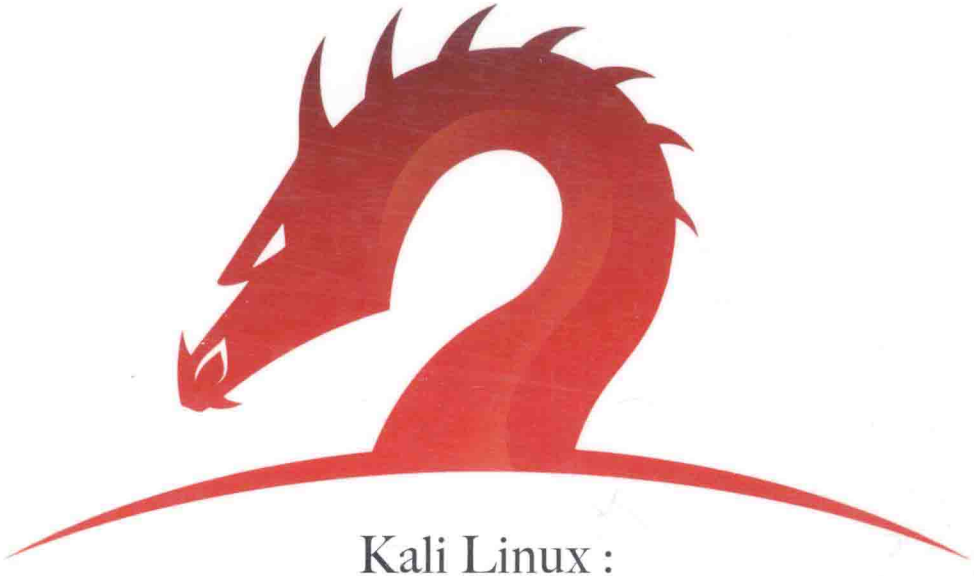
信息安全技术丛书

The quieter you become,
the more you are able to hear.

PACKT PUBLISHING



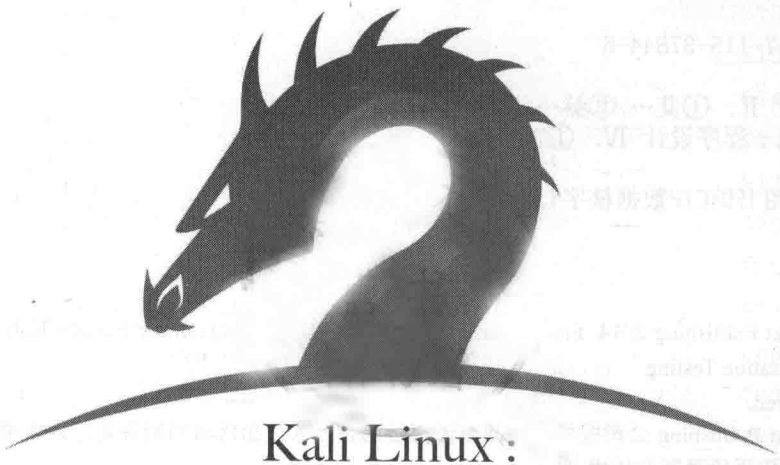
Kali Linux :
Assuring Security By Penetration Testing

Kali Linux
渗透测试的艺术

[英] Lee Allen
[印尼] Tedi Heriyanto 著
[英] Shakeel Ali
Archer 译

人民邮电出版社
POSTS & TELECOM PRESS

信息安全技术丛书



Kali Linux :
Assuring Security By Penetration Testing

Kali Linux
渗透测试的艺术

[英] Lee Allen
[印尼] Tedi Heriyanto 著
[英] Shakeel Ali
Archer 译

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

Kali Linux渗透测试的艺术 / （英）艾伦（Allen,L.），（印尼）赫里扬托（Heriyanto,T.），（英）阿里（Ali,S.）著 ；阿彻译. -- 北京 ：人民邮电出版社，2015.2
ISBN 978-7-115-37844-6

Ⅰ. ①K… Ⅱ. ①艾… ②赫… ③阿… ④阿… Ⅲ. ①Linux操作系统一程序设计 Ⅳ. ①TP316.89

中国版本图书馆CIP数据核字(2015)第005396号

◆ 著 [英] Lee Allen [印尼] Tedi Heriyanto
[英] Shakeel Ali
译 Archer
责任编辑 傅道坤
责任印制 张佳莹 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
北京艺辉印刷有限公司印刷
◆ 开本：800×1000 1/16
印张：24.75
字数：505 千字 2015 年 2 月第 1 版
印数：1-3 000 册 2015 年 2 月北京第 1 次印刷

著作权合同登记号 图字：01-2014-5790 号

定价：69.00 元

读者服务热线：(010)81055410 印装质量热线：(010)81055316
反盗版热线：(010)81055315

内容提要

Kali Linux 是一个渗透测试兼安全审计平台，集成了多款漏洞检测、目标识别和漏洞利用工具，在信息安全业界有着广泛的用途。

本书从业务角度出发，通过真实攻击案例并辅之以各种实用的黑客工具，探讨了进行渗透测试所需的各种准备工序和操作流程。本书共分为 12 章，其内容涵盖了 Kali Linux 的使用、渗透测试方法论、收集评估项目需求的标准流程、信息收集阶段的工作流程、在目标环境中探测终端设备的方法、服务枚举及用途、漏洞映射、社会工程学、漏洞利用、提升权限、操作系统后门和 Web 后文的相关技术、渗透测试文档报告的撰写等。

本书适合讲解步骤清晰易懂、示例丰富，无论是经验丰富的渗透测试老手，还是刚入门的新手，都会在本书中找到需要的知识。

关于作者

Lee Allen 是在顶尖大学里任职的安全架构师。多年以来，他持续关注信息安全行业和安全界内的新近发展。他有 15 年以上的 IT 行业经验，并且持有 OSWP 等多项业内的资格认证。

Lee Allen 还是 *Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide*（由 Packt Publishing 出版，人民邮电出版社出版了其中文版）一书的作者。

在此向我的爱人 Kellie 和我们的孩子表示感谢；他们为了本书的创作对我多有照顾。同时，我要向祖父母 Raymond 和 Ruth Johnson，以及岳父母 George 和 Helen Slocum 表示谢意；感谢他们这些年对我的支持和鼓励。

Tedi Heriyanto 是印尼一家信息安全公司的首席顾问。他一直在与（印尼）国内外的多家知名机构进行信息安全渗透测试方面的合作。他擅长设计安全网络架构、部署与管理企业级的信息安全系统、规范信息安全制度和流程、执行信息安全审计和评估，以及提供信息安全意识培训。在闲暇之余，他在印尼安全界的各种活动中不停地研究和学习。他还通过写作各种安全图书与大家分享界内知识。有兴趣的读者可以访问他的博客 `http://theriyanto.wordpress.com`。

感谢我的家人，谢谢他们在本书创作过程中给我的支持。感谢我的老板，谢谢他在本书的创作过程中给予我的信任、帮助和支持。感谢各位同事和客户，你们是我的良师益友。此外，感谢为本书提供宝贵意见和建议的 Packt Publishing 的各位同仁——Rubal Kaur、SwenySukumaran、Joel Goveya、Usha Iyer 和 Abhijit Suvarna。与此同时，感谢为本书投入大量时间和精力并分享了个人经验的技术审稿人 Alex Gkiouros 和 Neil Jones。最后要感谢本书的另外两名作者——Lee Allen 和 Shakeel Ali，他们通过这本书分享了各自的技术知识、热情、想法、挑战和建议，使我陶醉于这本书的创作过程。

最终要感谢的是您——本书的读者，感谢您购买了此书，希望您能喜欢它。祝您在信息安全的工作中一帆风顺。

Shakeel Ali 在世界 500 强公司里担任安全和风险管理顾问。在此之前，他是英国 Cipher Storm Ltd.的核心创始人。他从事过安全评估、系统审计、合规部门顾问、IT 管理和法证调查工作，积累了信息安全领域的各种知识。他还是 CSS Providers SAL 的首席安全员。他以废寝忘食的工作态度，为全球各类商业公司、教育机构和政府部门提供了不间断的安全支持服务。作为一名活跃的业内独立研究人员，他发表了大量的文章和白皮书。有兴趣的读者可以访问他的个人博客 `Ethical-Hacker.net`。此外，他还长期参与墨西哥举办的 BugCon Security Conferences 活动，定期报告最前沿的网络安全威胁，并分享相应的应对方案。

我向参与本书创作的各位朋友、审稿人和同事表示感谢。特别感谢 Packt Publishing 的团队和它们的技术编辑、审稿人，他们分享了无价的意见和建议，是这本书的幕后英雄。在此感谢本书的其他两位作者 Lee Allen 和 Tedi Heriyanto，本书的成功离不开他们不断的奉献、贡献、理念和技术讨论。最后，感谢我迄今为止遇到的各位搭档。他们总是能够在毫不松懈的安防工作中迸发出各种灵感。我相信，没有诸位的共同努力就没有安全稳定的信息安全环境。

关于审稿人

Alex Gkiouros 当前是一名独立的 IT 专业人士，参与过希腊的各种项目。他在 2006 年步入 IT 行业，已经持有 2 个 ISACA 的资格认证，目前在学习 CCNP。他热爱网络安全，并花费大量时间研究 Kali Linux 或 Backtrack。有兴趣的读者可以访问他的个人博客 `http://www.voovode.net/`。

Neil Jones 在一家总部在英国的全球安全公司任职安全顾问。他过去就希望在年轻的时候就进入安全行业，如今他不仅达成这一心愿，而且获取了业内认可的多项资格认证。

他是一名不折不扣的安全研究人员。他从吃饭、睡觉，甚至在呼吸之间都挤出时间进行研究，还为业内开发过多款开放源代码的安全工具。

前言

Kali Linux 是一个渗透测试平台兼安全审计平台，它集成了多款漏洞检测、目标识别和漏洞利用工具。在明确业务目标的情况下，测试人员采取适当的渗透测试方法论，结合详细的测试计划即可进行富有成效的渗透测试。

本书循序渐进地演示了多款尖端的黑客工具，连贯地介绍了各种实用的黑客技术，是一本系统化地讲解渗透测试技巧的图书。它从业务的角度出发，以时下数字时代的真实攻击案例入手，探讨了所需的各种必要的准备工序和测试流程。

本书揭示了渗透测试的最优逻辑思路和业内最佳的测试方法。

本书最先讲解了实验室的制备方法，依次说明了基本的安装和配置方法，讨论了渗透测试的不同类型，介绍了开放的安全测试方法，并提出了 Kali Linux 特有的测试过程。在此之后，本书将遵循正式的测试方法论，依据渗透测试各个阶段（范围界定、信息收集、目标发现、服务枚举、漏洞映射、社会工程学、提升权限、访问维护和文档报告）的需要介绍相应的测试工具。我们会通过真实的渗透案例来演示这些工具的使用和配置方法。本书最后一部分还简要介绍了额外的渗透工具以及渗透测试人员通常会参考的重要资源。

本书从零起步介绍了渗透测试的必备技能，可作为读者专业且实用的专家指导。在学习本书的内容之后，读者可以在现实环境中或者在实验测试平台中使用 Kali Linux 进行渗透测试。

本书内容

第 1 章，Kali Linux 入门。简要介绍 Kali Linux 的 Live DVD 的使用方法。本章首先介绍 Kali Linux 的研发简史和各类工具，然后介绍获取、使用、配置、更新 Kali Linux 的方法，以及多个重要网络服务（HTTP、MySQL、SSH）的配置方法。最后，本章还演示了使用镜像文件安装并配置一台漏洞百出的问题虚拟机，以及安装额外工具包的方法。

第 2 章，渗透测试方法论。探讨了标准渗透测试的基本概念、规则、管理、方法和流程。本章将介绍两种著名的类型渗透测试，即黑盒测试和白盒测试之间的明显区别。另外，它还分析了脆弱性评估和渗透测试之间的区别。本章重点讲解了各种渗透测试方法论的业务特性、功能和优点，分别讨论了 OSSTMM、ISSAF、OWASP 和 WASC-TC。最后，介绍了由 10 个连贯的测试阶段组成的 Kali Linux 的通用渗透测试流程。

第 3 章，范围界定。阐述收集评估项目需求的标准流程。本章将阐述制定渗透测试项目工作路线图所需的各个要素。这个阶段的工作可分为多个关键步骤，即收集需求、筹划工作、边界分析、明确业务指标、项目管理和统筹调度。本章讲解获取测试环境具体信息的方法。

第 4 章，信息收集。介绍信息收集阶段的工作流程。本章首先演示了通过公共资源获取目标环境有关信息的方法，然后介绍了分析 DNS 信息和收集网络路由信息的手段，最后讲解了利用搜索引擎获取目标域名、E-mail 地址和文件元数据的技术。

第 5 章，目标识别。讲解了在被测环境中探索终端设备的方法。本章介绍了目标识别阶段的任务以及相应的工具，以及对目标主机进行操作系统指纹识别的各种工具。

第 6 章，服务枚举。探讨了服务枚举及其用途。本章介绍了端口扫描的概念和相关工具。本章重点介绍 Nmap 的各种可用选项，以及在被测网络中搜索 SMB、SNMP 和 VPN 服务的各种工具。

第 7 章，漏洞映射。讨论了漏洞的两种类型：本地漏洞和远程漏洞。您将在本章了解漏洞区分依据和分类方法，及各种行业标准。此外，本章讲解了 OpenVAS、Cisco、Fuzzing、SMB、SNMP 和 Web 应用程序分析工具，这些工具可以用来查找、分析目标网络种存在的安全漏洞。

第 8 章，社会工程学攻击。介绍了社会工程学专业人员操纵他人，使后者泄露信息或进行某种行为的核心原则和业内认可的做法。本章将阐述社工涉及的基本心理学原理。社会工程学专业人士制定的社工目标和具体方法都是基于这些心理学原理。本章还通过实际案例讲解了社工的攻击流程和攻击方法。本章最后介绍了 Kali Linux 的社会工程学工具集，并演示了利用这些工具攻击人力资源部门的社工方法。

第 9 章，漏洞利用。重点介绍了可切实利用漏洞的实践方法和各种工具。本章讲解了漏洞研究领域的各个方面，以及理解、检验和测试目标环境脆弱性的关键手段。本章还列举了一些知名的漏洞资料库和使用方法。同时，本章还从安全评估的角度讲解了恶名昭彰的开发工具包，并演示了使用 Metasploit 的 exploit 模块编写简单的漏洞利用程序的方法。

第 10 章，提升权限。介绍了提升权限、网络监听及网络欺骗的概念。本章不仅介绍了

通过本地漏洞提升权限的方法，而且介绍了分别以离线和在线的方式碰撞用户密码的工具。本章最后还讲解了可用于网络欺骗和网络监听的多款工具。

第 11 章，访问维护。演示了操作系统后门和 Web 后门的有关技术。本章介绍了各种不同的后门及其使用方法。此外，本章还讲解了多款网络隧道工具，这些工具可以在攻击者和受害者之间建立秘密通信。

第 12 章，文档报告。涵盖了渗透测试文档、汇报文件和现场演示的有关内容。本章内容旨在指导读者以撰写系统化的、结构化的、一致的工程文档。此外，本章还介绍了验证测试结果、报告的不同种类、现场演示及测试的后期流程工作。

附录 A，辅助工具。介绍了渗透测试工作可能会用到的几款额外工具。

附录 B，关键资源。列举了多个可帮助您提高渗透测试技术的参考资源。

阅读群体

本书适合大体了解 UNIX/Linux 操作系统，并了解信息安全各项构成因素的 IT 安全专业人士或网络管理员，以及想要使用 Kali Linux 进行渗透测试的读者。

目录

第 1 部分　系统的搭建与测试

第3部分 额外资源