并行出现。多发攻击可以对同一个目标瞬时进行多种攻击，并且在同一时间攻击步骤可能发生重叠。

在本书中，我们已经修改了 Cloppert 的杀链，使之能更准确地反映攻击者如何在测试网络和数据服务时应用这些步骤。下图显示了一个攻击者的典型杀链：

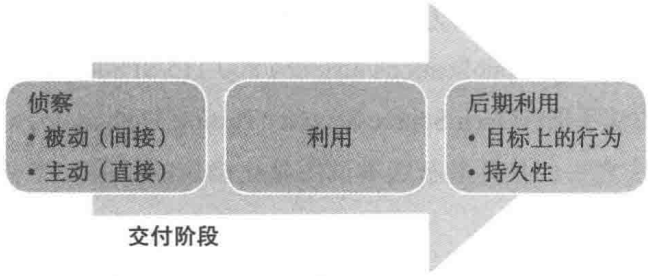

图　典型的杀链

一个攻击者的典型杀链可以描述为：

- 侦察阶段。有一句格言："侦察永远不浪费时间"。大多数军事组织承认，在进攻敌人之前，最好尽可能地去了解敌人的一切信息。同样，攻击者在攻击之前也会对目标展开广泛的侦察。事实上，据估计，针对渗透测试或攻击，至少有 70% 的"工作量"是进行侦察！一般来说，可采用两种类型的侦察：
  - 被动侦察。这种方式并不直接与目标以敌对方式进行交互。例如，攻击者将会审查公共的可用网站，评估在线媒体（尤其是社交媒体网站），并试图确定目标的"攻击表面"。

    一个详细的任务将会产生一份过去和现在的雇员名称的列表。这些名称将成为尝试蛮力攻击或密码猜测的基础。同样它们也被用到社会工程的攻击中。

    这种类型的侦察很难从普通用户的行为中区分出来。
  - 主动侦察。这种方式可以被目标检测到，但是很难从常规的背景中区分出大多数在线组织的表现。

    主动侦察期间的活动包括物理访问目标前端、端口扫描和远程漏洞扫描。
- 交付阶段。交付是选择和开发武器，武器用于完成攻击中的任务。精确的武器选择取决于攻击者的意图以及实施路线（例如，借助网络、通过无线，或通过基于 Web 的服务）。交付阶段的影响将在本书第二部分进行研究。
- 利用或攻击阶段。一个特定的漏洞被成功利用的时刻，此时攻击者实现他们的目标。攻击可能已经在一个特定的情景下发生（例如：通过缓冲区溢出利用一个已知操作系统的安全隐患），或者攻击可能在多个情景下发生（例如：一个攻击者物理访问公司住所，偷取他们的电话簿，用公司员工的名字来创建门户登录蛮力攻击列表。此外，电子邮件被发送到所有员工以引诱他们单击一个嵌入式链接，下载制作的 PDF 文件，这些文件会危及员工的计算机）。当恶意攻击者针对特定的企业时，多情景攻击是常态。
- 后期利用阶段 : 对目标的行动。这经常被称为"渗漏阶段"（exfiltration phase），这是错

误的，因为通常理解的攻击，仅仅以窃取敏感信息作为唯一的目的（如登录信息、个人信息和财务信息）；但是，通常情况下，攻击者有不同的攻击目标。例如，这一阶段必须专注于攻击者的许多可能的行动。

最常见的利用活动是攻击者试图提升他们的访问权限到最高级（纵向升级），并且破解尽可能多的账号（横向升级）。

- 后期利用：持久性。如果攻击一个网络或者系统是有价值的，那么这个价值很可能在持续攻击下增长。这就需要攻击者持续与被攻破的系统之间保持通信。从防护者的角度来看，这是攻击杀链中最容易检测到的一部分。

当攻击者试图攻击网络或特定的数据系统时，攻击杀链是攻击者行为的一种基本模型。作为一种元模型，它可以吸收任何私人的或商业的渗透测试方法。但是，也不同于这些方法，它使攻击者在一个战略高度上关注如何接近网络。这种专注于攻击者的活动将引导本书的布局和内容。

本书涵盖的内容

本书分为两个部分。第一部分会根据杀链的步骤，详细分析每个阶段。第二部分会专注于交付阶段和一些有用的方法，来明确攻击是怎么发生的，以及如何用这种方法来保护网络。

第 1 章介绍了 Kali Linux 的基础知识和它支持渗透测试的最优配置。

第 2 章提供了一个关于怎么样利用公共可用资源搜集目标信息的背景，以及简化侦察和信息管理的工具。

第 3 章介绍用来获得目标信息的隐形方法，尤其是识别漏洞的信息，这种信息可以充分利用。

第 4 章证明了可以用来找到并执行渗透的方法，允许黑客攻击一个系统。

第 5 章描述攻击者怎样逐步提高自己的权限，实现他们攻击系统的目标，包括盗窃数据、改变数据、发动更多的攻击，或创建一个拒绝服务。

第 6 章介绍了怎样设置一个受损系统，以便攻击者可以任意返回和继续利用漏洞进行攻击。

第 7 章介绍了为什么可以在物理上访问一个系统，或者与系统管理者交互，该章提供了一个最佳的利用方法。

第 8 章阐明了怎样利用普通无线链接来访问数据网络与隔离系统。

第 9 章提供一个关于获得安全的、最复杂的交付阶段的简要综述：暴露在公共因特网上的基于 Web 的应用。

第 10 章提供一个进入系统的重要方法，因为越来越多的机构采用分布式和在家办公的模式，这种模式依赖于远程访问通信，而这种通信很容易受到攻击。

第 11 章主要讨论针对终端用户系统上应用的攻击，因为这些应用不会频繁地为终端用户的系统提供与企业的私人网络相同程度的保护。

附录概述安装 Kali Linux 的主要步骤，以及怎样采用全盘加密来避免机密测试数据的拦截。

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 XP 的。虽然它在 2014 年 4 月已被弃用，但是该系统为许多工具提供了一个行为标准的“基线”。如果你知道怎样将一个方法应用到一个操作系统，那么你可以将它应用到更多现有的操作系统，例如 Windows 7 和 Windows 8。

本书的读者对象

本书适用于想要学习更多关于数据安全知识的人。特别是，它的目标人群是那些在实践中明白为什么要使用一个特定工具的人；而不是相反的一些人（为了查看一个系统是否有漏洞，他们使用尽可能多的工具）。我的目标是使读者开发他们自己的方法和方式来进行有效的渗透测试，这可以让他们试验和学习，使他们进步。我相信这种方法是理解黑客怎样攻击数据系统的唯一有效的方式；自然，这也是了解怎样在漏洞被利用之前弥补漏洞的唯一方法。

如果你是一名专业的安全人员、渗透测试人员，或者是对复杂数据环境的安全感兴趣的人，那么这本书是为你准备的。

Contents 目　录

推荐序
作者简介
审校者简介
前言

第一部分　攻击者杀链

第1章　走进Kali Linux ····· 2
1.1　Kali Linux ····· 2
1.2　配置网络服务和安全通信 ····· 4
1.2.1　调整网络代理设置 ····· 5
1.2.2　使用安全 Shell 保护通信安全 ··· 6
1.3　更新 Kali Linux ····· 7
1.4　配置和自定义 Kali Linux ····· 9
1.4.1　重置超级用户密码 ····· 9
1.4.2　添加普通用户 ····· 10
1.4.3　加速 Kali 运行 ····· 10
1.4.4　与 Microsoft Windows 共享文件夹 ····· 11
1.4.5　用 TrueCrypt 创建加密文件夹 ····· 13
1.5　第三方应用程序的管理 ····· 17
1.5.1　安装第三方应用程序 ····· 17
1.5.2　作为普通用户运行第三方应用程序 ····· 18
1.6　渗透测试的有效管理 ····· 19
1.7　总结 ····· 21

第2章　确定目标——被动侦察 ····· 22
2.1　侦察的基本原则 ····· 22
2.2　开源情报 ····· 23
2.3　DNS 侦察和路由映射 ····· 25
2.3.1　WHOIS ····· 25
2.3.2　DNS 侦察 ····· 26
2.3.3　映射路由到目标 ····· 29
2.4　获得用户信息 ····· 31
2.4.1　收集姓名和电子邮件地址 ····· 31
2.4.2　收集文件元数据 ····· 32
2.5　分析用户密码列表 ····· 34
2.6　小结 ····· 35

第3章　主动侦察和漏洞扫描 ····· 36
3.1　隐形扫描策略 ····· 37

3.1.1 调整源 IP 栈和工具识别设置……37
3.1.2 修改数据包参数……38
3.1.3 使用匿名网络代理（Tor 和 Privoxy）……39
3.2 识别网络基础设施……42
3.3 枚举主机……43
3.4 端口、操作系统和发现服务……44
3.4.1 端口扫描……44
3.4.2 指纹识别操作系统……45
3.4.3 确定主动服务……46
3.5 采用综合侦察应用……47
3.5.1 nmap……47
3.5.2 recon-ng 框架……49
3.5.3 Maltego……51
3.6 漏洞扫描……52
3.7 小结……53

第4章 漏洞利用……54

4.1 威胁建模……55
4.2 使用在线和本地漏洞资源……56
4.2.1 Metasploit 框架……59
4.2.2 利用易受攻击的应用程序……63
4.3 使用 Armitage 的多目标渗透……64
4.3.1 Armitage 测试团队……66
4.3.2 Armitage 攻击脚本……66
4.4 绕过 IDS 与反病毒侦测……67
4.5 小结……73

第5章 后期利用——行动的目的……74

5.1 绕过 Windows 用户账户控制……75
5.2 对已入侵的系统进行快速侦察……77
5.3 找到并提取敏感数据——掠夺目标……80
5.4 创建附加账户……83
5.5 使用 Metasploit 工具进行后期渗透活动……84
5.6 在已入侵主机上提升用户权限……87
5.7 使用 incognito 重放身份验证令牌……88
5.7.1 使用 Windows 凭据编辑器操作访问凭据……89
5.7.2 从管理员升级到系统管理员…90
5.8 访问新账户实现横向升级……90
5.9 消除痕迹……91
5.10 小结……93

第6章 后期利用——持久性……94

6.1 破解现有的系统和应用程序文件进行远程访问……95
6.1.1 启用远程服务……95
6.1.2 启用远程 Windows 终端服务…96
6.1.3 启用远程虚拟网络计算……97
6.2 使用持久代理……98
6.3 使用 Metasploit 框架保持持久性……101
6.3.1 使用 metsvc 脚本……101
6.3.2 使用 persistence 脚本……103
6.4 使用 Metasploit 框架创建一个独立持久代理……104
6.5 重定向端口来绕过网络控制……106
6.5.1 示例 1——简单端口重定向…106