Packt>

Kali Linux 无线渗透测试指南

（第3版）

Kali Linux Wireless Penetration Testing
Beginner's Guide
Third Edition

[英] 卡梅伦·布坎南（Cameron Buchanan）
[印度] 维韦克·拉玛钱德朗（Vivek Ramachandran）著
孙余强　王涛　译

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

Kali Linux 无线渗透测试指南

（第3版）

Kali Linux Wireless Penetration Testing
Beginner's Guide
Third Edition

[英] 卡梅伦·布坎南（Cameron Buchanan）
[印度] 维韦克·拉玛钱德朗（Vivek Ramachandran） 著
孙余强 王涛 译

人民邮电出版社
北京

图书在版编目（CIP）数据

Kali Linux无线渗透测试指南 : 第3版 / (英) 卡梅伦·布坎南 (Cameron Buchanan) , (印) 维韦克·拉玛钱德朗 (Vivek Ramachandran) 著 ; 孙余强, 王涛译
. -- 北京 : 人民邮电出版社, 2018.7
ISBN 978-7-115-48368-3

Ⅰ. ①K… Ⅱ. ①卡… ②维… ③孙… ④王… Ⅲ. ①Linux操作系统－指南 Ⅳ. ①TP316.85-62

中国版本图书馆CIP数据核字(2018)第095003号

版权声明

◆ 著　[英]卡梅伦·布坎南（Cameron Buchanan）
[印度]维韦克·拉玛钱德朗（Vivek Ramachandran）
译　孙余强　王　涛
责任编辑　傅道坤
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
三河市潮河印业有限公司印刷

◆ 开本：800×1000　1/16
印张：12.25
字数：165 千字　2018 年 7 月第 1 版
印数：1－2 400 册　2018 年 7 月河北第 1 次印刷

著作权合同登记号　图字：01-2018-2762 号

定价：49.00 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

内容提要

本书是无线领域渗透测试的入门指南，针对 Kali Linux 2017.3 版本进行了全面更新，旨在帮助读者认识与无线网络有关的各种安全漏洞，以及如何通过渗透测试来发现并堵住这些漏洞。

本书共分为 11 章，内容包括如何利用现成的硬件和开源软件搭建无线网络测试环境、WLAN 及其固有的安全隐患、规避 WLAN 验证的方法、认识 WLAN 加密的缺陷、如何利用这些缺陷搞定 WLAN 加密、如何对 WLAN 基础设施进行渗透测试，以及如何发动各种无线客户端攻击来破坏网络安全。此外，还介绍了当今最前沿的无线攻击手段、KRACK 攻击的新方法、攻击 WPA-Enterprise 和 RADIUS、WLAN 渗透测试的原理，以及 WPS 暴力攻击和探测嗅探攻击。

本书适合对无线渗透测试感兴趣，且具备无线网络基础知识的读者阅读。

关于作者

Cameron Buchanan 是一位渗透测试从业人员兼业余作家，为世界各地各行各业的许多客户进行过渗透测试工作。之前，Cameron 曾是英国皇家空军（RAF）的一员。在闲暇之余，他喜欢干一些“蠢事”，比如，试图让某些东西飞起来、触电，以及在冰水里泡澡。他已婚，居于伦敦。

Vivek Ramachandran 自 2003 年以来，一直从事 WiFi 安全相关的工作。他发现了 Caffe Latte 攻击，破解了 WEP Cloaking（一种 WEP 保护方案），并于 2007 年公开发布在 DEF CON 上。2011 年，他又首次演示了如何使用恶意软件通过 WiFi 来创建后门程序、蠕虫病毒甚至是僵尸网络。

之前，Vivek 效力于 Cisco 公司，任 6500 Catalyst 系列交换机 802.1x 协议和端口安全特性的程序员一职，他还是在印度举办的微软安全大赛（Microsoft Security Shootout）的获奖者之一。他作为 SecurityTube.net 的创始人，在黑客社区声名显赫，并经常发布各种与 WiFi 安全、汇编语言、攻击技巧有关的视频。SecurityTube.net 每个月的独立用户访问量都能突破 10 万。

Vivek 在无线安全方面的成就得到了多家媒体（BBC Online、InfoWorld、MacWorld、The Register 和 IT World Canada 等）的报道。今年，他将在多场安全会议（Blackhat、DEF CON、Hacktivity、44con、HITB-ML、BruCON Derbycon、Hashdays、SecurityZone 和 SecurityByte 等）上发言并进行培训工作。

关于审稿人

Daniel W. Dieterle 是一名蜚声国际的安全作家、研究人员和技术编辑。他拥有 20 年以上的 IT 从业经验，为数百家大大小小的公司或企业提供过各种各样的安全支持和服务。Daniel 负责 Cyber Arms 安全博客的运行并积极发帖，同时还参与物联网项目。

前言

当今世界，无线网络无处不在。全球每天都有无数人在家、在办公室或通过公共热点（public hotspot）用无线网络登录 Internet，处理公、私事宜。无线网络虽然让生活变得更加轻松写意，赋予人们极高的机动性，但同时也带来了风险。近来，时常有人钻不安全的无线网络的空子入侵公司、银行以及政府机构。此类攻击的频率还在不断加剧，因为很多网络管理员都不懂如何以健壮而又万无一失的方法加固无线网络。

本书旨在帮助读者认识与无线网络有关的各种安全漏洞，以及如何通过渗透测试来发现并封堵这些漏洞。对于那些希望在无线网络安全审计方面有所作为，同时需要得到一步步实践指导的读者而言，本书属于必读书籍。本书会先解释每一种无线攻击手法，然后再用实例加以演示，通读本书，读者的所学必将圆满。

本书选用 Kali Linux 为平台来演示本书所有的无线攻击场景。正如读者所知，Kali Linux 是世上最受欢迎的渗透测试 Linux 发行版。它集成了数百种安全及黑客工具，本书会用到其中的某些工具。

本书的内容

第 1 章，“搭建无线实验环境”，教读者如何使用现成的硬件和开源软件，搭建无线网络测试实验环境。为了试水本书记载的几十个实验场景，需要先搭建好一个无线网络实验环境。本章首先列出了硬件需求，包括无线网卡、

天线、接入点（AP）以及其他支持 WiFi 功能的设备。然后，将重点转移到软件需求上，包括操作系统、WiFi 驱动程序以及相关的安全工具。最后，会介绍如何针对书中的实验搭建测试无线网络平台，以及如何借助该平台来验证各种无线配置。

第 2 章，“WLAN 及其固有的隐患”，会重点讨论无线网络固有的设计缺陷，这样的无线网络一般都是由开箱即用的不安全网络设备搭建而成的。本章将首先借助于一款名为 Wireshark 的网络分析软件，引领读者简要回顾一下各种 802.11 WLAN 协议。这会让读者对这些协议的运作方式有一个实际的了解。最重要的是，一旦认识了管理、控制以及数据帧，理解无线客户端和 AP 在数据包层面上的通信方式自然也不在话下。然后，会教读者如何在无线网络中注入以及从中捕获数据包，同时会介绍一些执行相关任务的工具。

第 3 章，“规避 WLAN 验证”，揭示了破坏 WLAN 验证机制之法！本章会详细探讨攻陷开放验证和共享密钥验证的方法。在做相关实验的过程中，读者能学习到如何分析无线数据包，并借此弄清无线网络的身份验证机制。本章还会讲解如何攻陷隐藏了 SSID 以及开启 MAC 过滤功能的无线网络。隐藏 SSID 及开启 MAC 过滤这两种手段可使无线网络更为隐蔽，难以渗透，网管人员也经常使用，但规避起来也很容易。

第 4 章，“WLAN 加密漏洞”，描述了 WLAN 协议中最脆弱的一环，即加密方法——WEP、WPA 和 WPA2。在过去十多年里，黑客们在这些加密方法中发现了多处缺陷，编写了多款可公开获取的软件来破解这些方法及解密数据。而且，即便 WPA/WPA2 在设计上非常安全，但配置错误也会导致安全漏洞，使其被轻易攻陷。本章可让读者认识每种加密方法的安全隐患，会通过某些实操来演示如何攻陷这些加密方法。

第 5 章，“攻击 WLAN 基础设施”，重点关注 WLAN 基础设施的漏洞。本章探讨由配置和设计问题而引发的漏洞，还会以实操的方式来演示攻击，涉及 AP MAC 欺骗攻击、evil twin 攻击、无赖 AP 攻击以及拒绝服务攻击。本章将帮助读者深入了解如何对 WLAN 基础设施进行渗透测试。

第 6 章，“攻击无线客户端”，要是读者始终认为不必劳神无线客户端的安全性，那么本章将会让你大跌眼镜！大多数人在思考 WLAN 的安全性时，总会忽视无线客户端。本章无疑将会证明为什么在针对 WLAN 网络进行渗透测试时，无线客户端与 AP 是同等重要的。本章将研究如何发动各种无线客户端攻击（比如，蜜罐和误关联攻击、Caffe Latte 攻击、解除验证和取消关联攻击、Hirte 攻击、只用无线客户端的 WPA 个人口令破解攻击）来破坏 WLAN 网络安全。

第 7 章，“高级 WLAN 攻击”，着眼于更高级的攻击手段，本书至此已经涵盖了大多数针对无线基础设施和客户端的基本攻击手段。高级攻击通常涉及结合使用多种基本攻击手段，在更高难度的情况下破坏 WLAN 的安全性。这些高级攻击手段包括无线中间人攻击、逃避无线入侵检测和防御系统，以及部署启用自定义协议的无赖 AP。本章会介绍现实世界中最前沿的无线攻击手段。

第 8 章，“KRACK 攻击”，探讨了 2017 年最新发现的有关 WPA2 握手的漏洞。通读本章，读者将会详细了解 WPA2 握手的最新知识，以及如何发动这些新的攻击。

第 9 章，“攻击 WPA-Enterprise 和 RADIUS”，通过介绍针对 WPA-Enterprise 和 RADIUS 服务器架设的高级攻击手段，来提升读者的水平。当读者在对依赖 WPA-Enterprise 和 RADIUS 身份验证的大型企业网络进行渗透测试，来提高其安全性时，这些攻击手段将会派上用场。

第 10 章，“WLAN 渗透测试之道”，是对前几章所有学习内容的总结，会以抽丝剥茧般的方式来探讨如何进行无线渗透测试。本章将介绍渗透测试的各个阶段——规划（Planning）、发现（Discovery）、攻击（Attack）和报告（Reporting），以及如何将每个阶段应用于无线渗透测试。读者还将了解到在执行过无线渗透测试之后，如何提出安全建议和最佳做法。

第 11 章，“WPS 和探测”，介绍了自本书第 1 版发行以来在业界发展很快的

两种新型攻击手段——WPS 暴力攻击（WPS brute-force）和以监控为目的的探测嗅探攻击（probe sniffing for monitoring）。

本书的阅读准备

要想弄清并再现本书记载的各种实操场景，读者需要准备好两台配有内置 WiFi 网卡的笔记本电脑、一块 USB 无线 WiFi 适配器、Kali Linux 系统以及某些其他的软硬件，详情请见第 1 章。

当然，也可以在一台安装了 Windows OS 的笔记本上创建一台容纳 Kali Linux 的虚拟机，用 USB 接口将 WiFi 网卡配备给该虚拟机。如此一来，就不再需要两台笔记本电脑了。这可以让读者更快地使用本书来学习，但强烈建议使用运行 Kali Linux 的专用电脑来完成实操场景。

读者应具备无线网络的基础知识，包括对事关 802.11 协议和无线客户端/AP 通信的基本认知，这也是阅读本书的前提条件。哪怕读者已经掌握了上述概念，本书在搭建实验环境的内容里，还是会简单介绍一些这方面的内容。

本书的读者对象

本书适合各种水平的读者阅读，无论读者是业余水平还是无线网络安全专家，都能从本书受益。本书从最简单的攻击开始讲解，然后会解释较为复杂的攻击，最后还会探讨最前沿的攻击和研究成果。由于本书通过实操来解释所有攻击，所以无论读者是何等水平，都能很容易地掌握如何独自发动攻击。请注意，本书虽然着重介绍如何针对无线网络发动各种攻击，但真正的意图是引领读者成为无线网络渗透测试人员。身为一名称职的渗透测试人员，不但要能理解本书提及的所有攻击，而且如果客户提出请求，还能轻松地加以演示。

免责申明

本书只做教学之用，旨在帮助读者测试自用系统，以应对信息安全威胁，并保护自用 IT 基础设施免受类似攻击。对本书所授内容的不当使用所导致的一切后果，人民邮电出版社、Packt 出版社及作译者不承担任何责任。

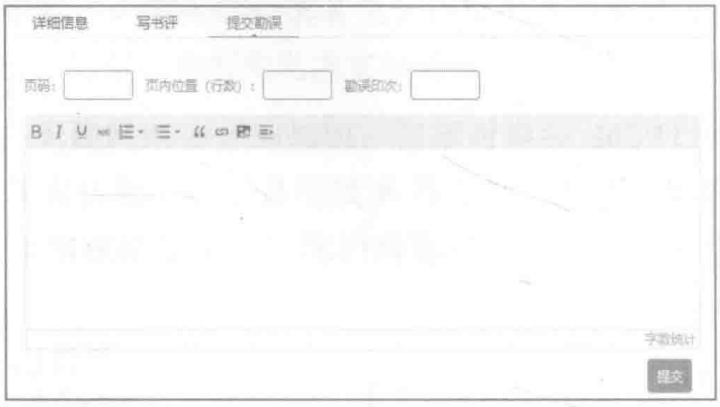
资源与支持

本书由异步社区出品，社区（https://www.epubit.com/）为您提供相关资源和后续服务。

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，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，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，按书名搜索，进入本书页面，点击“提交勘误”，输入勘误信息，点击“提交”按钮即可。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。积分可用于在异步社区兑换优惠券、样书或奖品。



扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。

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，请您发邮件给我们，并请在邮件标题中注明本书书名，

以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线提交投稿（直接访问 www.epubit.com/selfpublish/submission 即可）。

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，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部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。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

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。异步社区创办于 2015 年 8 月，提供大量精品 IT 技术图书和电子书，以及高品质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 专业图书的品牌，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，相关图书在封面上印有异步图书的 LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

异步社区

微信服务号

目录