网络攻防与实践

刘坤　主编

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

网络攻防与实践

主　编　刘　坤
副主编　杨正校　刘　静　沈　啸　汪小霞

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

内容简介

网络与信息安全方面的研究是当前信息行业的研究重点。这本书精心选取了目前网络安全攻击与防范方面具有普遍性的典型内容，具体内容包括网络攻防实验环境的搭建、网络扫描器的使用、网络嗅探抓包工具的使用、获取和破解用户密码、数据库攻击与加固技术、Web 渗透与加固技术、操作系统安全加固技术等 7 个工作项目及若干个工作任务。

图书在版编目（CIP）数据

网络攻防与实践 / 刘坤主编 . —北京：北京理工大学出版社，2018. 7
ISBN 978 - 7 - 5682 - 5132 - 7

Ⅰ. ①网…　Ⅱ. ①刘…　Ⅲ. ①计算机网络 - 网络安全　Ⅳ. ①TP393. 08

中国版本图书馆 CIP 数据核字（2018）第 000466 号

出版发行 / 北京理工大学出版社有限责任公司
社　　址 / 北京市海淀区中关村南大街 5 号
邮　　编 / 100081
电　　话 / （010）68914775（总编室）
　　（010）82562903（教材售后服务热线）
　　（010）68948351（其他图书服务热线）
网　　址 / http：//www. bitpress. com. cn
经　　销 / 全国各地新华书店
印　　刷 / 山东临沂新华印刷物流集团有限责任公司
开　　本 / 787 毫米 ×1 092 毫米　1/16
印　　张 / 21
字　　数 / 495 千字
版　　次 / 2018 年 7 月第 1 版　2018 年 7 月第 1 次印刷
定　　价 / 75. 00 元

责任编辑 / 杜春英
文案编辑 / 杜春英
责任校对 / 周瑞红
责任印制 / 施胜娟

前　言

本教材针对计算机网络专业学生及计算机网络安全技术爱好者，教材突出以下特点：以能力为本位，贯彻精讲多练的原则，强调培养学生的实践技能；以项目化教学为特色，选取适当的项目载体，采用任务驱动，实施工作过程导向的理实一体化教学。每个项目有若干个工作任务，每个任务都是以行动为导向，帮助同学们通过任务训练操作来理解知识点，每个项目后面都安排了一定数量的练习与实践。

本课程按照“以能力为本位、以职业技能训练为主线、以项目课程为载体的模块化专业课程体系”的总体设计要求，按理论实践一体化要求设计。体现“以就业为导向、以能力为本位”的培养目标，遵照网络安全管理员岗位的需求，课程项目选取的依据是该门课程涉及的工作领域和工作任务范围，以当前网络攻防技术的典型实际工作项目为载体，设计出具体的学习项目。

通过对网络安全管理员岗位的调研，与行业、企业专家进行深入细致、系统的分析，课程整体设计针对网络安全管理员岗位职能需求和网络攻防操作技能要求设计教学内容，采用由浅入深、由简单到复杂的方式组织项目内容，开展“任务驱动、赛项融合、攻防一体”的教学模式，一共设计了7个教学项目，涵盖了网络扫描、网络嗅探抓包分析、数据库攻击与加固、Web渗透与加固、系统加固等方面的知识点和技能点。

教材紧紧抓住学生对网络安全攻防的兴趣点，设计攻防一体学习任务，正确引导读者对系统漏洞、黑客入侵的重视，并在编写教材中融入了让学生快乐学习的方法。教材内容设计加强创设真实的企业情境，强调探究性学习、互动学习、协作学习等多种学习策略，培养学生的可持续发展能力。

本书由苏州健雄职业技术学院软件与服务外包学院信息安全与管理专业教师刘坤主编，杨正校、刘静、沈啸、汪小霞任副主编，其中刘静老师编写项目1，杨正校老师编写项目2，汪小霞老师编写项目7，刘坤老师编写项目3、4和6，沈啸老师编写项目5，由刘坤老师负责书稿的统稿工作。

在使用本书的过程中，如果发现不足和错误之处，敬请读者将修改意见发到电子邮箱liukun1008@sohu.com。本书在编写过程中还得到了苏州健雄职业技术学院软件与服务外包学院其他老师的大力帮助，在此一并表示衷心感谢。

编　者

目　录

项目1　网络攻防实验环境的搭建

项目2　网络扫描器的使用

项目3　网络嗅探抓包工具的使用

项目4　获取和破解用户密码

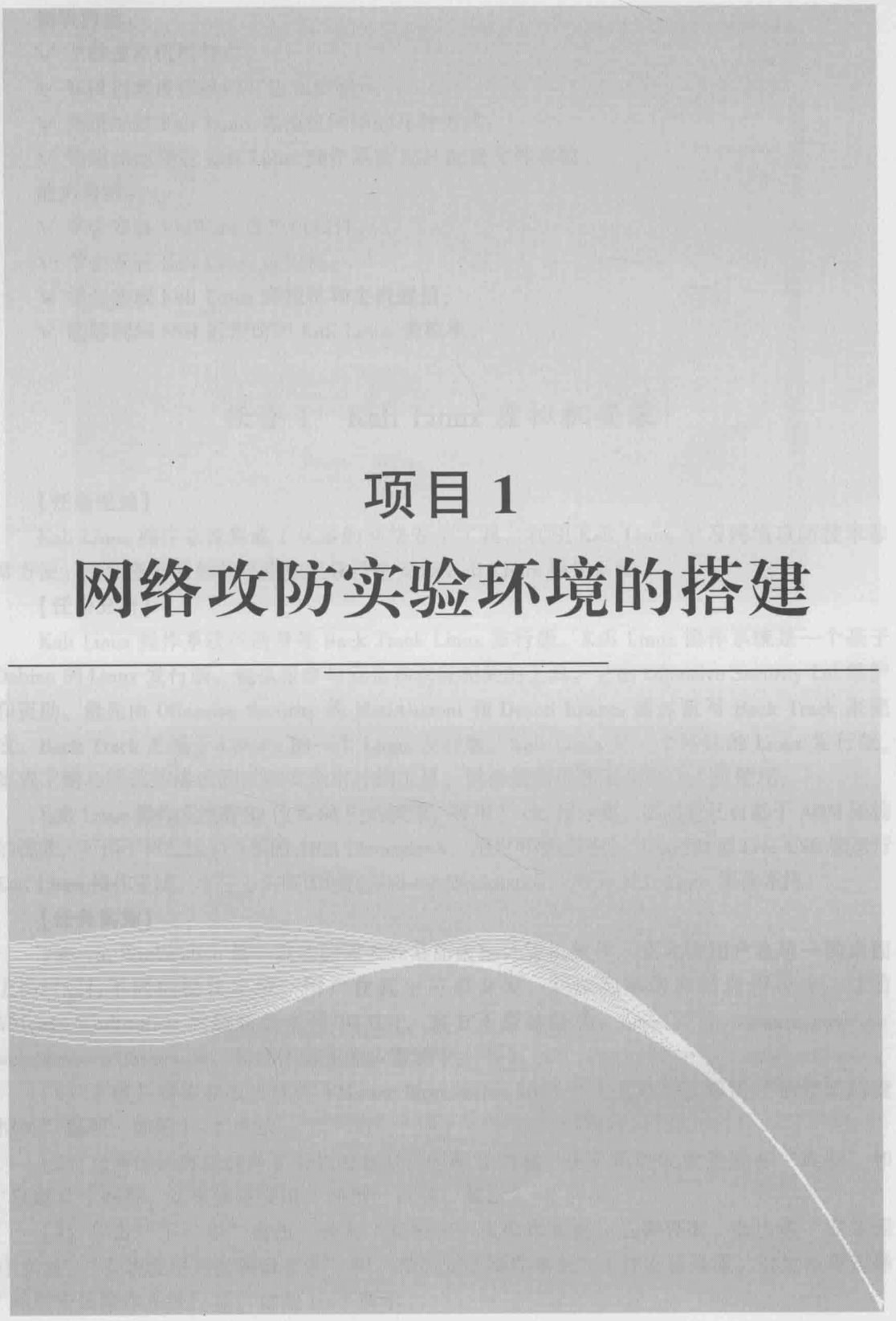
项目5　数据库攻击与加固技术

项目6　Web 渗透与加固技术

项目 7　操作系统安全加固技术

项目 1

网络攻防实验环境的搭建



项目1

网络攻防实验环境的搭建

知识目标：

√ 了解虚拟机的特点；

√ 知道创建虚拟机的方法和步骤；

√ 知道配置 Kali Linux 虚拟机网络的几种方式；

√ 知道如何设置 Kali Linux 操作系统 SSH 配置文件参数。

能力目标：

√ 学会安装 VMWare 虚拟机软件；

√ 学会安装 Kali Linux 虚拟机；

√ 学会实现 Kali Linux 虚拟机和主机通信；

√ 能够利用 SSH 远程访问 Kali Linux 虚拟机。

任务1　Kali Linux 虚拟机安装

【任务描述】

Kali Linux 操作系统集成了众多的网络安全工具，利用 Kali Linux 学习网络攻防技术非常方便。本任务学习如何在虚拟机软件中安装 Kali Linux 操作系统。

【任务分析】

Kali Linux 操作系统的前身是 Back Track Linux 发行版。Kali Linux 操作系统是一个基于 Debian 的 Linux 发行版，包括很多与安全和取证相关的工具。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 是一个特殊的 Linux 发行版，集成了精心挑选的渗透测试和安全审计的工具，供渗透测试和安全设计人员使用。

Kali Linux 操作系统有 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。本任务讲解如何在 VMware Workstation 上安装 Kali Linux 操作系统。

【任务实施】

VMware Workstation 是一款功能强大的桌面虚拟计算机软件。它允许用户在单一的桌面上同时运行不同的操作系统，用户在其中可以开发、测试和部署新的应用程序。目前 VMware Workstation 的最新版本是 10.0.1，官方下载地址为：https://my.vmware.com/cn/web/vmware/downloads。其具体的实施步骤如下：

（1）下载并安装虚拟机软件 VMware Workstation 10.0.1 工具软件，单击“创建新的虚拟机”选项，如图 1-1 所示。

（2）在弹出的界面选择要安装的虚拟机的配置类型。虚拟机的配置类型有“典型”和“自定义”两种，这里推荐使用“典型”配置，如图 1-2 所示。

（3）单击“下一步”按钮，进入“安装客户机操作系统”选择界面，会出现“安装程序光盘”“安装程序光盘映像文件”和“稍后安装操作系统”3 种安装来源，这里推荐选择“稍后安装操作系统”项，如图 1-3 所示。

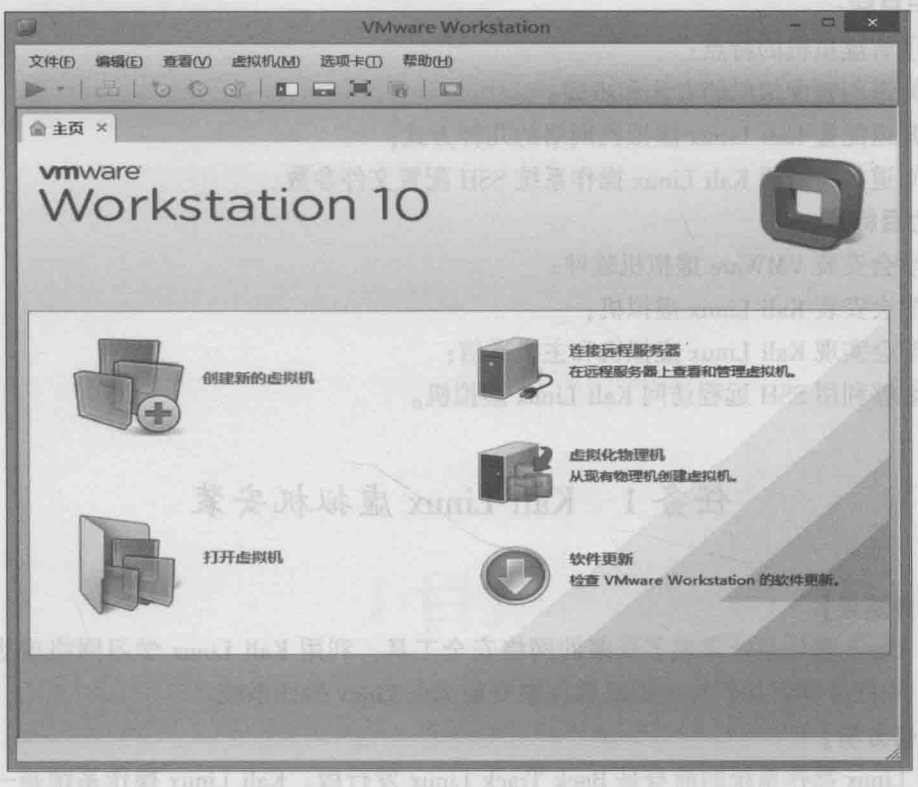


图 1-1 创建新的虚拟机

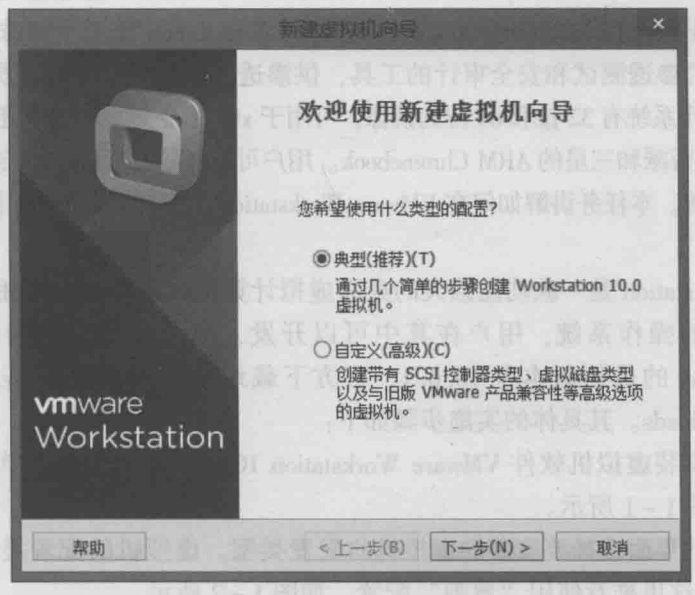


图 1-2 选择“典型”配置

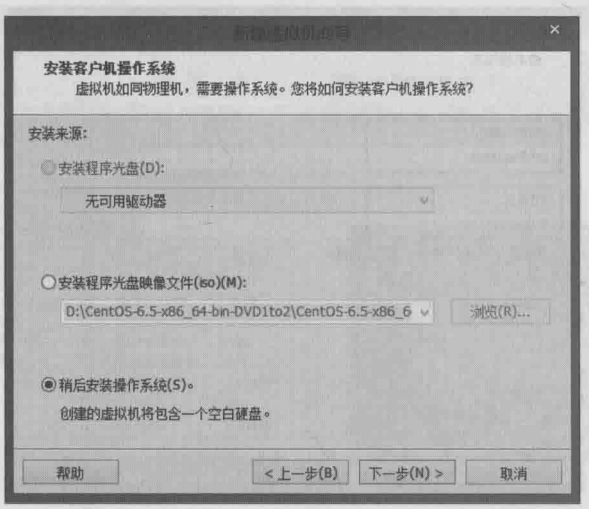


图1-3　“安装客户机操作系统”选择界面

(4) 单击“下一步”按钮，在弹出的界面选择要安装的操作系统和版本。这里选择“Linux”操作系统，版本为“其他 Linux 3. x 内核 64 位”，如图1-4所示。

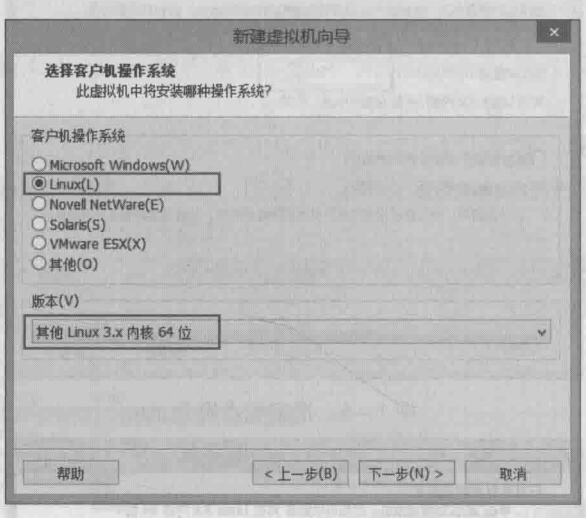


图1-4　选择“客户机操作系统”类型

(5) 单击“下一步”按钮，在弹出的界面中为虚拟机创建一个名称，并设置虚拟机的安装位置。这里我们设置虚拟机名称为“kali linux test”，保存位置为“D:\kali linux test”，如图1-5所示。

(6) 单击“下一步”按钮，在弹出的界面中设置磁盘的容量。如果有足够大的磁盘，则建议磁盘容量设置得大些，以免造成磁盘容量不足。这里设置为50 GB，如图1-6所示。

(7) 单击“下一步”按钮，在弹出的界面中显示了所要创建的虚拟机的详细设置，如图1-7所示，此时就可以创建操作系统了。

(8) 单击“完成”按钮后，虚拟机“kali linux test”就创建好了。该界面显示了新创建的虚拟机的详细信息，如图1-8所示。

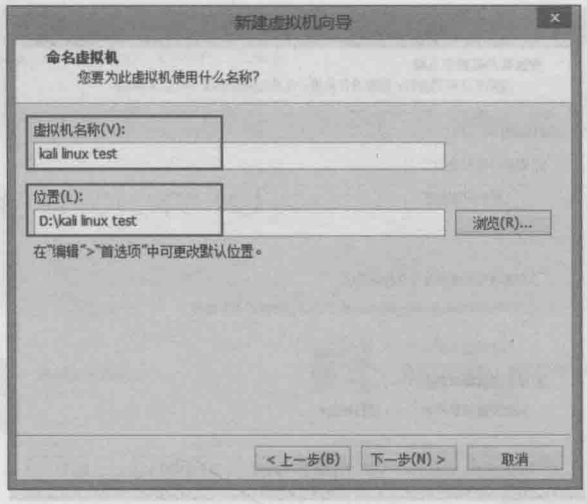


图 1-5　命名虚拟机

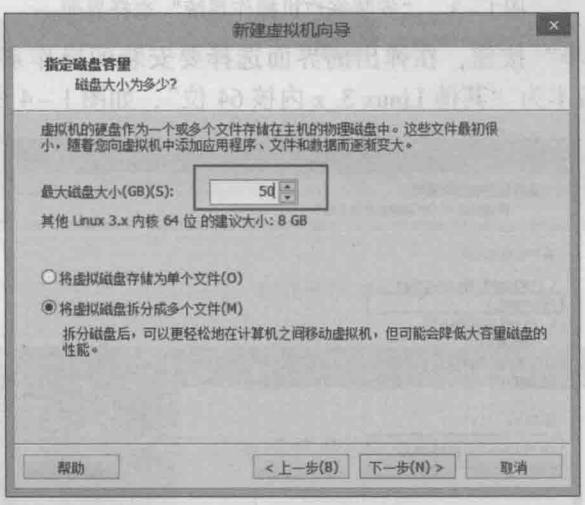


图 1-6　指定磁盘容量

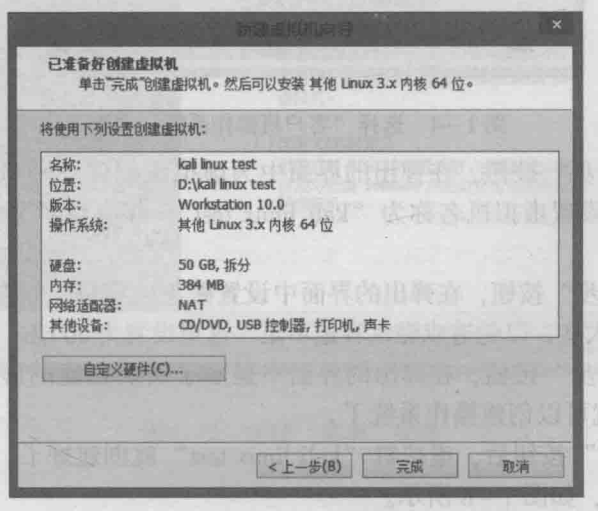


图 1-7　显示虚拟机详细设置

图1-8　虚拟机详细信息

(9) 现在准备安装 Kali Linux 操作系统。在安装 Kali Linux 操作系统之前需要设置一些信息，在“VMware Workstation”窗口中单击“编辑虚拟机设置”命令（见图1-8），将显示如图1-9所示的界面。在该界面选择“CD/DVD (IDE)”选项，接着在右侧选中“使用ISO映像文件”单选按钮，单击“浏览”按钮，选择 Kali Linux 的映像文件。然后单击“确定”按钮，将返回到图1-8所示的界面。

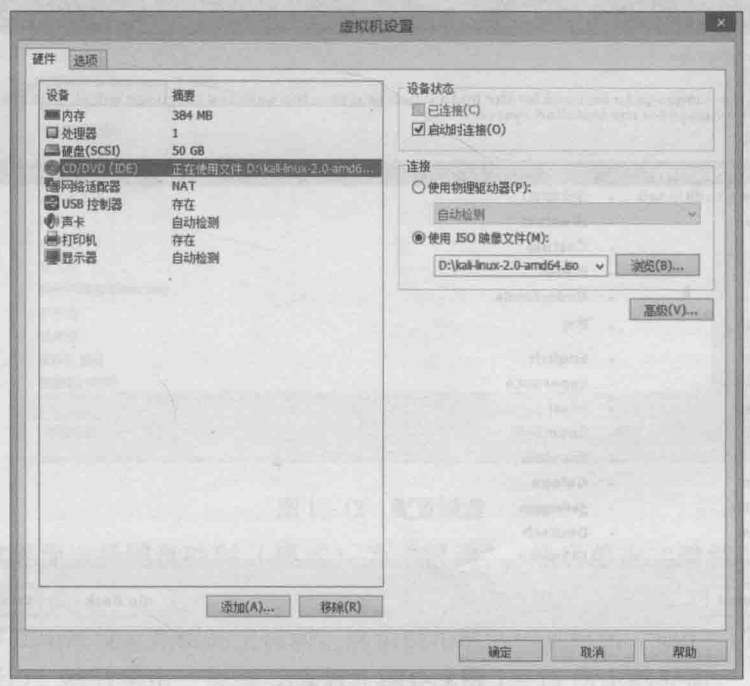


图1-9　设置虚拟机映像文件

（10）在图1－8所示的界面中，单击“开启此虚拟机”命令，将显示一个新的窗口，如图1－10所示。

图1－10　开始安装 Kaili Linux 操作系统

（11）图1－10所示界面是 Kali Linux 操作系统的引导界面，在该界面选择 Kali Linux 操作系统的安装方式。这里选择“Graphical install”（图形界面安装），将显示图1－11所示的界面。

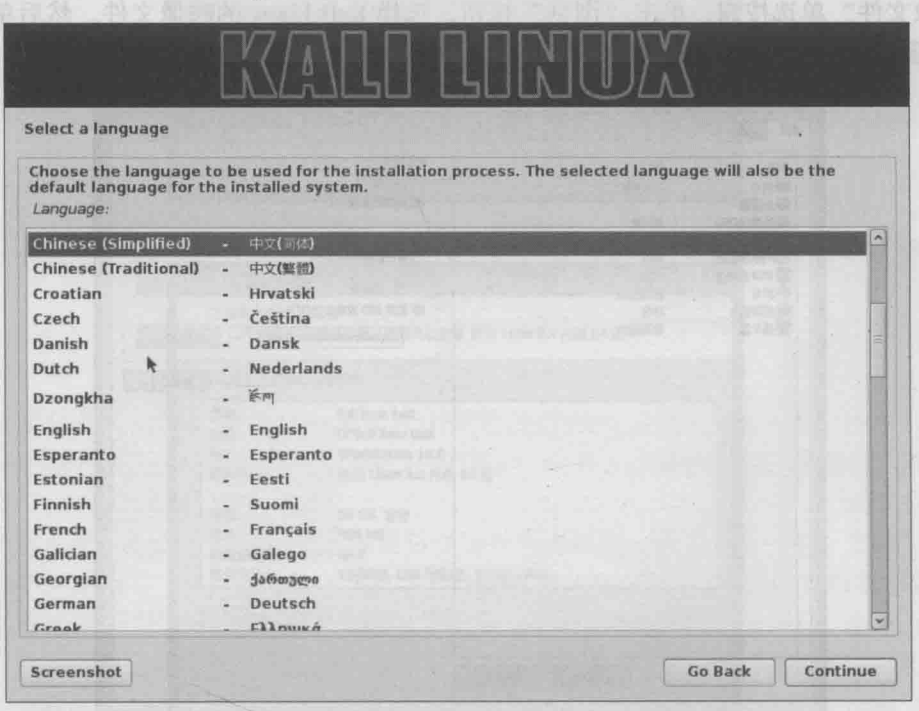


图1－11　选择语言

（12）在该界面选择安装系统的语言。这里选择默认语言“Chinese（Simplified）”，然后单击“Continue”按钮，将显示图1－12所示的界面。

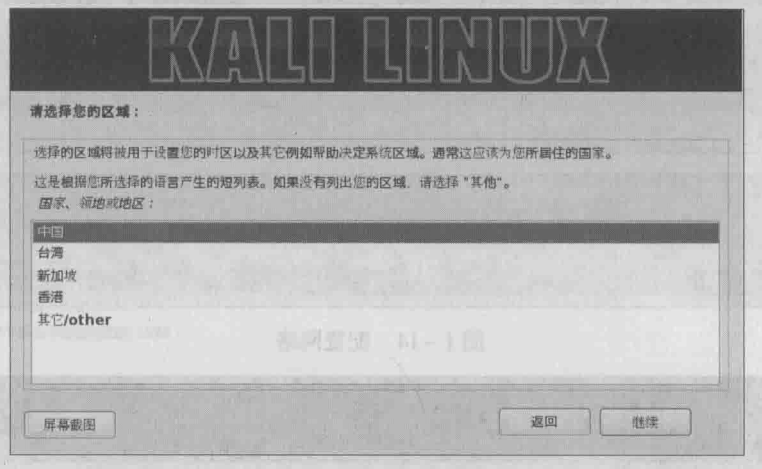


图1－12　选择你的区域

（13）在该界面选择区域。这里选择“中国”，然后单击“继续”按钮，将显示图1－13所示的界面。

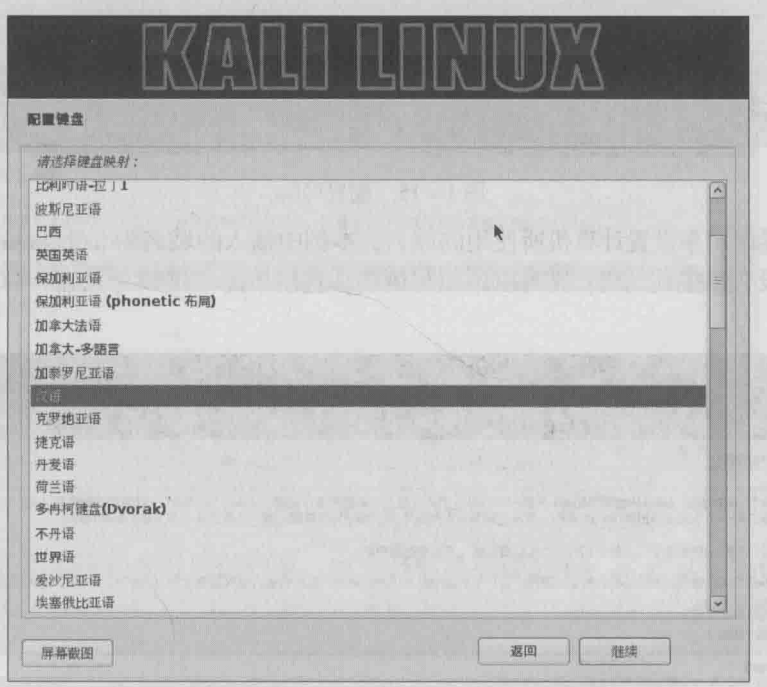


图1－13　配置键盘

（14）在该界面选择键盘映射（模式）为“汉语”，然后单击“继续”按钮，将显示图1－14所示的界面。

（15）该界面用来设置系统的主机名。这里使用默认的主机名“kali”（用户也可以自定义系统的主机名），然后单击“继续”按钮，将显示图1－15所示的界面。

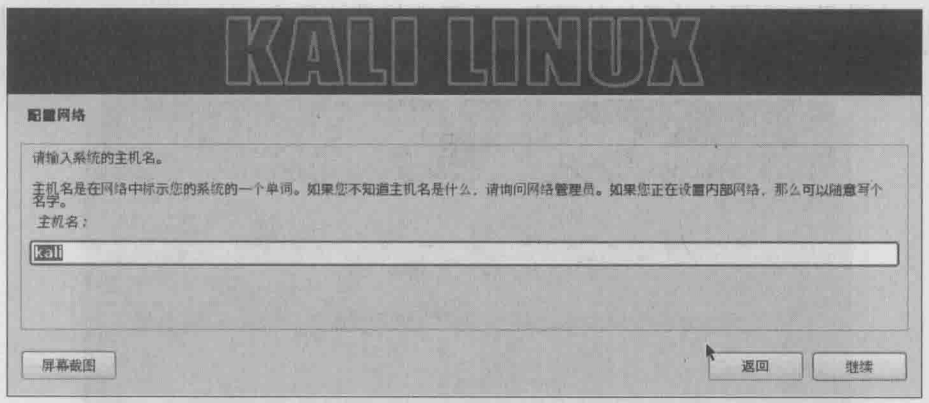


图 1－14　配置网络

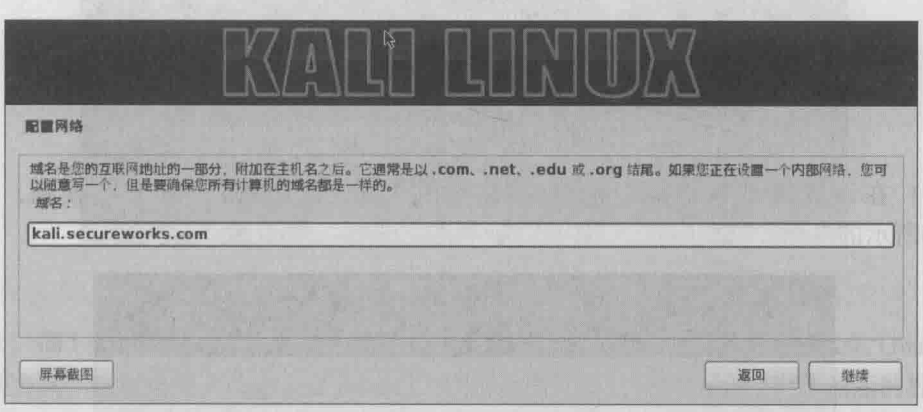


图 1－15　配置网络

（16）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，则可以不填写域名，直接单击“继续”按钮，将显示图 1－16所示的界面。

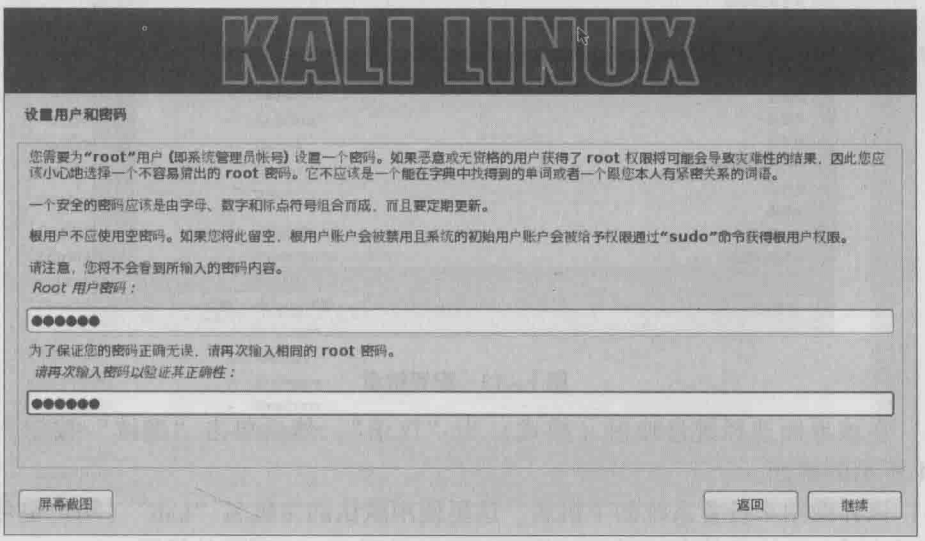


图 1－16　设置用户和密码