Kali Linux
渗透测试技术详解

杨波　编著

基于39款专用工具和38个实例，详细介绍了Kali Linux渗透测试的各种核心技术
涵盖从安装配置，到信息收集和漏洞扫描及利用，再到权限提升及各种渗透测试等技术

- ☑ 基于最为流行的Kali Linux系统，全面介绍了渗透测试的各种核心技术
- ☑ 涉及渗透测试的基础知识、操作系统、网络协议和社会工程学等诸多领域
- ☑ 结合Wireshark等工具，以直观的形式由表及里地展示了网络渗透的奥秘
- ☑ 遵循渗透测试的基本流程，重点介绍了渗透测试的4个大环节及其相关技术
- ☑ 注重操作，避免纯理论讲解，让读者可以轻松掌握渗透测试的实施方法

清华大学出版社

Kali Linux
渗透测试技术详解

杨波　编著

清华大学出版社
北　京

内 容 简 介

本书由浅入深地介绍了 Kali Linux 的各种渗透测试技术。书中选取了最核心和最基础的内容进行讲解，让读者能够掌握渗透测试的流程，而不会被高难度的内容所淹没。本书涉及面广，从基本的知识介绍、安装及配置 Kali Linux，到信息收集和漏洞扫描及利用，再到权限提升及各种渗透测试，均有涉及。

本书共 9 章，分为 3 篇。第 1 篇为 Linux 安全渗透测试基础，介绍了 Linux 安全渗透简介、安装及配置 Kali Linux 操作系统、配置目标测试系统；第 2 篇为信息的收集及利用，介绍了信息收集、漏洞扫描、漏洞利用等技术；第 3 篇为各种渗透测试，介绍了权限提升、密码攻击、无线网络攻击、渗透测试等技术。

本书适合使用 Linux 各个层次的人员作为学习渗透测试技术的基础读物，也适合对安全、渗透感兴趣的人、网络管理员及专门从事搞安全的人员等阅读。

图书在版编目（CIP）数据

Kali Linux 渗透测试技术详解 / 杨波编著. —北京：清华大学出版社，2015
ISBN 978-7-302-38964-4

Ⅰ. ①K…　Ⅱ. ①杨…　Ⅲ. ①Linux 操作系统　Ⅳ. ①TP316.89

中国版本图书馆 CIP 数据核字（2015）第 005625 号

责任编辑：杨如林
封面设计：欧振旭
责任校对：徐俊伟
责任印制：王静怡

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 刷 者：北京鑫丰华彩印有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：20.25　　**字　　数**：506 千字
版　　次：2015 年 3 月第 1 版　　**印　　次**：2015 年 3 月第 1 次印刷
印　　数：1～3500
定　　价：59.80 元

产品编号：062966-01

前　言

由于网络的使用越来越广泛，网络安全问题也越来越被大众关注。在此背景下，Kali Linux 于 2013 年发布。Kali Linux 的前身为网络安全业界知名的 BackTrack。Kali Linux 集成了海量的渗透测试工具，如 nmap、Wireshark、John the Ripper 和 Airecrack-ng 等。

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。

本书选取了 Kali Linux 最核心和最基础的内容进行了讲解，让读者能够掌握渗透测试的流程，并使用 Wireshark 工具，通过分析捕获的数据包，详细介绍了攻击的实现方式。学习完本书后，读者应该可以具备独立进行一些基本渗透测试的能力。

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，而全面转向 Kali Linux，所以 Kali 将成为安全人士的不二选择。本书基于 Kali Linux 来展现渗透测试的各项内容。

2．内容难度适当

本书介绍了 Linux 安全渗透测试的基础知识及操作系统、网络协议、社会工程学等诸多领域，最后还详细介绍了各种渗透测试无线网络。

3．理论和操作结合讲解

本书没有枯燥的罗列理论，也没有一味的讲解操作，而是将两者结合起来，让读者明白测试所基于的理论，以及从中衍生出的测试攻击手段。这样，读者可以更为清楚地掌握书中的内容。

4．更直观的讲述方式

由于网络协议工作在底层，并且渗透工具将功能封装，读者很难看到攻击的实现方式。为了让读者更直观的理解，本书采用 Wireshark 抓包和分析包的方式，给读者展示了攻击过程中实现的各个细节。这样，读者既可以掌握理论，也可以避免成为只会使用工具的初级技术工。

5. 提供多种学习和交流的方式

为了方便大家学习和交流，我们提供了多种方式供读者交流。读者可以在论坛 www.wanjuanchina.net 上发帖讨论，也可以通过 QQ 群 336212690 转入对应的技术群；还可以就图书阅读中遇到的问题致信 book@wanjuanchina.net 或 bookservice2008@163.com，以获得帮助。另外，本书涉及的工具也可以在论坛的相关版块获取。

本书内容及体系结构

第1篇　Linux安全渗透测试基础（第1～3章）

本篇主要内容包括：Linux 安全渗透简介、配置 Kali Linux 和高级测试实验室。通过本篇的学习，读者可以了解安全渗透测试的概念及所需的工具、在各种设备上安装 Kali Linux 操作系统、配置目标系统等。

第2篇　信息的收集及利用（第4～6章）

本篇主要内容包括：信息收集、漏洞扫描和漏洞利用等。通过本篇的学习，读者可以收集大量目标主机的信息、扫描目标主机存在的漏洞及利用这些漏洞，为后续渗透攻击做好准备。

第3篇　各种渗透测试（第7～9章）

本篇主要内容包括：提升用户权限、密码攻击和无线网络渗透测试等。通过本篇的学习，读者可以通过提升自己的权限，实现各种密码攻击，如获取目标主机上各种服务的用户名、密码和无线网络的登录密码等。

学习建议

- 掌握基本的网络协议。通常攻击目标主机，需要了解其存在的漏洞或开放的端口，但是这些端口都对应有一个网络协议，了解对应的网络协议和工作机制，可以更好地收集信息和寻找漏洞。
- 一定要有耐心。渗透测试往往需要花费大量的时间，例如通常在破解密码时，如果没有一个很好的密码字典，会需要几个小时、甚至几天的时间。再比如要抓取理想的数据包，往往需要长时间的等待，然后从海量数据包中寻找需要的信息。

本书读者对象

- Linux 初学者；
- 想成为安全渗透测试人员；
- 渗透测试兴趣爱好者；

- 网络管理员；
- 专业的安全渗透测试人员；
- 大中专院校的学生；
- 社会培训班学员；
- 需要一本案头必备手册的程序员。

本书作者

本书主要由兰州文理学院电子信息工程学院的杨波主笔编写。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　Linux 安全渗透测试基础

第 2 篇　信息的收集及利用

第 1 篇　Linux 安全渗透测试基础

第 1 章　Linux 安全渗透简介

渗透测试是对用户信息安全措施积极评估的过程。通过系统化的操作和分析，积极发现系统和网络中存在的各种缺陷和弱点，如设计缺陷和技术缺陷。本章将简要介绍 Linux 安全渗透及安全渗透工具的相关内容。其主要知识点如下：

- 什么是安全渗透；
- 安全渗透所需的工具；
- Kali Linux 简介；
- 安装 Kali Linux；
- Kali 更新与升级；
- 基本设置。

1.1　什么是安全渗透

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。

渗透测试有黑盒和白盒两种测试方法。黑盒测试是指在对基础设施不知情的情况下进行测试。白盒测试是指在完全了解结构的情况下进行测试。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。

1.2　安全渗透所需的工具

了解了渗透测试的概念后，接下来就要学习进行渗透测试所使用的各种工具。在做渗透测试之前，需要先了解渗透所需的工具。渗透测试所需的工具如表 1-1 所示。

表 1-1　渗透所需的工具

splint	unhide	scrub
pscan	examiner	ht
flawfinder	srm	driftnet
rats	nwipe	binwalk
ddrescue	firstaidkit-gui	scalpel
gparted	xmount	pdfcrack
testdisk	dc3dd	wipe
foremost	afftools	safecopy
sectool-gui	scanmem	hfsutils
unhide	sleuthkit	cmospwd
examiner	macchanger	secuirty-menus
srm	ngrep	nc6
nwipe	ntfs-3g	mc
firstaidkit-gui	ntfsprogs	screen
net-snmp	pcapdiff	openvas-scanner
hexedit	netsed	rkhunter
irssi	dnstop	labrea
powertop	sslstrip	nebula
mutt	bonesi	tripwire
nano	proxychains	prelude-lml
vim-enhanced	prewikka	iftop
wget	prelude-manager	scamper
yum-utils	picviz-gui	iptraf-ng
mcabber	telnet	iperf
firstaidkit-plugin-all	onenssh	nethogs
vnstat	dnstracer	uperf
aircrack-ng	chkrootkit	nload
airsnort	aide	ntop
kismet	pads	trafshow
weplab	cowpatty	wavemon

由于篇幅原因，这里只列了一部分工具。渗透测试所需的工具可以在各种 Linux 操作系统中找到，然后手动安装这些工具。由于工具繁杂，安装这些工具，会变成一个浩大的工程。为了方便用户进行渗透方面的工作，有人将所有的工具都预装在一个 Linux 系统。其中，典型的操作系统就是本书所使用的 Kali Linux。

该系统主要用于渗透测试。它预装了许多渗透测试软件，包括 nmap 端口扫描器、Wireshark（数据包分析器）、John the Ripper（密码破解）及 Aircrack-ng（一套用于对无线局域网进行渗透测试的软件）。用户可通过硬盘、Live CD 或 Live USB 来运行 Kali Linux。

1.3　Kali Linux 简介

Kali Linux 的前身是 BackTrack Linux 发行版。Kali Linux 是一个基于 Debian 的 Linux

发行版，包括很多安全和取证方面的相关工具。它由 Offensive Security Ltd 维护和资助，最先由 Offensive Security 的 MatiAharoni 和 Devon Kearns 通过重写 Back Track 来完成。Back Track 是基于 Ubuntu 的一个 Linux 发行版。

Kali Linux 有 32 位和 64 位的镜像，可用于 x86 指令集。同时它还有基于 ARM 架构的镜像，可用于树莓派和三星的 ARM Chromebook。用户可通过硬盘、Live CD 或 Live USB 来运行 Kali Linux 操作系统。

1.4　安装 Kali Linux

如今 Linux 的安装过程已经非常“傻瓜”化，只需要轻点几下鼠标，就能够完成整个系统的安装。Kali Linux 操作系统的安装也非常简单。本节将分别介绍安装 Kali Linux 至硬盘、USB 驱动器、树莓派、VMware Workstation 和 Womuare Tods 的详细过程。

1.4.1　安装至硬盘

安装到硬盘是最基本的操作之一。该工作的实现可以让用户不使用 DVD，而正常的运行 Kali Linux。在安装这个全新的操作系统之前，需要做一些准备工作。例如，从哪里得到 Linux？对电脑配置有什么要求？.....下面将逐一列出这些要求。

- Kali Linux 安装的磁盘空间的最小值是 8GB。为了便于使用，这里推荐至少 25GB 去保存附加程序和文件。
- 内存最好为 512MB 以上。
- Kali Linux 的下载地址 http://www.kali.org/downloads/，下载界面如图 1.1 所示。

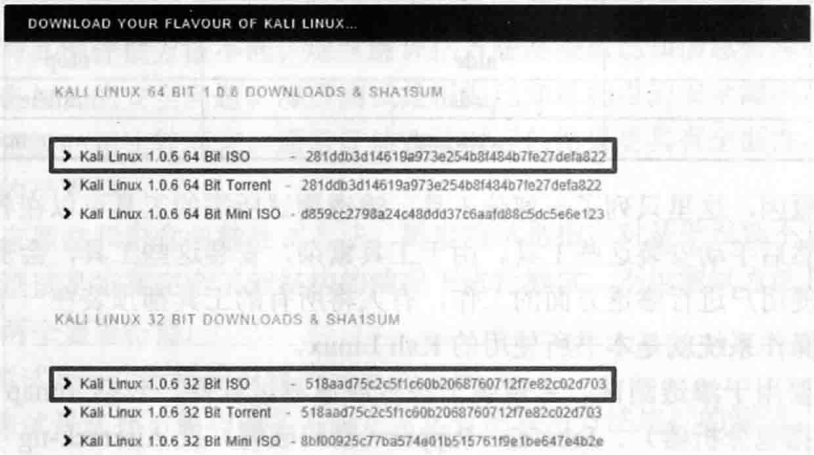

图 1.1　下载 Kali Linux 界面

该官方网站提供了 32 位和 64 位 ISO 文件。本书中以 32 位为例来讲解安装和使用。下载完 ISO 文件后，将该映像文件刻录到一张 DVD 光盘上。接下来就可以着手将 KaliLinux 安装至硬盘中了。

（1）将安装光盘 DVD 插入到用户计算机的光驱中，重新启动系统，将看到如图 1.2 所示的界面。

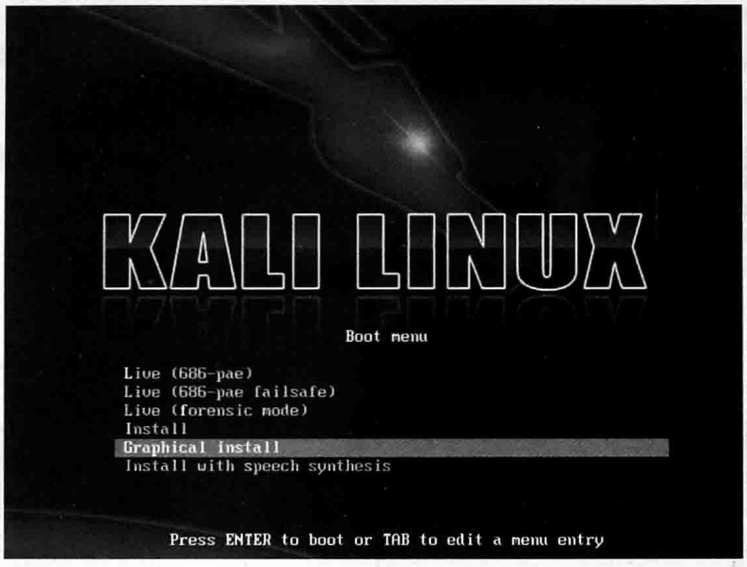

图 1.2　启动界面

（2）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），将显示如图 1.3 所示的界面。

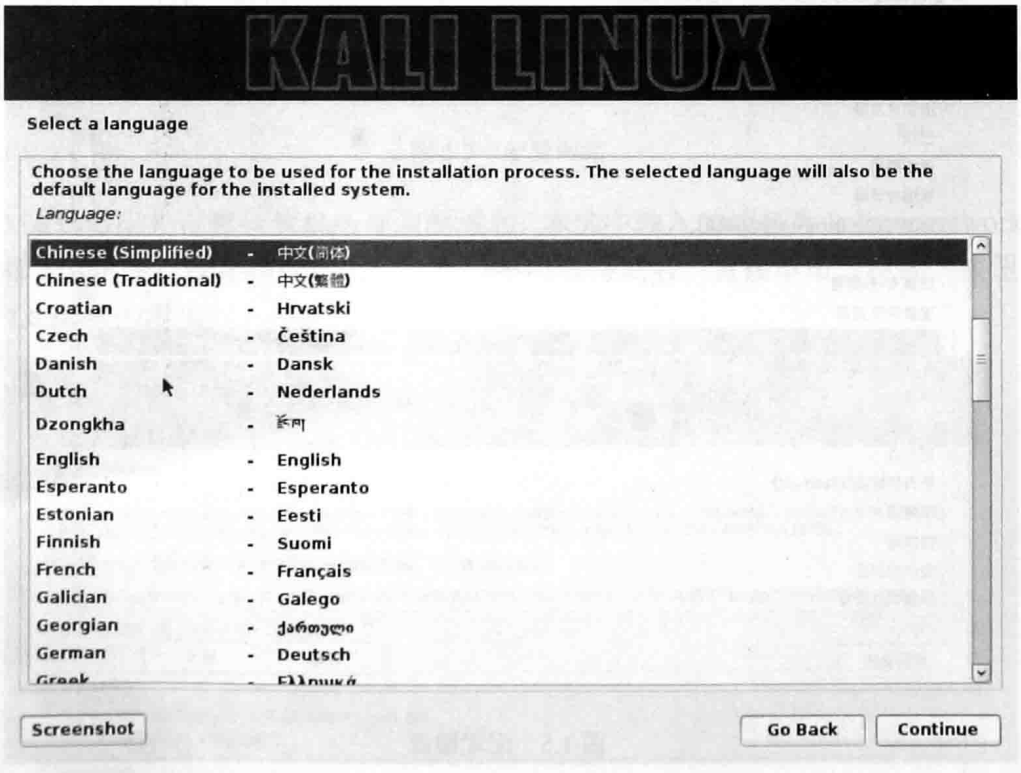

图 1.3　选择语言

（3）在该界面选择安装系统的默认语言为 Chinese（Simplified），然后单击 Continue 按钮，将显示如图 1.4 所示的界面。

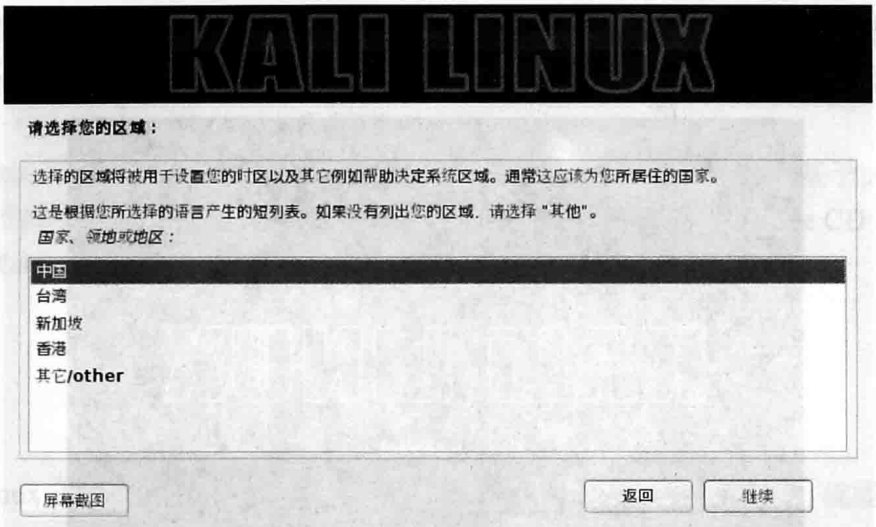

图 1.4　选择您的区域

（4）在该界面选择区域为“中国”，然后单击“继续”按钮，将显示如图 1.5 所示的界面。

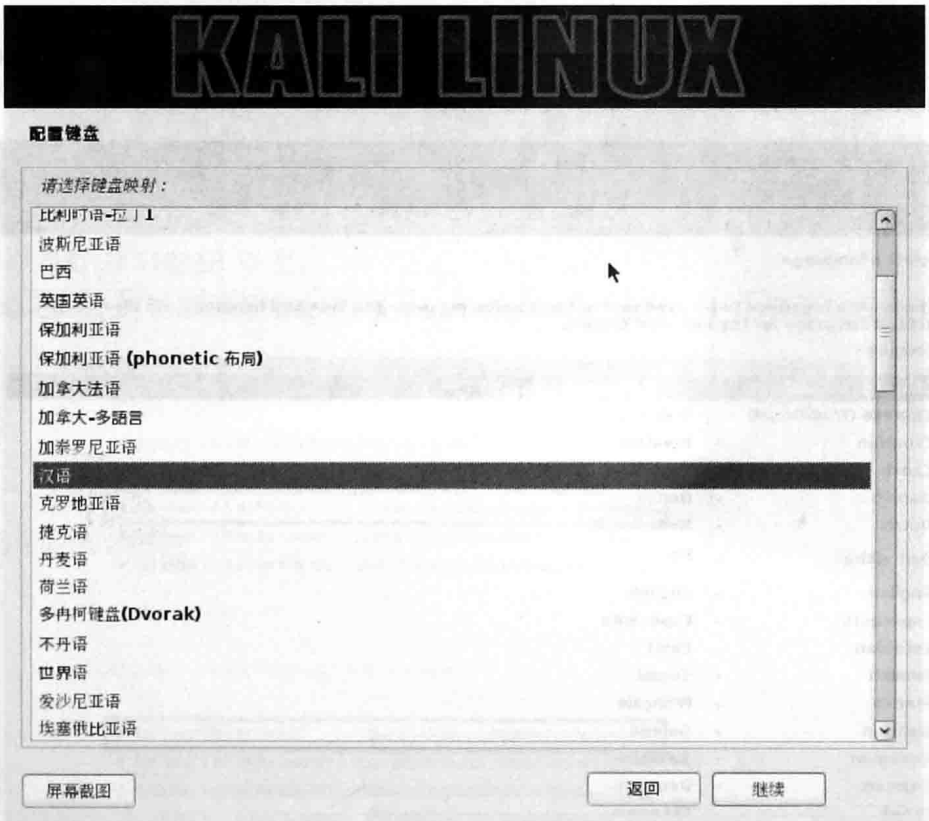

图 1.5　配置键盘

（5）在该界面选择键盘模式为“汉语”，然后单击“继续”按钮，将显示如图 1.6 所示的界面。

（6）该界面用来设置系统的主机名，这里使用默认的主机名 Kali（用户也可以输入自己系统的名字）。然后单击“继续”按钮，将显示如图 1.7 所示的界面。

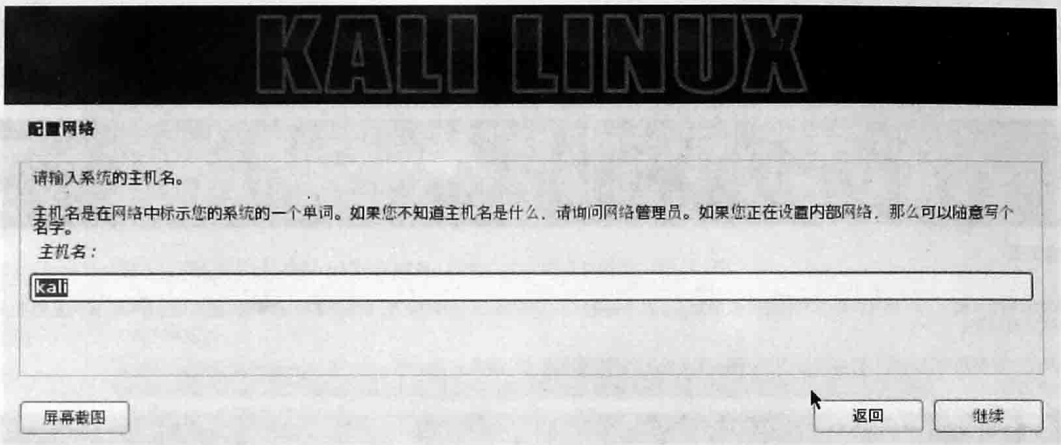

图 1.6　配置网络

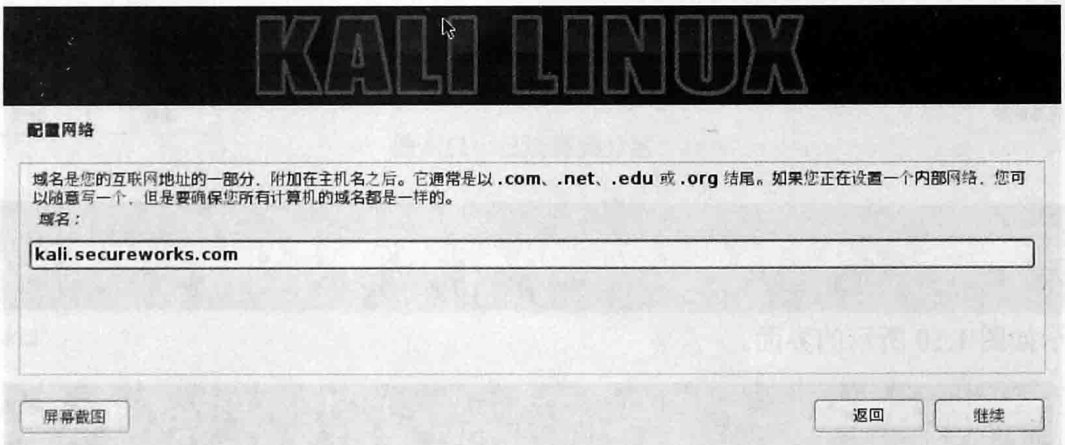

图 1.7　配置网络

（7）该界面用来设置计算机所使用的域名，本例中输入的域名为 kali.secureworks.com。如果当前计算机没有连接到网络的话，可以不用填写域名，直接单击“继续”按钮，将显示如图 1.8 所示的界面。

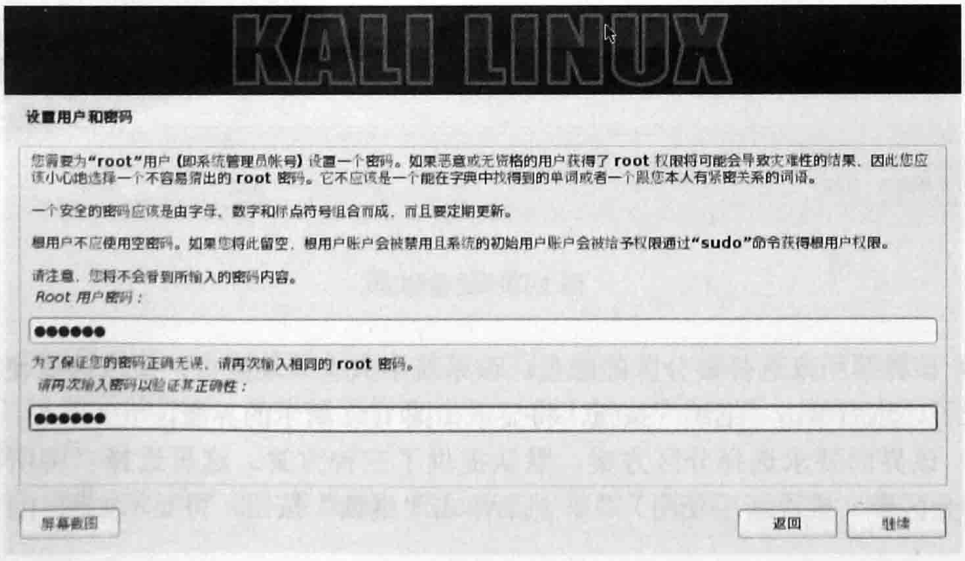

图 1.8　设置用户和密码