项目 5

基于 Kali Linux 的 Nmap

视频讲解

5.1 Kali Linux 简介

Kali Linux 是基于 Debian 的 Linux 发行版，用于数字取证操作系统，由 Offensive Security Ltd. 维护和资助，最先由 Offensive Security 的 Mati Aharoni 和 Devon Kearns 通过重写 BackTrack Linux 来完成，BackTrack Linux 是之前用于取证的 Linux 发行版，第一版于 2014 年 5 月 27 日发布。

Kali Linux 预装了许多渗透测试工具，包括信息收集、漏洞分析、Web 程序、数据库评估软件、密码攻击、无线攻击、逆向工程、漏洞利用工具集、嗅探工具、权限维持、数字取证、报告工具集等，为所有工具运行提供了一个稳定一致的操作系统基础。

5.2 Kali Linux 主要特性

Kali Linux 是 BackTrack Linux 完全遵循 Debian 开发标准的完整重建，创建了全新的目录框架，复查并打包所有工具，还为 VCS 建立了 Git 树。其具有以下特点。

(1) 超过 300 个渗透测试工具。复查了 BackTrack Linux 里的每一个工具之后，去掉了一部分已经无效或功能重复的工具。

(2) 永久免费。使用者无须为 Kali Linux 付费。

(3) 开源 Git 树。那些想调整或重建包的人可以浏览开发树得到所有源代码。

(4) 遵循 FHS。Kali 的开发遵循 Linux 目录结构标准，用户可以方便地找到命令文件、帮助文件、库文件等。

(5) 支持大量无线设备。尽可能地使 Kali Linux 支持更多的无线设备，能正常运行在各种各样的硬件上，能兼容大量 USB 和其他无线设备。

(6) 集成注入补丁的内核。作为渗透测试者或开发团队经常需要做无线安全评估，所用的内核包含了最新的注入补丁。

(7) 安全的开发环境。Kali Linux 开发团队由一群可信任的人组成，他们只能在使用多种安全协议的时候提交包或管理源。

(8) 包和源有 GPG 签名。每个开发者都会在编译和提交 Kali 的包时对它进行签名，并且源也会对它进行签名。

(9) 多语言。虽然渗透工具趋向于用英语，但为了确保 Kali 有多种语言支持，可以让

用户使用本国语言找到他们工作时需要的工具。

(10) 完全的可定制。不是每个人都赞同一致的设计,所以让更多有创新精神的用户能定制 Kali Linux(甚至定制内核)成他们喜欢的样子。

5.3　Kali Linux 安装

可到 Kali Linux 的官网下载安装文件,但速度较慢,到清华大学开源软件镜像站下载较快,如图 5.1 所示。选择任意安装版本均可,下载的是 kali-2020.4 目录下的 Kali-Linux-2020.4-live-i386.iso 文件。因为教学使用,所以在虚拟机下安装 Kali Linux,安装步骤如下。

图 5.1　下载网站

1. 新建虚拟机

(1) 虚拟机的安装比较简单,这里就不再叙述,在“虚拟机文件(F)”下新建虚拟机,选择“自定义(高级)(C)”单选按钮,如图 5.2 所示,单击“下一步”按钮。

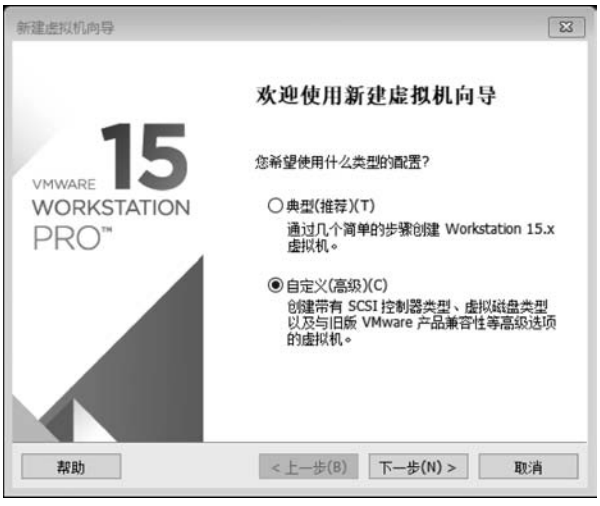

图 5.2　自定义安装

(2) 选择“稍后安装操作系统(S)”单选按钮,如图 5.3 所示,单击“下一步”按钮。

图 5.3 稍后安装操作系统

(3) 客户机操作系统选择“Linux(L)”,版本选择 Debian 7.x,如图 5.4 所示,单击“下一步”按钮。

图 5.4 操作系统的选择

(4) 定义虚拟机的名字和安装的位置,这里名字为 kali,安装到 F:\kali,如图 5.5 所示,单击“下一步”按钮。

(5) 分配虚拟机的内存,至少为 2GB,如图 5.6 所示,单击“下一步”按钮。

(6) 网络选择默认的 NAT 方式,如图 5.7 所示,单击“下一步”按钮。

图 5.5　定义名字和安装目录

图 5.6　定义内存

图 5.7　选择 NAT 方式

(7) 其他选择默认方式安装,指定磁盘大小为 50GB,将虚拟磁盘存储为单个文件,如图 5.8 所示,单击“下一步”按钮。

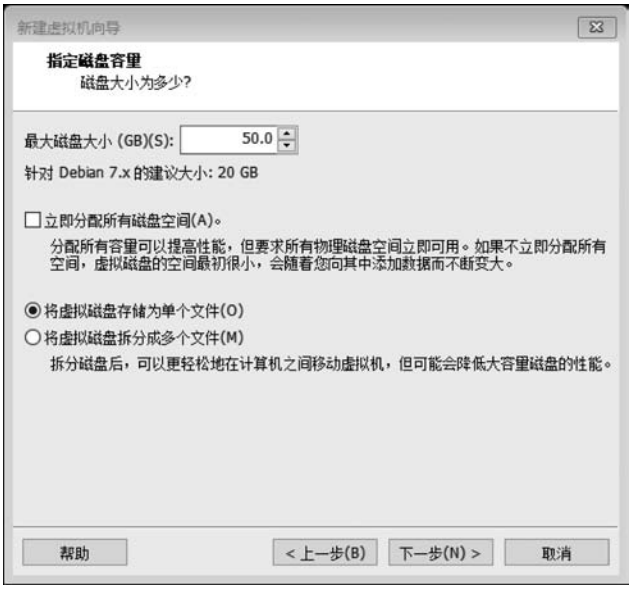

图 5.8 定义磁盘大小

(8) 指定 50GB 的磁盘文件存储的位置,存储到 F:\kali 下,文件名为 kali.vmdk,如图 5.9 所示,单击“下一步”按钮。

图 5.9 创建 Kali 的虚拟机文件

(9) 完成 Kali 虚拟机的创建,如图 5.10 所示,单击“完成”按钮。

(10) 创建完成后,在虚拟机的左面显示创建的虚拟机的名字 kali,如图 5.11 所示。

图 5.10　完成创建

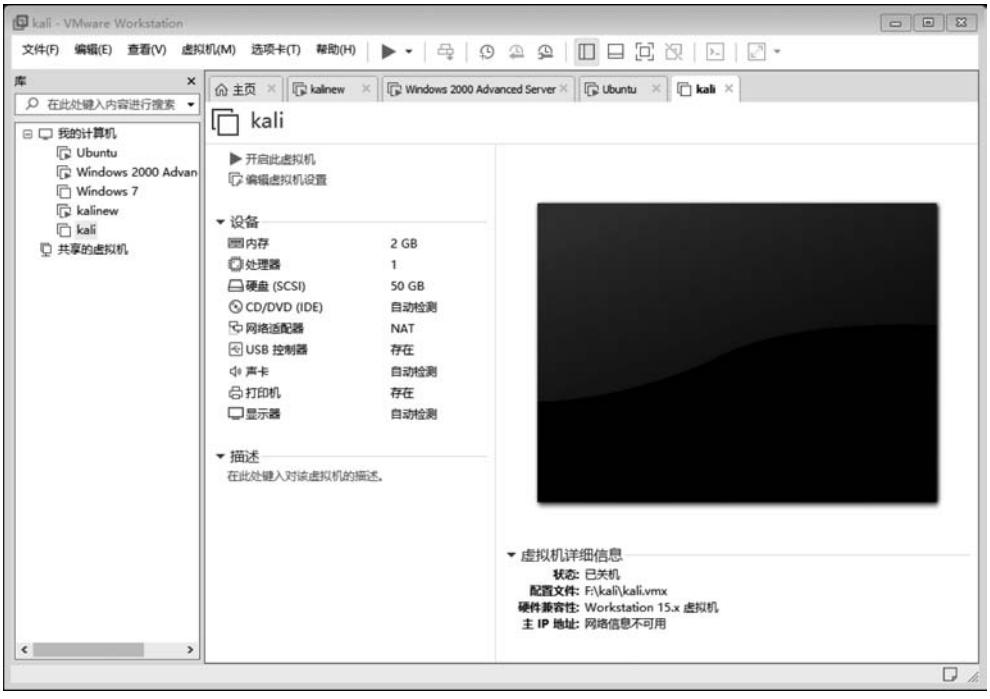

图 5.11　创建好的虚拟机 Kali

2. 安装 Kali Linux

(1) 单击对话框中部"设备"下的"CD/DVD(IDE)"选项,添加 kali-linux-2020.4-live-i386.iso 文件,如图 5.12 所示,单击"确定"按钮。

(2) 单击主界面下的绿色按钮,启动客户机操作系统,Kali 启动后的界面如图 5.13 所示,选择 Graphical install 选项,按回车键开始安装 Kali。

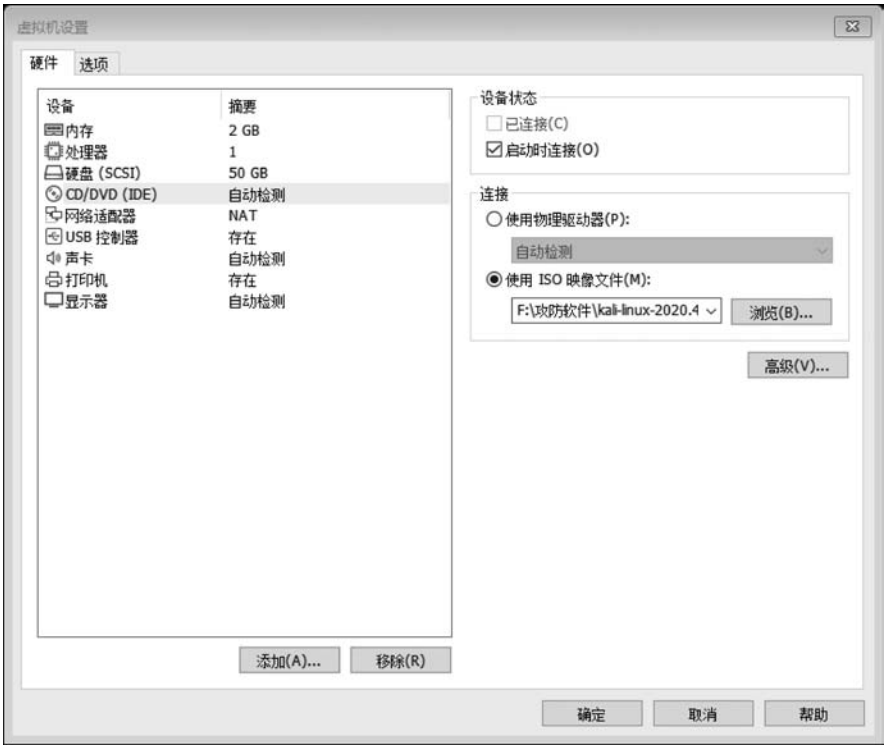

图 5.12　添加 Kali 映像文件

图 5.13　Kali 启动后的界面

（3）语言选择“中文(简体)”，如图 5.14 所示，单击 Continue 按钮。

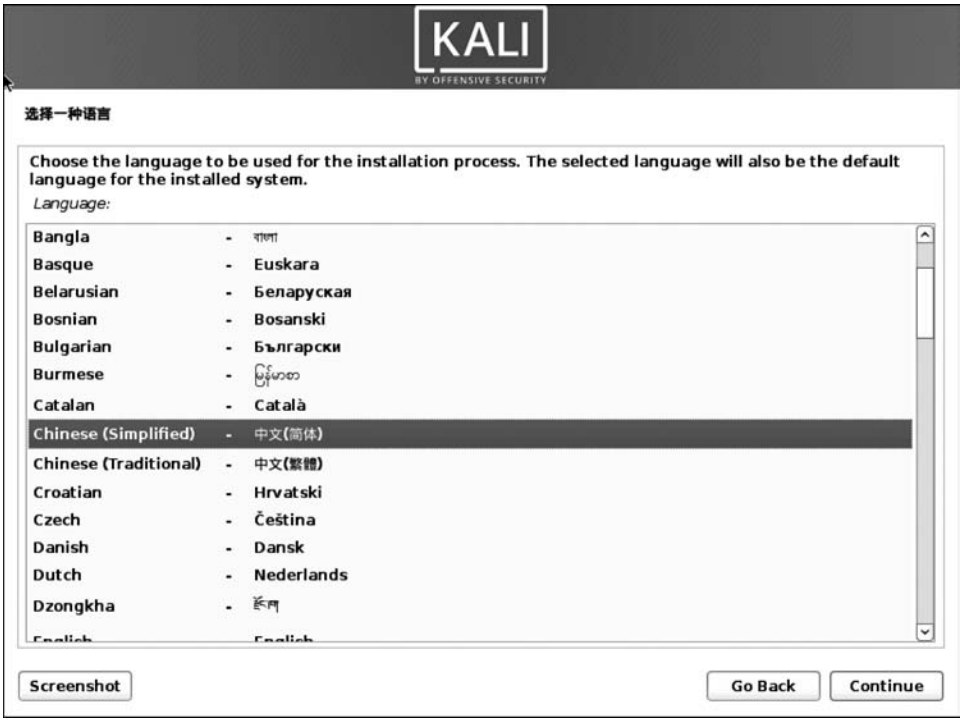

图 5.14　选择中文简体

（4）区域选择“中国”，如图 5.15 所示，单击“继续”按钮。

图 5.15　区域选择

(5) 键盘选择“汉语”,如图 5.16 所示,单击“继续”按钮。

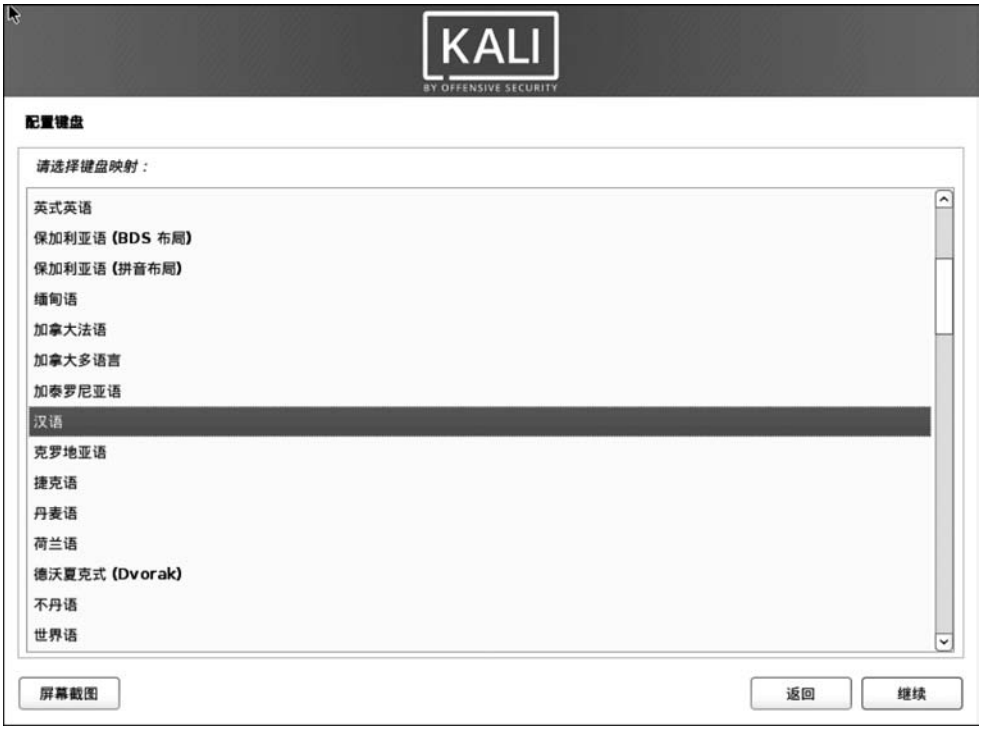

图 5.16 键盘的选择

(6) 定义主机名,此处为 kali,如图 5.17 所示,单击“继续”按钮。

图 5.17 定义主机名

（7）配置网络，此处域名为空白，如图 5.18 所示，单击“继续”按钮。

图 5.18　配置网络

（8）设置用户名，如图 5.19 所示，单击“继续”按钮。

图 5.19　设置用户名