Kali Linux

无线网络渗透测试详解

李亚伟　编著

基于世界知名的Kali Linux专业渗透测试环境，详细展现无线网络渗透测试的五大环节及各种核心技术，全面分析WiFi网络的四种加密模式的破解方式和防护措施

- 涉及经典无线网络加密模式WPS、WEP、WPA和WPA+Radius的分析和渗透
- 结合Wireshark等工具，讲解如何从WiFi网络中捕获并提取关键数据
- 遵循无线网络渗透测试的基本流程，详细讲解监听、捕获、分析和破解等各个环节
- 注重操作，避免纯理论讲解，让读者可以轻松掌握无线网络渗透测试的实施方法

清华大学出版社

Kali Linux
无线网络渗透测试详解

李亚伟　编著

清华大学出版社
北　京

内 容 简 介

本书是国内第一本无线网络安全渗透测试图书。本书基于 Kali Linux 操作系统，由浅入深，全面而系统地介绍了无线网络渗透技术。本书针对不同的加密方式的工作原理及存在的漏洞进行了详细介绍，并根据每种加密方式存在的漏洞介绍了实施渗透测试的方法。另外，本书最后还特意介绍了针对每种加密方法漏洞的应对措施。

本书共 10 章，分为 3 篇。第 1 篇为基础篇，涵盖的主要内容有搭建渗透测试环境和 WiFi 网络的构成。第 2 篇为无线数据篇，涵盖的主要内容有监听 WiFi 网络、捕获数据包、分析数据包和获取信息。第 3 篇为无线网络加密篇，涵盖的主要内容有 WPS 加密模式、WEP 加密模式、WPA 加密模式和 WPA+RADIUS 加密模式。

本书涉及面广，从基本环境搭建到数据包的捕获，再到数据包的分析及信息获取，最后对 WiFi 网络中的各种加密模式进行了分析和渗透测试。本书不仅适合想全面学习 WiFi 网络渗透测试技术的人员阅读，同样适合网络维护人员和各类信息安全从业人员阅读。

图书在版编目（CIP）数据

Kali Linux 无线网络渗透测试详解 / 李亚伟编著. —北京：清华大学出版社，2016
ISBN 978-7-302-42083-5

Ⅰ. ①K…　Ⅱ. ①李…　Ⅲ. ①计算机网络 – 安全技术　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 263983 号

责任编辑：冯志强
封面设计：欧振旭
责任校对：徐俊伟
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**15.5　　**字　　数：**387 千字
版　　次：2016 年 2 月第 1 版　　**印　　次：**2016 年 2 月第 1 次印刷
印　　数：1～3500
定　　价：49.80 元

产品编号：067209-01

前　言

如今，为了满足用户对网络的需求，无线网络得到了广泛应用。同时，无线网络的搭建也越来越简单，仅需要一个无线路由器即可实现。由于无线网络环境中数据是以广播的形式传输的，所以引起了无线网络的安全问题。在无线路由器中，用户可以通过设置不同的加密方法来保证数据的安全。但是，由于某些加密算法存在漏洞，因此专业人士可以将其密码破解出来。所以，无线网络的安全问题已经成为各类安全人员和网络维护人员不得不关注的重点。而发现和解决这类安全问题，就得用到无线网络渗透测试技术。通过对无线网络实施渗透，测试人员就可以获得进入该无线网络的权限，从而解决相关问题。

为了便于读者较好地掌握无线网络渗透测试技术，笔者结合自己多年的网络安全从业经验，分析和总结了无线网络存在的各种问题，编写了这本 Kali Linux 无线网络渗透测试图书。希望各位读者能够在本书的引领下跨入无线网络渗透测试的大门，并成为一名无线网络渗透测试高手。

本书针对无线网络存在的安全问题，介绍了针对各种加密方式实施渗透测试的方法，如 PIN、WEP、WPA/WPA2 和 WPA+RADIUS。另外，本书还介绍了使用 Wireshark 捕获无线网络数据包的方式，并对捕获的包进行解密及分析。学习完本书，相信读者能够具备独立进行无线网络渗透测试的能力。

本书特色

1．基于最新的渗透测试系统Kali Linux

BackTrack 曾是安全领域最知名的测试专用 Linux 系统。但是由于其已经停止更新，全面转向 Kali Linux，所以 Kali Linux 将成为安全人士的不二选择。

2．理论知识和实际操作相结合

本书没有不厌其烦地罗列一大堆枯燥的理论知识，也没有一味地讲解操作，而是将两者结合起来，让读者首先明白测试所依据的理论知识，从而衍生出相应的渗透测试方法。这样，读者可以更加容易掌握书中的内容。

3．内容全面

本书内容全面，首先对无线网络的基础知识进行了详细介绍，如 WiFi 网络的构成、捕获数据的方法，以及分析数据的方法。然后，针对无线网络的各种加密模式给出了具体的渗透测试方法及应对措施。

本书内容及体系结构

第1篇　基础篇（第1～2章）

本篇涵盖的主要内容有搭建渗透测试环境和 WiFi 网络的构成。通过学习本篇内容，读者可以了解 WiFi 网络的基础知识，如 WiFi 网络概述、802.11 协议概述及无线 AP 的设置等。

第2篇　无线数据篇（第3～6章）

本篇涵盖的主要内容有监听 WiFi 网络、捕获数据包、分析数据包和获取信息等。通过学习本篇内容，读者可以掌握捕获各种加密类型的包，并进行解密。而且，读者还可以通过分析数据包，获取重要信息，如 AP 的 SSID、MAC 地址、加密方式及客户端相关信息等。

第3篇　无线网络加密篇（第7～10章）

本篇涵盖的主要内容有 WPS 加密模式、WEP 加密模式、WPA 加密模式和 WPA+RADIUS 加密模式。通过学习本篇内容，读者可以详细了解和掌握各种加密方式的工作原理、优缺点、破解方法及应对措施等。

本书读者对象

- 无线网络渗透测试初学者；
- 想全面理解无线网络渗透测试本质的读者；
- 无线网络渗透测试爱好者；
- 信息安全和网络安全从业人员；
- 初中、高中及大中专院校的学生；
- 社会培训班的学员。

学习建议

- 创建适当的密码字典。对网络实施渗透测试需要有一个强大的字典，否则即使花费大量时间，也未必就能获得自己想要的结果。
- 准备一个大功率的无线网卡。如果想要更好地实施无线网络渗透测试，需要有一个大功率的无线网卡。使用大功率的无线网卡的好处是信号强、信号稳定。
- 要有耐心。通常在破解密码时，如果没有一个很好的密码字典，将需要大量的时间，需要有足够的耐心。

本书配套资源获取方式

本书涉及的一些工具包等配套资源需要读者自行下载。读者可以在本书的服务网站

（www.wanjuanchina.net）上的相关版块上下载这些配套资源。

本书售后服务方式

编程学习的最佳方式是共同学习。但是由于环境所限，大部分读者都是独自前行。为了便于读者更好地学习无线渗透技术语言，我们构建了多样的学习环境，力图打造立体化的学习方式，除了对内容精雕细琢之外，还提供了完善的学习交流和沟通方式。主要有以下几种方式：

- 提供技术论坛 http://www.wanjuanchina.net，读者可以将学习过程中遇到的问题发布到论坛上以获得帮助。
- 提供 QQ 交流群 336212690，读者申请加入该群后便可以和作者及广大读者交流学习心得，解决学习中遇到的各种问题。
- 提供 book@wanjuanchina.net 和 bookservice2008@163.com 服务邮箱，读者可以将自己的疑问发电子邮件以获取帮助。

本书作者

本书主要由李亚伟主笔编写。其他参与编写的人员有魏星、吴宝生、伍远明、谢平、项宇峰、徐楚辉、闫常友、阳麟、杨纪梅、杨松梅、余月、张广龙、张亮、张晓辉、张雪华、赵海波、赵伟、周成、朱森。

阅读本书的过程中若有任何疑问，都可以发邮件或者在论坛和 QQ 群里提问，会有专人为您解答。最后顺祝各位读者读书快乐！

编者

目　录

第 1 篇　基础篇

第 2 篇　无线数据篇

第 3 篇　无线网络加密篇

第 1 篇　基础篇

第 1 章　搭建渗透测试环境

许多提供安全服务的机构会使用一些术语，如安全审计、网络或风险评估，以及渗透测试。这些术语在含义上有一些重叠，从定义上来看，审计是对系统或应用的量化的技术评估。风险评估意为对风险的评测，是指用以发现系统、应用和过程中存在的漏洞的服务。渗透测试的含义则不只是评估，它会用已发现的漏洞来进行测试，以验证该漏洞是否真的存在。本章将介绍搭建渗透测试环境。

1.1　什么是渗透测试

渗透测试并没有一个标准的定义。国外一些安全组织达成共识的通用的说法是，渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析。这个分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

渗透测试与其他评估方法不同。通常的评估方法是根据已知信息资源或其他被评估对象，去发现所有相关的安全问题。渗透测试是根据已知可利用的安全漏洞，去发现是否存在相应的信息资源。相比较而言，通常评估方法对评估结果更具有全面性，而渗透测试更注重安全漏洞的严重性。

通常在渗透测试时，使用两种渗透测试方法，分别是黑盒测试和白盒测试。下面将详细介绍这两种渗透测试方法。

1. 白盒测试

使用白盒测试，需要和客户组织一起工作，来识别出潜在的安全风险，客户组织将会向用户展示它们的系统与网络环境。白盒测试最大的好处就是攻击者将拥有所有的内部知识，并可以在不需要害怕被阻断的情况下任意地实施攻击。而白盒测试的最大问题在于，无法有效地测试客户组织的应急响应程序，也无法判断出它们的安全防护计划对检测特定攻击的效率。如果时间有限，或是特定的渗透测试环节（如信息收集并不在范围之内的话），那么白盒测试是最好的渗透测试方法。

2. 黑盒测试

黑盒测试与白盒测试不同的是，经过授权的黑盒测试是设计为模拟攻击者的入侵行为，并在不了解客户组织大部分信息和知识的情况下实施的。黑盒测试可以用来测试内部安全团队检测和应对一次攻击的能力。黑盒测试是比较费时费力的，同时需要渗透测试者具备更强的技术能力。它依靠攻击者的能力探测获取目标系统的信息。因此，作为一次黑

盒测试的渗透测试者，通常并不需要找出目标系统的所有安全漏洞，而只需要尝试找出并利用可以获取目标系统访问权代价最小的攻击路径，并保证不被检测到。

不论测试方法是否相同，渗透测试通常具有两个显著特点。

- 渗透测试是一个渐进的并且逐步深入的过程。
- 渗透测试是选择不影响业务系统正常运行的攻击方法进行的测试。

注意：在渗透测试之前，需要考虑一些需求，如法律边界、时间限制和约束条件等。所以，在渗透测试时首先要获得客户的许可。如果不这样做的话，将可能导致法律诉讼的问题。因此，一定要进行正确的判断。

1.2　安装 Kali Linux 操作系统

Kali Linux 是一个基于 Debian 的 Linux 发行版，它的前身是 BackTrack Linux 发行版。在该操作系统中，自带了大量安全和取证方面的相关工具。为了方便用户进行渗透测试，本书选择使用 Kali Linux 操作系统。用户可以将 Kali Linux 操作系统安装在物理机、虚拟机、树莓派、U 盘和手机等设备。本节将介绍 Kali Linux 操作系统的安装方法。

1.2.1　在物理机上安装 Kali Linux

在物理机上安装 Kali Linux 操作系统之前，需要做一些准备工作，如确认磁盘空间大小、内存等。为了方便用户的使用，建议磁盘空间至少 25GB，内存最好为 512MB 以上。接下来，就是将 Kali Linux 系统的 ISO 文件刻录到一张 DVD 光盘上。如果用户没有光驱的话，可以将 Kali Linux 系统的 ISO 文件写入到 U 盘上。然后使用 U 盘，引导启动系统。下面将分别介绍这两种安装方法。

当用户确认所安装该操作系统的计算机，硬件没问题的话，接下来需要下载 Kali Linux 的 ISO 文件。Kali Linux 的官方下载地址为 http://www.kali.org/downloads/，目前最新版本为 1.1.0。下载界面如图 1.1 所示。

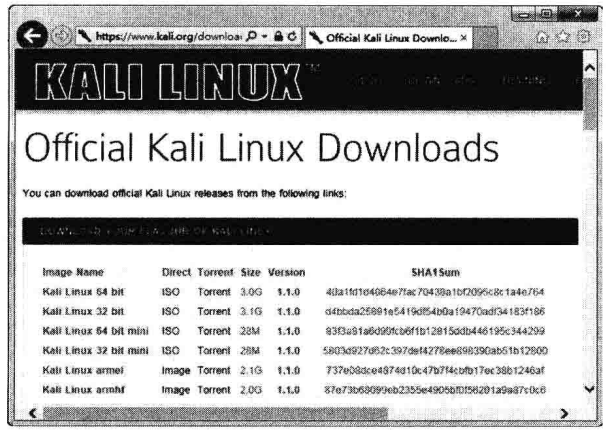

图 1.1　Kali Linux ISO 文件下载界面

从该界面可以看到，Kali Linux 目前最新的版本是 1.1.0，并且在该网站提供了 32 位和 64 位 ISO 文件。由于本书主要介绍对无线网络进行渗透测试，Aircrack-ng 工具是专门用于无线渗透测试的工具，但是，该工具只有在 Kali Linux1.0.5 的内核中才支持。为了使用户更好地使用该工具，本书将介绍安装 Kali Linux1.0.5 操作系统，然后升级到最新版 1.1.0。这样可以保留 1.0.5 操作系统的内核，也就可以很好地使用 Aircrack-ng 工具。目前官方网站已经不提供 1.0.5 的下载，需要到 http://cdimage.kali.org/网站下载，如图 1.2 所示。

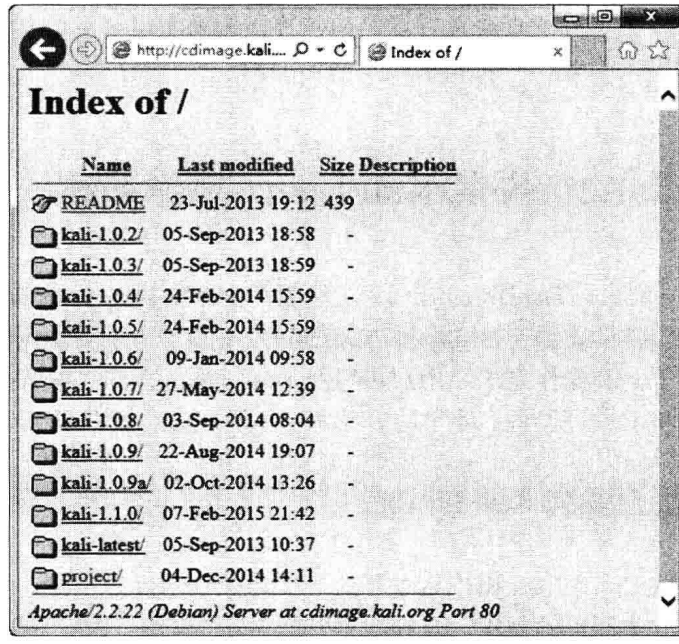

图 1.2　Kali 操作系统的下载页面

从该界面可以看到，在该网站提供了 Kali Linux 操作系统所有版本的下载。这里选择 kali-1.0.5 版本，将打开如图 1.3 所示的界面。

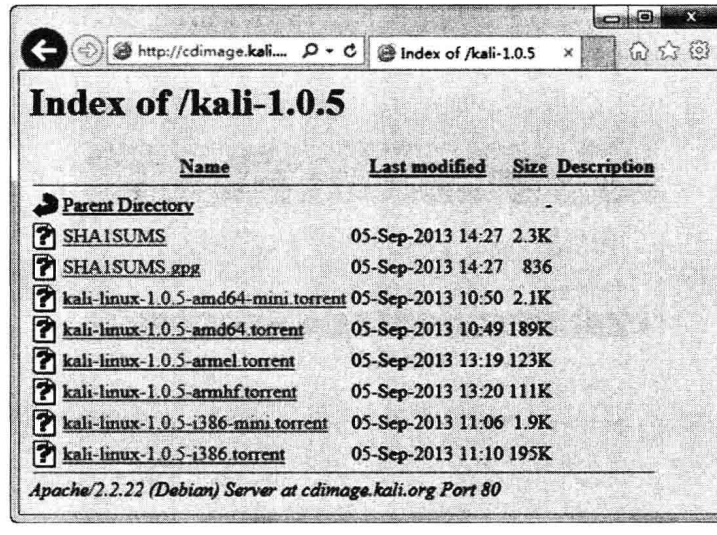

图 1.3　下载 kali linux 1.0.5

从该界面可以看到提供了 Kali Linux1.0.5 各种平台的种子。本书以 64 位操作系统为例，讲解 Kali Linux 的安装和使用，所以选择使用迅雷下载 kali-linux-1.0.5-amd64.torrent 种子的 ISO 文件。用户可以根据自己的硬件配置，选择相应的种子下载。

1. 使用DVD光盘安装Kali Linux

（1）将下载好的 Kali Linux ISO 文件刻录到一张 DVD 光盘上。

（2）将刻录好的 DVD 光盘插入到用户计算机的光驱中，启动系统设置 BIOS 以光盘为第一启动项。然后保存 BIOS 设置，重新启动系统将显示如图 1.4 所示的界面。

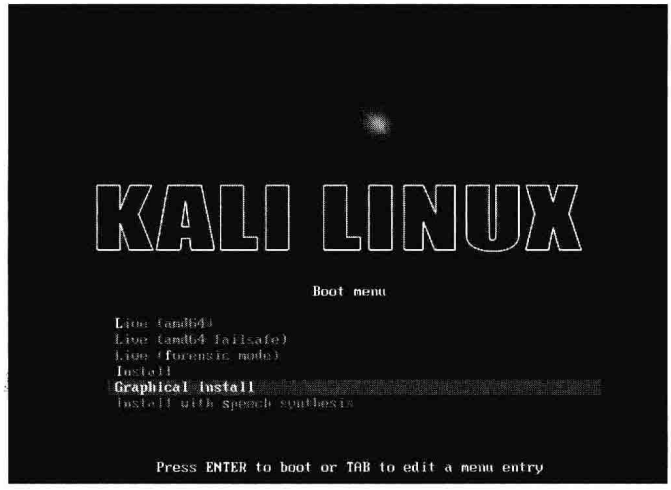

图 1.4　安装界面

（3）该界面是 Kali 的引导界面，在该界面选择安装方式。这里选择 Graphical install（图形界面安装）选项，将显示如图 1.5 所示的界面。

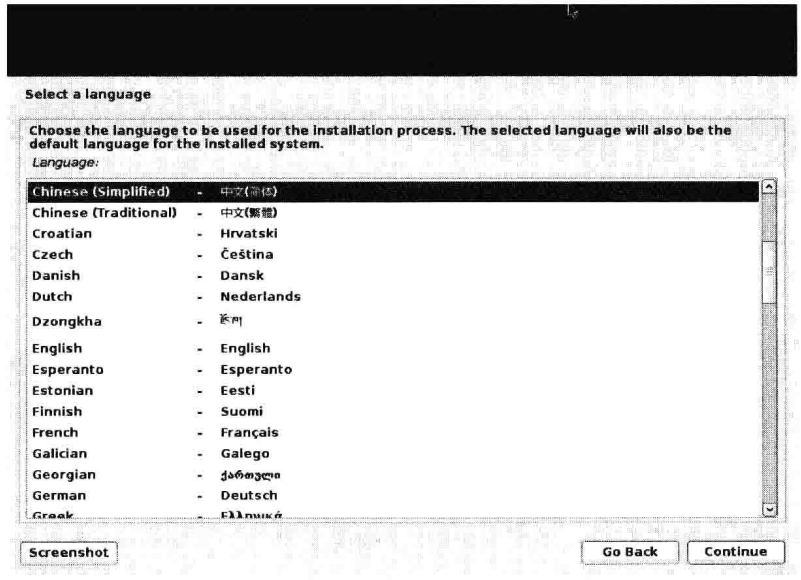

图 1.5　选择语言

（4）在该界面选择安装系统语言，这里选择 Chinese（Simplified）选项。然后单击 Continue 按钮，将显示如图 1.6 所示的界面。

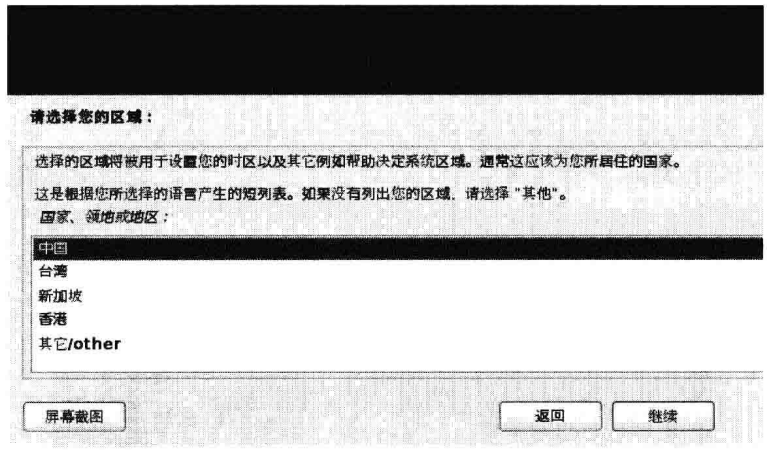

图 1.6　选择区域

（5）在该界面选择用户当前所在的区域，这里选择默认设置“中国”。然后单击“继续”按钮，将显示如图 1.7 所示的界面。

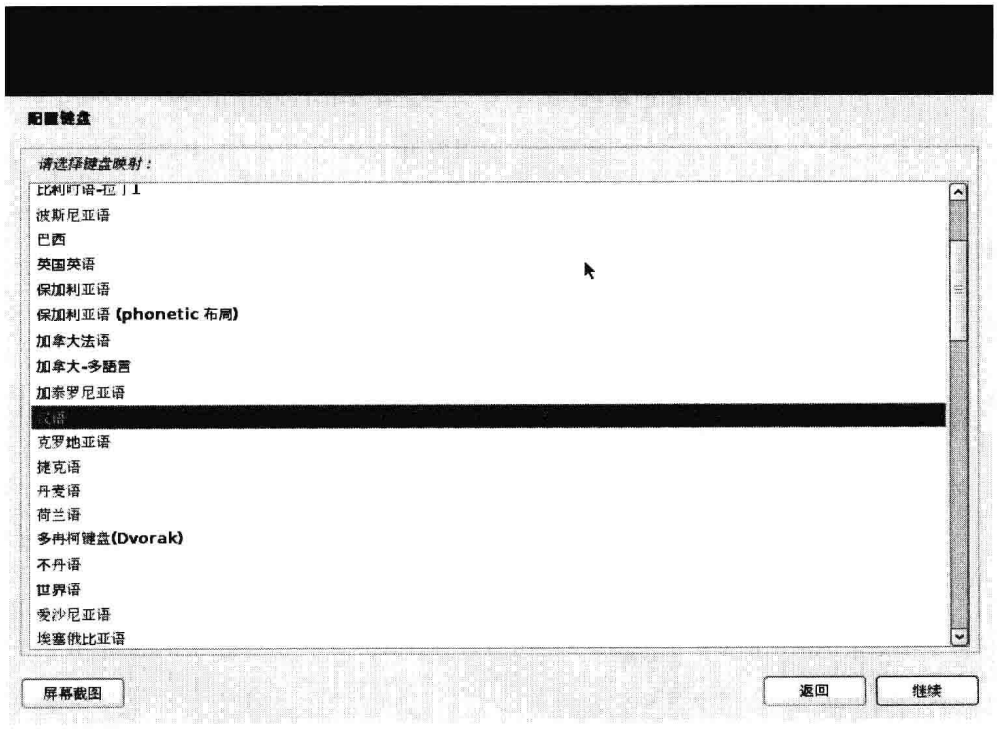

图 1.7　配置键盘

（6）该界面用来配置键盘。这里选择默认的键盘格式“汉语”，然后单击“继续”按钮，将显示如图 1.8 所示的界面。

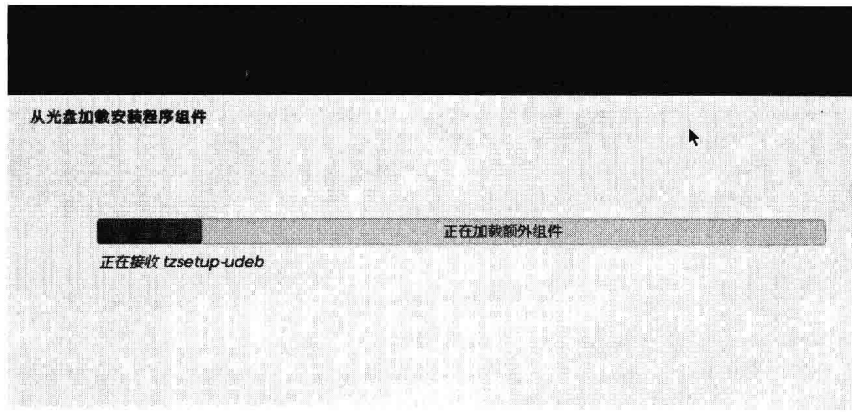

图 1.8　加载额外组件

（7）该过程中会加载一些额外组件并且配置网络。当网络配置成功后，将显示如图 1.9 所示的界面。

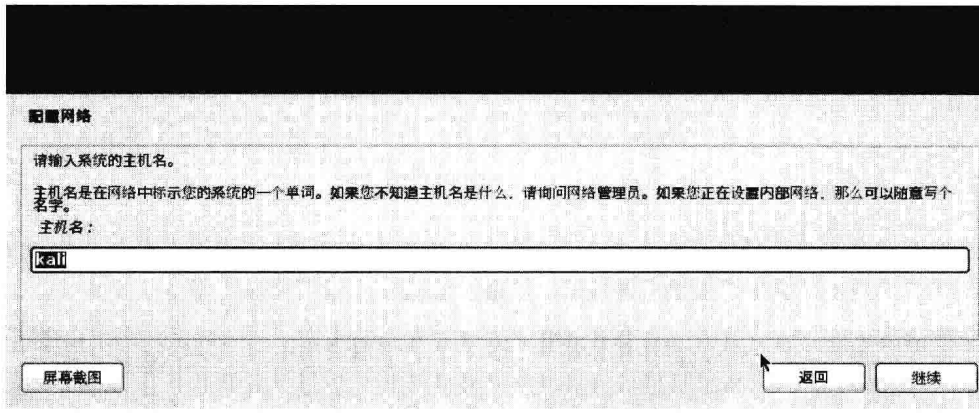

图 1.9　设置主机名

（8）在该界面要求用户设置主机名，这里使用默认设置的名称 Kali。该名称可以任意设置，设置完后单击“继续”按钮，将显示如图 1.10 所示的界面。

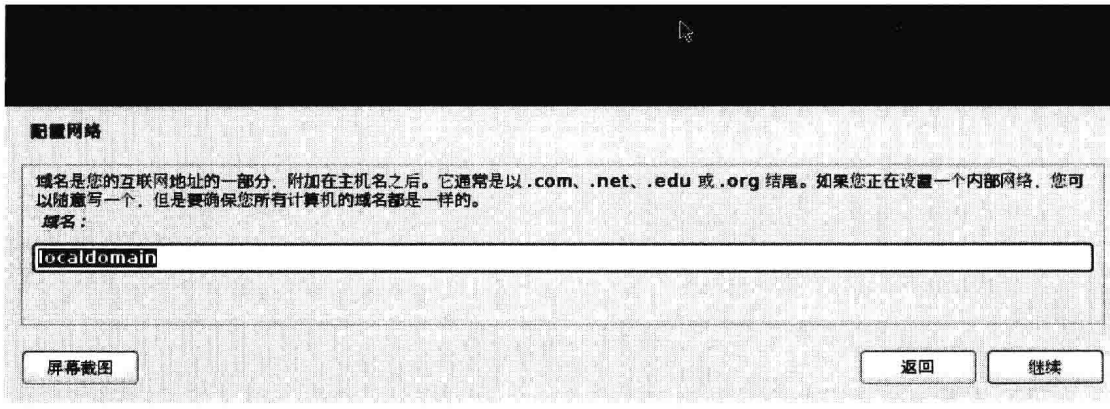

图 1.10　设置域名