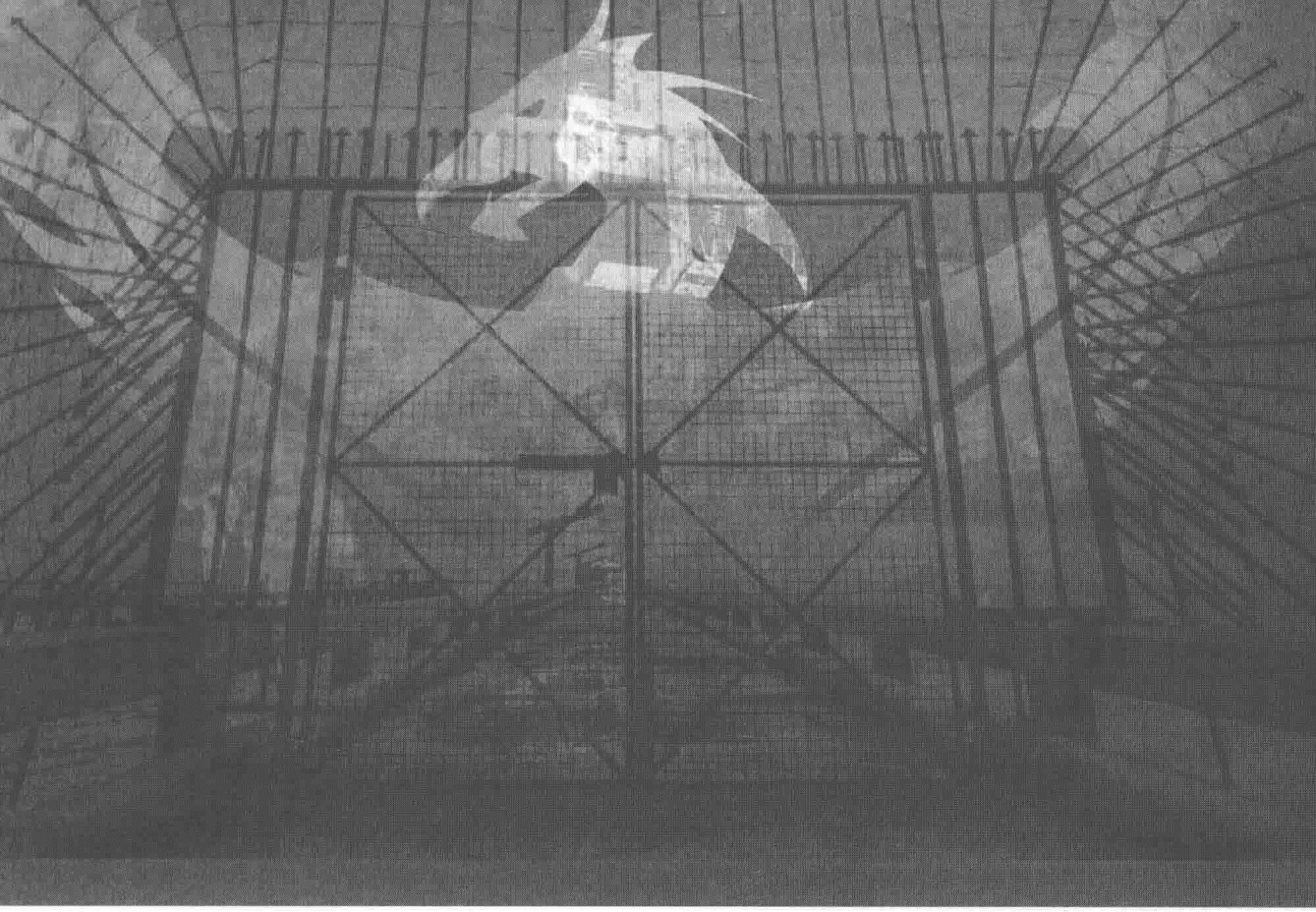
树莓派渗透测试实战

Penetration Testing with Raspberry Pi

[美] Joseph Muniz　Aamir Lakhani　著
朱筱丹　译

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



树莓派渗透测试实战

[美] Joseph Muniz　Aamir Lakhani　著
朱筱丹　译

人 民 邮 电 出 版 社
北　京

图书在版编目（CIP）数据

树莓派渗透测试实战 /（美）约瑟夫·穆尼斯（Joseph Muniz），（美）阿米尔·拉克哈尼（Aamir Lakhani）著；朱筱丹译. -- 北京：人民邮电出版社，2017.5
ISBN 978-7-115-44907-8

Ⅰ. ①树… Ⅱ. ①约… ②阿… ③朱… Ⅲ. ①软件工具－程序设计 Ⅳ. ①TP311.561

中国版本图书馆CIP数据核字(2017)第044951号

版权声明

◆ 著　[美] Joseph Muniz　Aamir Lakhani
译　朱筱丹
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
三河市海波印务有限公司印刷

◆ 开本：800×1000　1/16
印张：12.25
字数：166 千字　2017 年 5 月第 1 版
印数：1－2 000 册　2017 年 5 月河北第 1 次印刷

著作权合同登记号　图字：01-2016-3940 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：京东工商广字第 8052 号

内容提要

本书讲解了使用便携廉价的树莓派搭配 Kali Linux 进行渗透测试的方法。

本书分为 6 章，介绍了树莓派和 Kali Linux 的基础知识、适用于树莓派的 Kali Linux ARM 版本的基本知识和环境优化、渗透测试相关的知识、树莓派的各种攻击手段、渗透测试后的工作，以及与树莓派相关的其他项目。

本书内容组织有序，通过步骤式讲解来凸显实用性和实操性，适合信息安全从业人员阅读。

关于作者

Aamir Lakhani是一位著名的网络安全架构师、高级策略师兼研究员，负责为重要的商业和联邦企业部门提供IT安全解决方案。Lakhani曾经作为项目负责人，先后为世界500强公司、政府部门、重要的医疗服务提供商、教育机构、金融和媒体公司实施了安全策略。Lakhani曾经设计过以进攻为主的防御措施，并协助多家公司防御由地下安全组织发起的主动攻击。Lakhani被认为是行业领导者，他在网络防御、移动应用威胁、恶意软件、高级持续性威胁（APT）研究、暗安全（Dark Security）等主题领域提供了详细的架构约定（architectural engagements）和项目。Kakhani还是多本图书的作者和特约作者，其中包括*Web Penetration Testing with Kali Linux*和*XenMobile MDM*（两者均为Packt Publishing出版）。他还曾作为网络安全专家在美国国家公共广播电台上露面。

Lakhani运营着DrChaos.com博客，该站点被FedTech Magazine评为网络安全技术的一个重要参考来源。他被评为社交媒体上最顶尖的人物之一，在他的技术领域享有盛名。他将继续致力于网络安全、研究和教育领域。

Joseph Muniz是思科公司的一名顾问，同时还是一位安全研究员。他的职业生涯始于软件开发，然后以外包技术人员的身份从事网络管理。Joseph后来进入咨询行业，而且在与许多不同的客户进行会谈时，发现自己对安全行业产生了激情。他曾经设计和实施过许多项目，其客户既有世界500强公司，也有大型的联邦网络。Joseph是多本图书的作者和特约作者，还是许多主流安全会议的发言人。通过访问他的博客www.thesecurityblogger.com可以看到最新的安全事件、研究和技术。

关于审稿人

Bill Van Besien 是一位软件工程师，其工作主要集中在航天器飞行软件架构、无人机自主软件，以及和空间任务操作相关的网络安全等领域。在过去几年，他一直从事软件开发，并服务于执行多个 NASA 太空任务的任务操作团队。他拥有计算机科学的学士和硕士学位，重点关注密码学和计算机安全。Bill 在约翰·霍普金斯大学应用物理实验室的航天器软件组工作，同时还在华盛顿哥伦比亚特区的一家太阳能初创公司 Nextility 任职。读者可通过 http://billvb.github.io 了解与他的项目相关的信息。

Bob Perciaccante 是思科公司的一名安全咨询系统工程师，在信息安全领域浸淫了 20 多年。他还在网络和系统漏洞评估、企业监控与响应，以及不同行业中的网络访问控制等领域有过从业经验。他当前关注的是能够有效解决动态安全需求的主动网络和系统安全架构。

Antonio Rodríguez 在很小的时候就进入信息安全领域，并学习编程、网络和电子相关的知识，后来毕业于计算机工程专业。

他有 20 多年的从业经验，专门从事注入恶意软件分析、软件逆向分析、机器学习等主题的研究，还主导了多个安全学科相关的学术研究。

他目前供职于西班牙国家网络安全研究所（INCIBE），在 CERT 团队担任资深 IT 安全研究员。

读者可以通过 http://twitter.com/moebiuz 关注他。

Kumar Sumeet 当前在英国伦敦大学霍洛威学院攻读信息安全专业的硕

士学位。他的研究兴趣是系统和软件安全、数字取证和安全测试。他在 2013 年从印度 DA-IICT 毕业，获得了 ICT（信息与通信技术）的学士学位。

在攻读学士学位期间，他还是 Nmap 项目的一名贡献人，而且在技术协会组织的讲座上担任发言人。2013 年大学毕业之后，他在印度的 TIFAC-DST 公司找了一份兼职工作，职位是网络安全研究助理。与此同时，他也从事信息安全方面的独立研究，发现了 Skype 和 Nimbuzz 中的一些漏洞，并且发表了一篇基于应用行为来分类加密流量的论文。

有关他的项目的最新消息，请访问 https://krsumeet.com。

Marius Voila 是一位具有 14 年经验的 Linux 系统管理员，在运维领域造诣颇深。他专门从事部署、云计算、负载均衡、规模扩展和性能调优，以及开发灾难恢复最佳实践等领域的工作，比如备份和恢复、防火墙和服务器安全审计。

前言

本书的主要内容是通过综合 Kali Linux 的强大威力和树莓派便携又廉价的特点，两者强强联手，在不需要大运算量的项目里，构造一套异常灵活的渗透测试平台。我们已经把这套软硬件组合运用于远程渗透和漏洞测试。由于树莓派非常便携，可以方便地在不同位置进行安全测试评估，还可以通过配置，既能远程控制树莓派，又不会留下什么痕迹。此外，树莓派不落痕迹的特点，加上其低功耗的特色，使得在搭配外置 USB 电源后，能在户外的环境里工作 1～2 天。对渗透测试人员来说，在树莓派平台上使用 Kali Linux 实现安全测试的目标，是一种独特又高性价比的选择。

本书内容安排

第 1 章，树莓派和 Kali Linux 基础知识：如何购买树莓派，安装 Kali Linux，最开始怎样登录 Kali Linux 和一些常见问题的解答。

第 2 章，树莓派预备步骤：初步介绍 Kali Linux ARM 版本操作系统，以及如何优化环境，使树莓派适用于本地和远程渗透测试。

第 3 章，渗透测试：目标是帮助读者理解网络扫描、无线破解、中间人攻击和突破加密通信等技术手段。

第 4 章，树莓派攻击：介绍利用树莓派上的工具和方法，怎样攻击测试的目标，手段包括攻击工具、社会工程学、钓鱼和恶意蜜罐。

第 5 章，结束渗透测试的工作：包括如何在报告里整理结果，如何在渗透测试后掩盖痕迹。

第 6 章，其他树莓派项目：介绍其他渗透测试工具集、防护工具和各种树莓派使用场景[①]。

阅读本书的先决条件

如果希望用树莓派作为安全评估的工具，请参见第 1 章关于购买树莓派和其他系统组件的详细信息，在后续章节中会用到。Kali Linux 和本书提到的其他软件应用都是开源的，可以免费下载。

本书读者对象

本书的主题是用最流行的开源渗透工具集 Kali Linux，把树莓派变成一套黑客适用的军火库。如果各位读者需要寻找一款价格低、体积小的黑客工具，可以从远程访问，本书的理念就非常适合你。如果作为渗透测试人员，希望削减出差成本，只要把这个低价的节点设备放到目标网络，然后通过本书的方法，就可以大大地节省成本。如果你是渗透测试领域里的新人，希望学习渗透经验又不希望花太多的钱在昂贵的硬件上，本书也会很有帮助。如果你恰好是一位树莓派玩家，但也对黑客技术感兴趣，本书就同时覆盖了这两方面的内容。本书的读者并不需要是有经验的黑客或程序员。当然如果有网络方面的经验会更好；但要学习本书的知识理念，并不强求具备网络知识。

① 译者注：此处原文为 use case，翻译成“用例”只是原来的约定俗成，并不利于理解。本书有无数的地方出现了 use case，译为“使用场景”均比“用例”更易懂，故修改。

目录

第 1 章
树莓派和 Kali Linux 基础知识

Kali Linux 的用户包括全球各地的安全专家、黑客们和研究者，是最受欢迎的渗透测试平台之一，主要用于安全和漏洞评估、攻击研究和风险测试。Kali Linux 包含众多流行的开源工具，适用于渗透测试的方方面面。Kali Linux 的前身是 BackTrack 5 R3，然后逐渐进化到一套完整的 Linux 桌面系统。

树莓派电脑以超低价著称，它使用 HDMI（高清晰度多媒体接口，High Definition Multimedia Interface）线与显示器相连，可以外接 USB 键盘和鼠标。许多计算机专家都记得以前的电脑并不是打开电源就立刻能用的，那时候的电脑往往还得先在机器上折腾一下才能运作。树莓派可以用于学习计算机体系和编程，而价钱却非常便宜。人们已经利用它的便携性和低价，搭建出各种学习设备、远程摄像头、安全系统、地震监测仪和诸多各类项目。

本章讲解了以下内容：

- 如何购买和组装树莓派；
- 安装 Kali Linux；
- 怎么把 Kali Linux 和树莓派结合起来；
- 克隆树莓派 SD 卡；
- 需要规避的常见问题。

1.1　购买树莓派

本书中，选择的是树莓派 Model B+型号。其他型号也都大同小异，当然，如果型号不同，可能需要自己微调某些配置。

图 1-1 中展示的就是树莓派 B+产品。

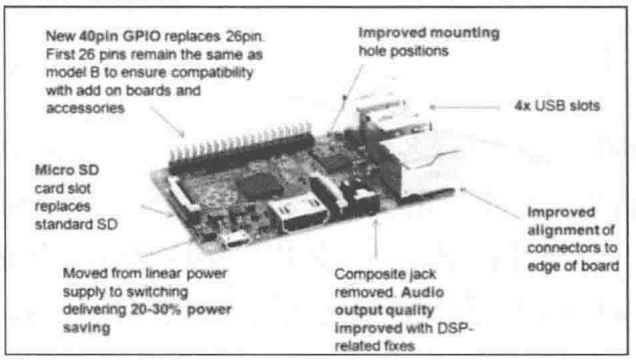


图 1-1

树莓派 B+型号和前代相比，有以下重要改进：

- 更多的 USB 接口；
- 更强的热插拔处理能力；
- 网卡配置了新的状态灯显示；
- 支持 40 针脚的 GPIP（General-Purpose Input/Output）接线头；
- 使用 microSD 卡而非完整尺寸的 SD 卡；
- 低能耗要求。

网上有一些现成的树莓派套装，如树莓派完备版套件（Ultimate Kit），在本书写作时，美国亚马逊网站上的价格为 79.99 美元。套装里包括一个树莓派 B+型号主机、外壳、电源适配器和一个 Wi-Fi 无线网卡。当然也可以只买一个基本的 B+主机而不买电源适配器、SD 卡等。如果只买主机本身，在

www.amazon.com 上只需要大概 40 美金。要完成某些任务，如网络监听，就需要用到第 2 块网卡了。而树莓派默认只有一个有线网卡。要实现这些目标，就要再花 11 美金买一个 USB 接口的有线网卡[①]。而且，大部分的套装也没有包括适用于电脑上 SD 卡槽的转接套[②]。例如，MacBook Pro 电脑上有 SD 卡接口，但还得配备一个 microSD 卡的转接套，才能对树莓派的 microSD 卡进行格式化，这个转接套的价钱大概在 10 美金左右。对无线渗透测试来说，还需要一个 USB 无线网卡，大概 10 美元可以买到。总的来说，大部分树莓派的组件都不算贵，所以整套系统的价格也就在 50～100 美元。

图 1-2 显示的是从盒子中取出来的树莓派主板。

图 1-3 所示为在 eBay 上销售的一款树莓派套装。

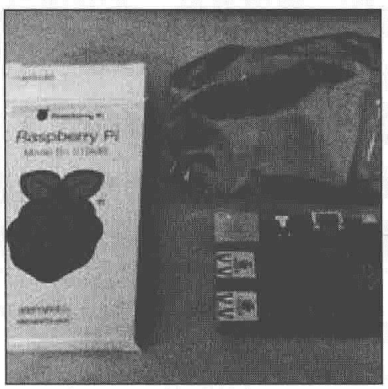


图 1-2

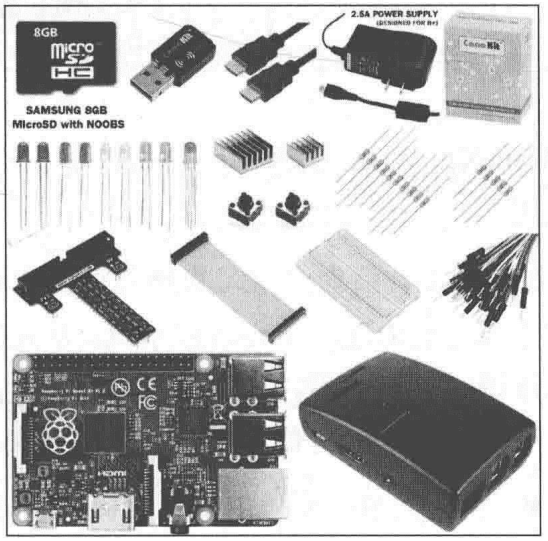


图 1-3

图 1-4 所示为一个 USB 有线网卡。

图 1-5 所示为 microSD 到 SD 卡的转接套。

① 译者注：原文直译是“以太网卡”，但改成有线网卡普通读者应该更容易理解。

② 译者注：这里“转接套”对应的英文是 adapter，adapter 这个单词指代非常含糊。在有把握的地方，酌情改成容易理解的称呼。

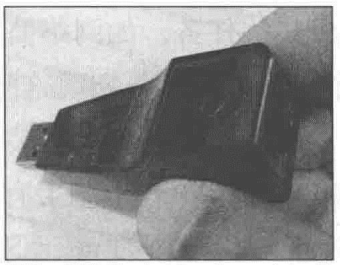


图 1-4

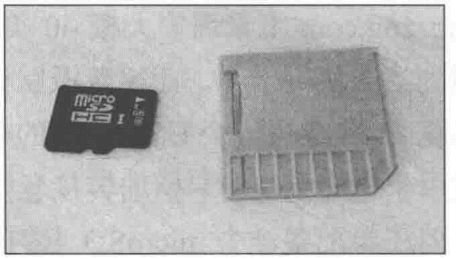


图 1-5

图 1-6 为 USB 接口的无线网卡。

图 1-6

CanaKit Wi-Fi 无线网卡体积较小，便携性佳，兼容性强，非常适合树莓派使用。

在本书中，我们会学习将树莓派作为远程渗透测试的探头[①]使用，并使用它的无线功能再连回中心管理系统。在逐渐熟悉了树莓派和 Kali Linux，以及其他渗透测试应用后，很可能就会用到上面提到的这些组件。以下是构造一套用于渗透测试的树莓派需要的清单列表：

- 树莓派 B+ 型号主机，大概 35～45 美元；
- USB 无线网卡，大概 10～20 美元；
- USB 有线网卡，大概 10～20 美元；
- SD 和 microSD 卡转换器，包括 microSD 卡，大概 10～20 美元；
- 电源适配器，大概 5～10 美元；

① 译者注：这里的原文是 agent，和前面的 adapter 一样，较为含糊，酌情叫“探头”。