

---

# 前 言

Kali Linux 是业内最知名的安全渗透测试专用操作系统。它的前身就是业界知名的 BackTrack 操作系统。BackTrack 在 2013 年停止更新，转为 Kali Linux。Kali Linux 集成了海量渗透测试、网络扫描、攻击等专用工具。通过系统更新，用户可以快速获取最新的各类工具。所以，Kali Linux 是专业人员的不二选择。

当今，由于无线网络使用方便，无线网络的应用非常广泛。并且无线网络的搭建也比较简单，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，因此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的漏洞，使得专业人员可以将其密码破解出来。

本教程就针对无线网络存在的安全问题，介绍了对各种加密方式实施渗透的方法，如 PIN、WEP、WPA/WPA2、WPA+RADIUS。通过对无线网络实施渗透，可以获取到无线网络的各种信息。本教程还介绍了使用 Wireshark 捕获无线网络的数据包，并进行分析。

## 1.学习所需的系统和软件

- 安装 Kali Linux 操作系统
- 大功率的 USB 无线网卡

## 2.学习建议

大家学习之前，可以致信到 xxxxxxxxxxxx，获取相关的资料 and 软件。如果大家在学习过程遇到问题，也可以将问题发送到该邮箱。我们尽可能给大家解决。

# 目 录

第 1 章	搭建渗透测试环境	1
1.1	什么是渗透测试	1
1.2	安装Kali Linux操作系统	2
1.2.1	在物理机上安装Kali Linux	2
1.2.2	在VMware Workstation上安装Kali Linux	14
1.2.3	安装VMware tools	18
1.2.4	升级操作系统	19
1.3	Kali Linux的基本配置	24
1.3.1	配置软件源	24
1.3.2	安装中文输入法	24
1.3.3	虚拟机中使用USB设备	26
第 2 章	WiFi网络的构成	30
2.1	WiFi网络概述	30
2.1.1	什么是WiFi网络	30
2.1.2	WiFi网络结构	30
2.1.3	WiFi工作原理	31
2.1.4	AP常用术语概述	31
2.2	802.11 协议概述	32
2.2.1	频段	32
2.2.2	使用WirelessMon规划频段	33
2.2.3	带宽	37
2.3	配置无线AP	38
2.3.1	在路由器上设置AP	38
2.3.2	在随身WiFi上设置AP	40
第 3 章	监听WiFi网络	43
3.1	网络监听原理	43
3.1.1	网卡的工作模式	43
3.1.2	工作原理	43
3.2	配置管理无线网卡	44
3.2.1	Linux支持的无线网卡	44
3.2.2	虚拟机使用无线网卡	46
3.2.3	设置无线网卡	46
3.3	设置监听模式	50
3.3.1	Aircrack-ng工具介绍	50
3.3.2	Aircrack-ng支持的网卡	51

3.3.3	启动监听模式 .....	52
3.4	扫描网络范围 .....	54
3.4.1	使用airodump-ng扫描 .....	54
3.4.2	使用Kismet扫描 .....	56
第 4 章	捕获数据包 .....	64
4.1	数据包简介 .....	64
4.1.1	握手包 .....	64
4.1.2	非加密包 .....	64
4.1.3	加密包 .....	64
4.2	使用Wireshark捕获数据包 .....	65
4.2.1	捕获非加密模式的数据包 .....	65
4.2.2	捕获WEP加密模式的数据包 .....	67
4.2.3	捕获WPA-PSK/WPA2-PSK加密模式的数据包 .....	72
4.3	使用伪AP .....	74
4.3.1	AP的工作模式 .....	74
4.3.2	创建伪AP .....	76
4.3.3	强制客户端下线 .....	81
4.3.4	捕获数据包 .....	81
第 5 章	分析数据包 .....	83
5.1	Wireshark简介 .....	83
5.1.1	捕获过滤器 .....	83
5.1.2	显示过滤器 .....	87
5.1.3	数据包导出 .....	90
5.1.4	在Packet List面板增加无线专用列 .....	94
5.2	使用Wireshark .....	98
5.2.1	802.11 数据包结构 .....	98
5.2.2	分析特定BSSID包 .....	101
5.2.3	分析特定的包类型 .....	102
5.2.4	分析特定频率的包 .....	103
5.3	分析无线AP认证包 .....	104
5.3.1	分析WEP认证包 .....	104
5.3.2	分析WPA认证包 .....	112
第 6 章	获取信息 .....	121
6.1	AP的信息 .....	121
6.1.1	AP的SSID名称 .....	121
6.1.2	AP的MAC地址 .....	123
6.1.3	AP工作的信道 .....	123
6.1.4	AP使用的加密方式 .....	124
6.2	客户端的信息 .....	126
6.2.1	客户端连接的AP .....	126
6.2.2	判断是否有客户端蹭网 .....	128

---

6.2.3	查看客户端使用的QQ号.....	131
6.2.4	查看手机客户端是否有流量产生.....	133
第7章	WPS加密模式.....	138
7.1	WPS简介.....	138
7.1.1	什么是WPS加密.....	138
7.1.2	WPS工作原理.....	138
7.1.3	WPS的漏洞.....	138
7.1.4	WPS的优点和缺点.....	139
7.2	设置WPS.....	139
7.2.1	开启WPS功能.....	139
7.2.1	在无线网卡上设置WPS加密.....	141
7.2.2	在移动客户端上设置WPS加密.....	147
7.3	破解WPS加密.....	153
7.3.1	使用Reaver工具.....	153
7.3.2	使用Wifite工具.....	156
7.3.3	使用Fern WiFi Cracker工具.....	158
第8章	WEP加密模式.....	161
8.1	WEP加密简介.....	161
8.1.1	什么是WEP加密.....	161
8.1.2	WEP工作原理.....	161
8.1.3	WEP漏洞分析.....	162
8.2	设置WEP加密.....	163
8.2.1	WEP加密认证类型.....	163
8.2.2	在AP中设置WEP加密模式.....	164
8.3	破解WEP加密.....	166
8.3.1	使用Aircrack-ng工具.....	166
8.3.2	使用Wifite工具破解WEP加密.....	169
8.3.3	使用Gerix WiFi Cracker工具破解WEP加密.....	170
8.4	应对措施.....	178
第9章	WPA加密模式.....	181
9.1	WPA加密简介.....	181
9.1.1	什么是WPA加密.....	181
9.1.2	WPA加密工作原理.....	182
9.1.3	WPA弥补了WEP的安全问题.....	182
9.2	设置WPA加密模式.....	183
9.2.1	WPA认证类型.....	183
9.2.2	加密算法.....	183
9.2.3	设置AP为WPA加密模式.....	184
9.3	创建密码字典.....	186
9.3.1	使用Crunch工具.....	186
9.3.2	使用pwgen工具.....	191

---

9.3.3	创建彩虹表 .....	192
9.4	破解WPA加密 .....	195
9.4.1	使用Aircrack-ng工具 .....	196
9.4.2	使用Wifite工具破解WPA加密 .....	199
9.4.3	不指定字典破解WPA加密 .....	200
9.5	WPA的安全措施 .....	201
第 10 章	WPA+RADIUS加密模式 .....	202
10.1	RADIUS简介 .....	202
10.1.1	什么是RADIUS协议 .....	202
10.1.2	RADIUS的工作原理 .....	202
10.2	搭建RADIUS服务 .....	203
10.2.1	安装RADIUS服务 .....	203
10.2.2	配置文件介绍 .....	206
10.3	设置WPA+RADIUS加密 .....	208
10.3.1	配置RADIUS服务 .....	208
10.3.2	配置MySQL数据库服务 .....	210
10.3.3	配置WiFi网络 .....	213
10.4	连接RADIUS加密的WiFi网络 .....	214
10.4.1	在Windows下连接RADIUS加密的WiFi网络 .....	215
10.4.2	在Linux下连接RADIUS加密的WiFi网络 .....	220
10.4.3	移动客户端连接RADIUS加密的WiFi网络 .....	222
10.5	破解RADIUS加密的WiFi网络 .....	223
10.5.1	使用hostapd-wpe创建伪AP .....	223
10.5.2	Kali Linux的问题处理 .....	227
10.5.3	使用asleap破解密码 .....	228
10.6	WPA+RADIUS的安全措施 .....	228

# 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。安全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。

渗透测试与其它评估方法不同。通常的评估方法是根据已知信息资源或其它被评估对象，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通过探测获取目标系统的系统。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。

□ 渗透测试是选择一个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、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 1.0.9a。下载界面如图 1.1 所示。

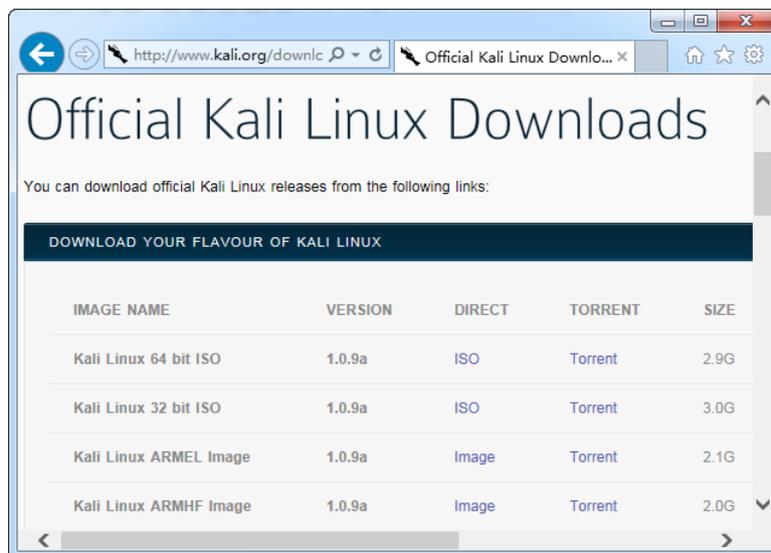


图 1.1 Kali Linux ISO 文件下载界面

从该界面可以看到，Kali Linux 目前最新的版本是 1.0.9a，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 Linux 1.0.5 的内核中才支持。为了使用户更好的使用该工具，本书将介绍安装 Kali Linux 1.0.5 操作系统。然后，升级到最新版 1.0.9a。

这样可以保留 1.0.5 操作系统的内核，也就可以很好的使用 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。

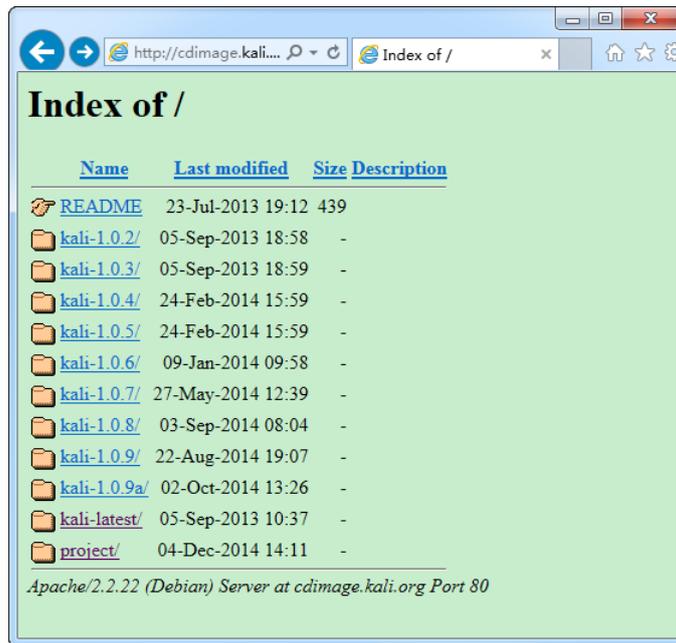


图 1.2 Kali 操作系统的下载页面

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，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 Linux 1.0.5 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

(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）选项，将显示如图 1.5 所示的界面。

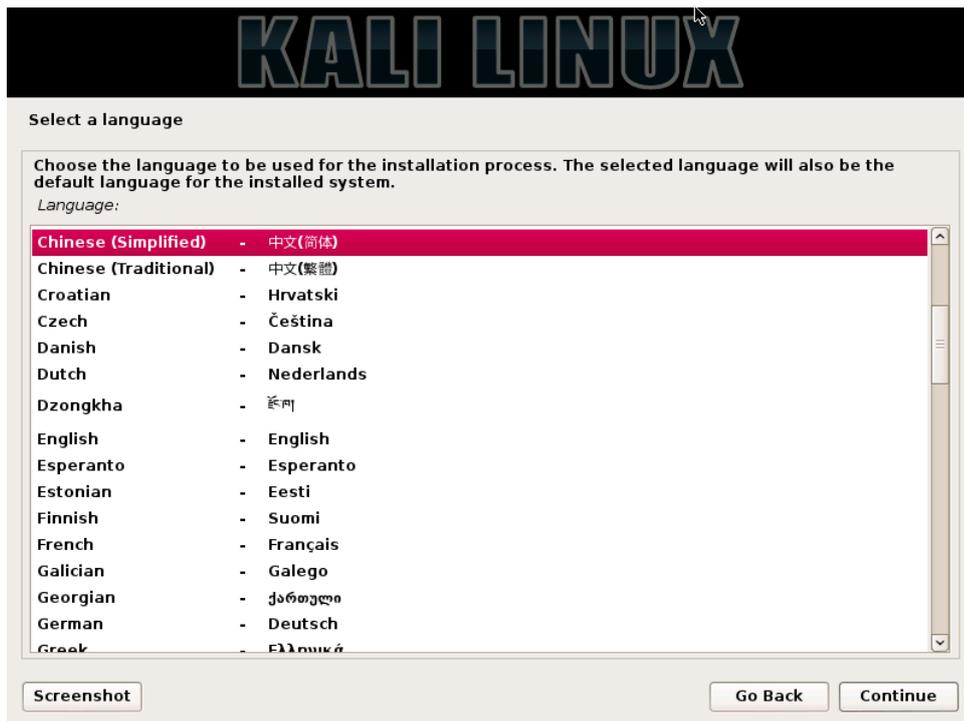


图 1.5 选择语言

(3) 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。

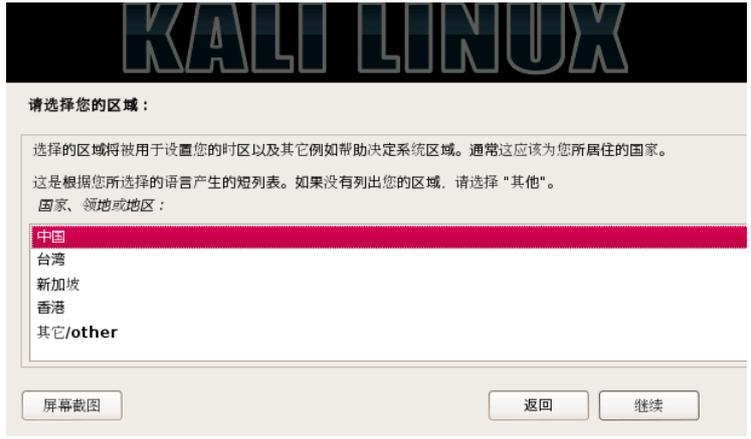


图 1.6 选择区域

(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，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。

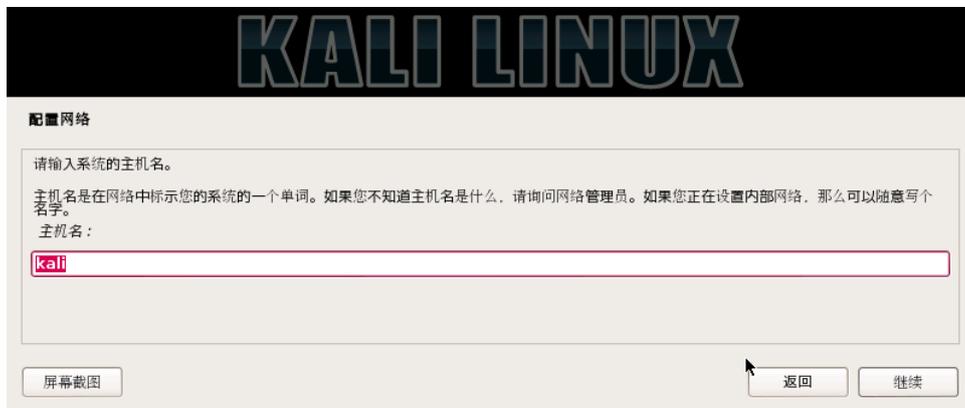


图 1.9 设置主机名

(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

(9) 该界面用来设置计算机使用的域名，用户也可以不设置。这里使用默认提供的域名 localdomain，然后单击“继续”按钮，将显示如图 1.11 所示的界面。

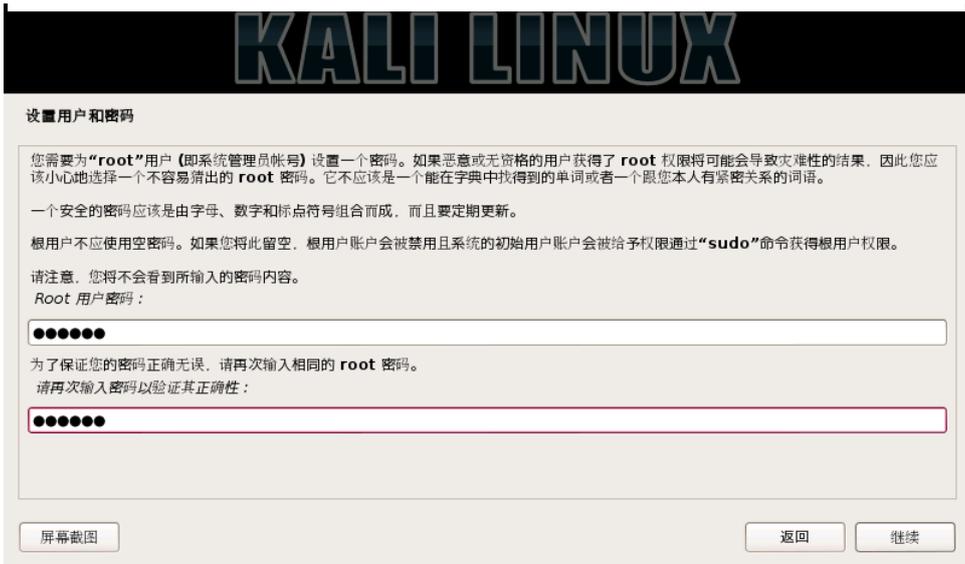


图 1.11 设置用户名和密码

(10) 该界面用来设置根 root 用户的密码。为了安全起见，建议设置一个比较复杂点的密码。设置完成后单击“继续”按钮，将显示如图 1.12 所示的界面。



图 1.12 磁盘分区

(11) 该界面用来选择分区方法。这里选择“使用整个磁盘”选项，然后单击“继续”按钮，将显示如图 1.13 所示的界面。



图 1.13 选择要分区的磁盘

(12) 在该界面选择要分区的磁盘。当前系统中只有一块磁盘，所有这里选择这一块就可以了。然后单击“继续”按钮，将显示如图 1.14 所示的界面。



图 1.14 选择分区方案

(13) 在该界面选择分区方案，默认提供了三种方案。这里选择“将所有文件放在同一个分区中（推荐新手使用）”选项，然后单击“继续”按钮，将显示如图 1.15 所示的界面。

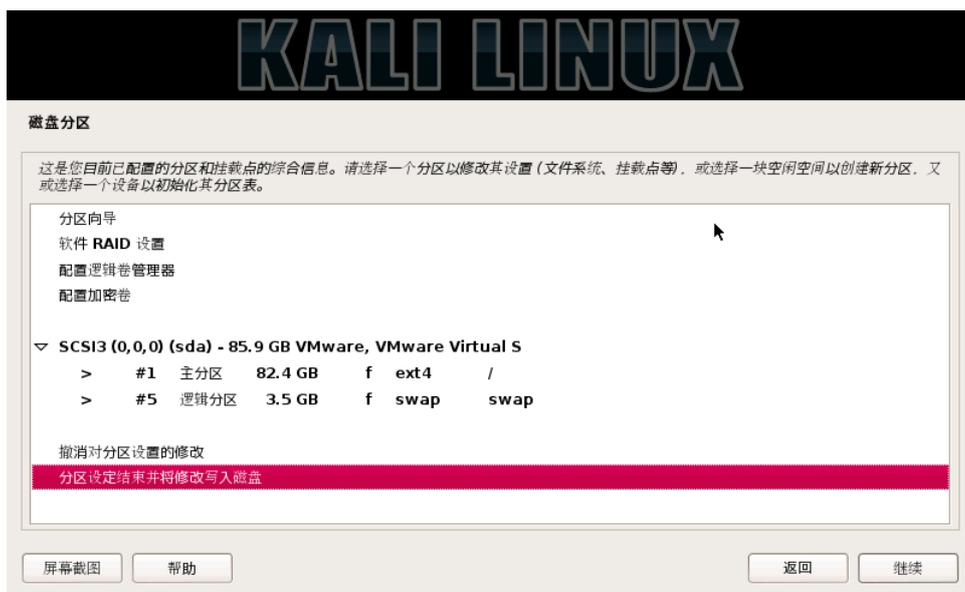


图 1.15 分区情况

(14) 该界面显示了当前系统的分区情况。从该界面可以看到目前分了两个区，分别是根分区和 SWAP 分区。如果用户想修改目前的分区，选择“撤销对分区设置的修改”选项，重新进行分区。如果不进行修改，则选择“分区设定结束并将修改写入磁盘”选项。然后单击“继续”按钮，将显示如图 1.16 所示的界面。



图 1.16 格式化分区

(15) 在该界面提示是否要将改动写入磁盘，也就是对磁盘进行格式化。这里选择“是”复选框，然后单击“继续”按钮，将显示如图 1.17 所示的界面。



图 1.17 安装系统

(16) 此时，开始安装系统。在安装过程中需要设置一些信息，如设置网络镜像，如图 1.18 所示。如果安装 Kali Linux 系统的计算机没有连接到网络的话，在该界面选择“否”复选框，然后单击“继续”按钮。这里选择“是”复选框，将显示如图 1.19 所示的界面。

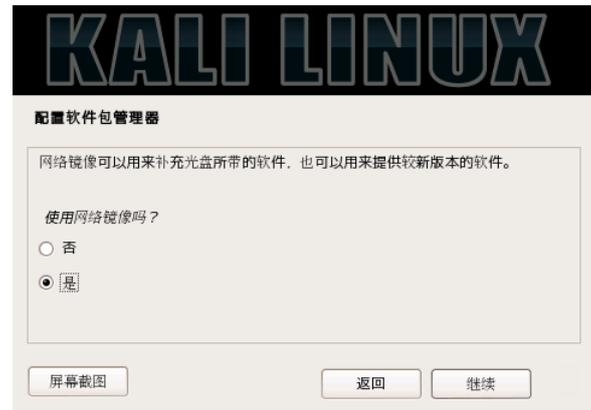




图 1.18 配置软件包管理器

图 1.19 设置 HTTP 代理

(17) 在该界面设置 HTTP 代理的信息。如果不需要通过 HTTP 代理来连接到外部网络的话，直接单击“继续”按钮，将显示如图 1.20 所示的界面。



图 1.20 配置软件包管理器

(18) 该界面显示正在配置软件包管理器。配置完成后，将显示如图 1.21 所示的界面。



图 1.21 将 GRUB 启动引导器安装到主引导记录 (MBR) 上吗?

(19) 在该界面提示是否将 GRUB 启动引导器安装到主引导记录 (MBR) 上吗? 这里选择“是”复选框。然后单击“继续”按钮, 将显示如图 1.22 所示的界面。



图 1.22 将 GRUB 安装至硬盘

(20) 此时将继续进行安装, 安装完 GRUB 后, 将显示如图 1.23 所示的界面。



图 1.23 操作系统安装完成

(21) 从该界面可以看到操作系统已经安装完成。接下来, 需要重新启动进行操作系统了。所以, 单击“继续”按钮, 结束安装进程, 并重新启动操作系统, 如图 1.24 所示。



图 1.24 结束安装进程

(22) 从该界面可以看到正在结束安装进程。当安装进程结束后, 将自动重新启动并进行操作系统。成功启动系统后, 将显示如图 1.25 所示的界面。

(23) 在该界面选择登录的用户名。由于在安装操作系统过程中没有创建任何用户, 所以这里仅显示了“其他”文本框。此时单击“其他”选项, 将显示如图 1.26 所示的界面。

(24) 在该界面输入登录系统的用户名。这里输入超级用户 root, 然后单击“登录”按钮, 将显示如图 1.27 所示的界面。



图 1.25 登录系统



图 1.26 输入用户名



图 1.27 输入登录用

户的密码

(25) 在该界面输入超级用户 root 的密码，该密码就是在安装操作系统过程中设置的密码。输入密码后，单击“登录”按钮。如果成功登录系统后，将看到如图 1.28 所示的界面。



图 1.28 登录系统的界面

(26) 当看到该界面时，表示 root 用户成功登陆了系统。此时，就可以在该操作系统

中实施 WiFi 渗透测试了。

## 2.使用 U 盘安装 Kali Linux

当用户在物理机安装操作系统时，如果没有光驱的话，就可以使用 U 盘来实现。并且使用光盘安装时，也没有使用 U 盘安装的速度快。下面将介绍如果使用 U 盘安装 Kali Linux。在使用 U 盘安装 Kali Linux 之前，需要做几个准备工作。如下所示：

- ❑ 准备一个最少 4GB 的优盘。
- ❑ 下载 Kali Linux 的 ISO 文件。
- ❑ 下载一个将 ISO 文件写到 U 盘的实用工具，这里使用名为 Win32 Disk Imager 的工具。

将以上工作准备好后，就可以安装 Kali Linux 操作系统了。如下所示：

(1) 将准备的优盘插入到一台主机上，然后启动 Win32 Disk Imager 工具，将显示如图 1.29 所示的界面。

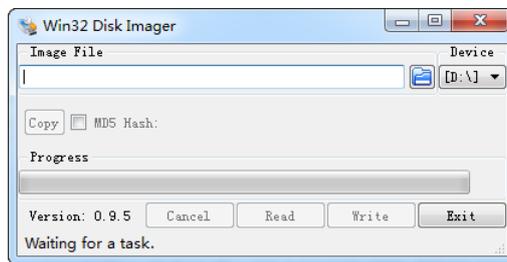


图 1.29 Win32 Disk Imager 启动界面

(2) 在该界面单击  图标，选中 kali Linux 的 ISO 文件，将显示如图 1.30 所示的界面。

(3) 此时，在该界面单击 Write 按钮，将显示如图 1.31 所示的界面。

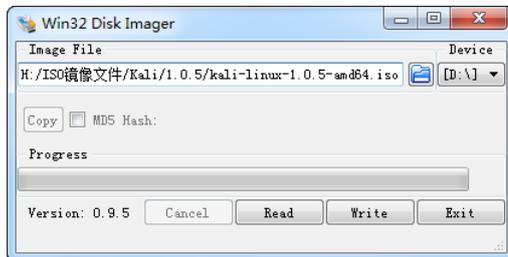


图 1.30 加载 ISO 文件

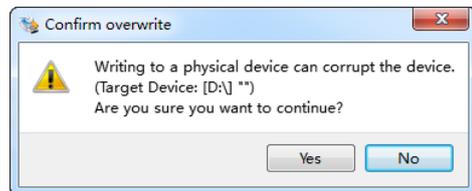


图 1.31 确认写入数据到目标设备

(4) 该界面提示是否确定要将数据写入到 D 设备吗？这里单击 Yes 按钮，将显示如图 1.32 所示的界面。

(5) 从该界面可以看到正在向目标设备写入数据。写入完成后，将显示如图 1.33 所示的界面。

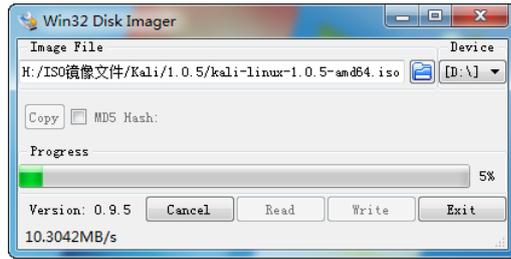


图 1.32 开始写入数据

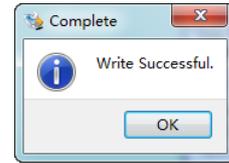


图 1.33 成功写入数据

(6) 从该界面可以看到在目标设备上成功写入数据。此时单击 OK 按钮，将返回到如图 1.30 所示的界面。然后单击 Exit 按钮，关闭 Win32 Disk Imager 工具。然后，将插入的 U 盘弹出。

(7) 现在，将刚才写入 ISO 文件内容的 U 盘插入到安装 Kali Linux 系统的计算机上。启动系统设置 BIOS 以优盘为第一启动项，然后保存 BIOS 设置并重新启动系统后，将显示如图 1.34 所示的界面。

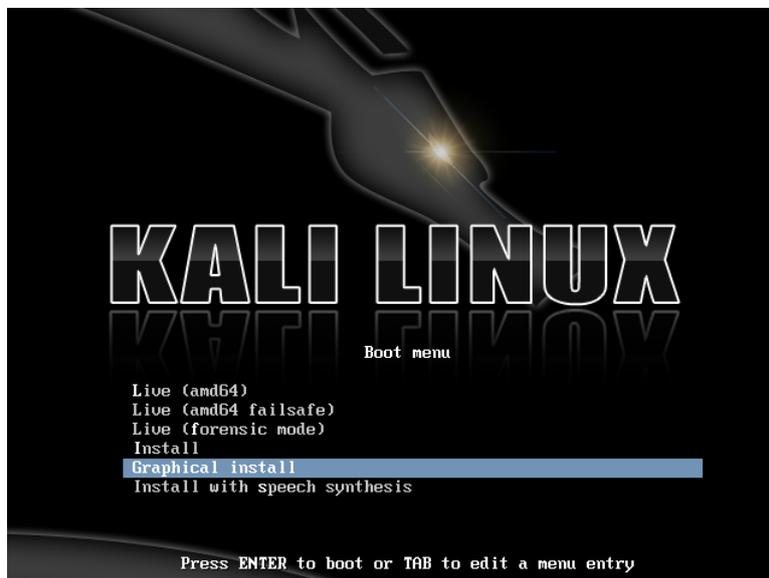


图 1.34 安装界面

(8) 该界面就是 Kali Linux 的安装界面。这时候的安装方法，和前面的安装方法相同，这里不再介绍。

## 1.2.2 在 VMware Workstation 上安装 Kali Linux

VMware Workstation 是一款功能强大的桌面虚拟计算机软件。该软件允许用户在单一的桌面上同时运行不同的操作系统，并且可以进行开发、测试、部署新的应用程序等。VMware Workstation 可在一部实体机器上模拟完整的网络环境，以及可便于携带的虚拟机器。当用户没有合适的物理机可以安装操作系统时，在 VMware Workstation 上安装操作系统是一个不错的选择。在渗透测试时，往往需要多个目标主机作为靶机，并且是不可缺少的。所以，用户可以在 VMware Workstation 上安装不同的操作系统。下面将介绍在 VMware Workstation 上安装 Kali Linux 操作系统。

(1) 下载 VMware Workstation 软件，其下载地址为

<https://my.vmware.com/cn/web/vmware/downloads>。该软件目前最新的版本是 10.0.4，下载界面如图 1.35 所示。

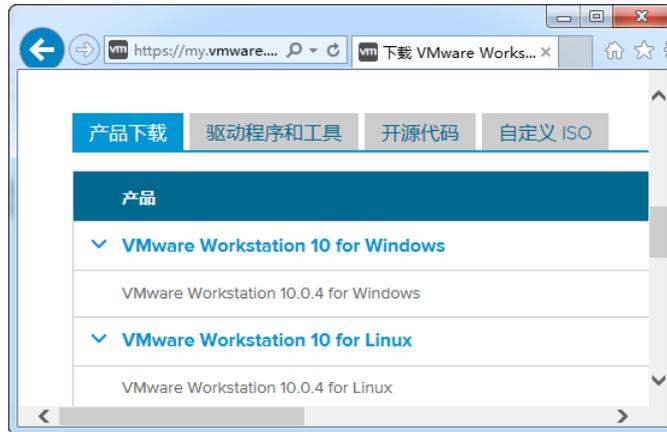


图 1.35 下载 VMware Workstation

(2) 从该界面可以看到，VMware Workstation 可以安装在 Windows 和 Linux 系统中。本书选择将该软件安装到 Windows 操作系统，所以选择下载 VMware Workstation 10 for Windows。下载完后，通过双击下载的软件名根据提示进行安装。该软件的安装方法比较简单，这里不进行讲解。

(3) 启动 VMware Workstation，将显示如图 1.36 所示的界面。



图 1.36 VMware Workstation 启动界面

(4) 从该界面可以看到，有六个图标可以点击。这里单击“创建新的虚拟机”图标，将显示如图 1.37 所示的界面。

(5) 从该界面可以看到，显示了两种安装类型，分别是“典型”和“自定义”。如果使用“自定义”类型安装的话，用户还需要手动设置其它配置。这里推荐使用“典型”的类型，然后单击“下一步”按钮，将显示如图 1.38 所示的界面。



图 1.37 新建虚拟机向导



图 1.38 安装客户机操作系统

(6) 该界面选择安装客户机操作系统的方式。从该界面可以看到，提供了三种方法。这里选择使用“稍后安装操作系统(S)”选项，然后单击“下一步”按钮，将显示如图 1.39 所示的界面。

(7) 在该界面选择安装的操作系统和版本。这里选择 Linux 操作系统，版本为“其它 Linux 3.X 内核 64 位”，然后单击“下一步”按钮，将显示如图 1.40 所示的界面。



图 1.39 选择客户机操作系统

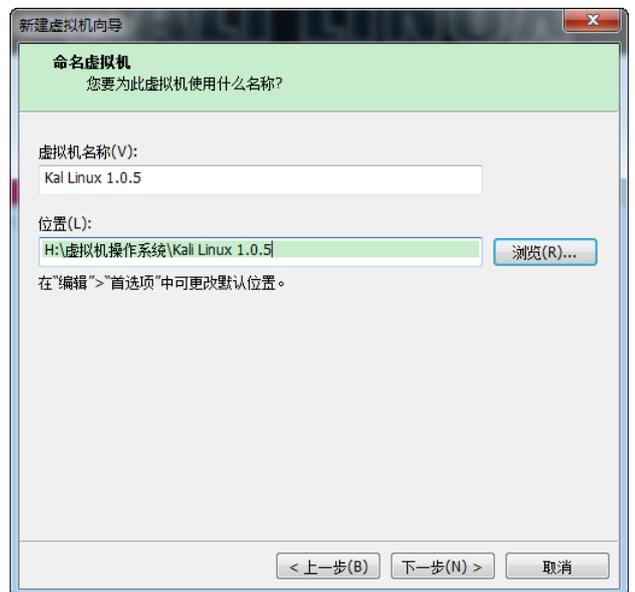


图 1.40 命名虚拟机

(8) 在该界面为虚拟机创建一个名称，并设置虚拟机的安装位置。设置完成后，单击“下一步”按钮，将显示如图 1.41 所示的界面。

(9) 在该界面设置磁盘的容量。如果当前主机有足够大的磁盘时，建议设置的磁盘容量大点，避免造成磁盘容量不足。这里设置为 80GB，然后单击“下一步”按钮，将显示如图 1.42 所示的界面。



图 1.41 指定磁盘容量

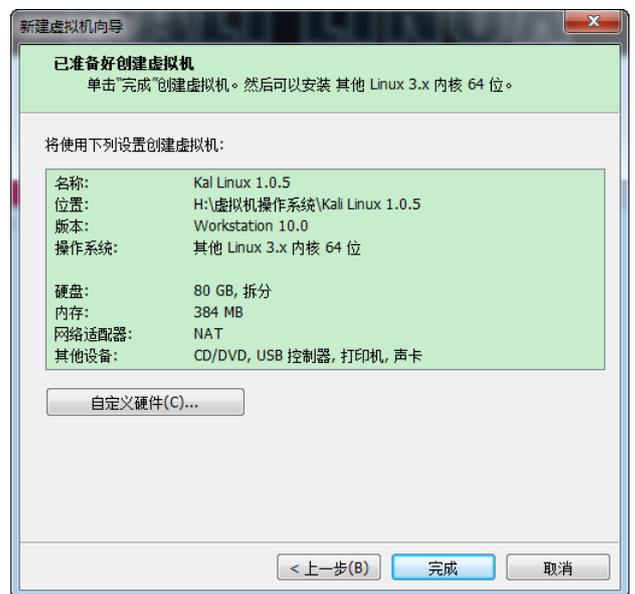


图 1.42 已准备好创建虚拟机

(10) 该界面显示了所创建虚拟机的详细信息，此时就可以创建操作系统了。然后单击“完成”按钮，将显示如图 1.43 所示的界面。

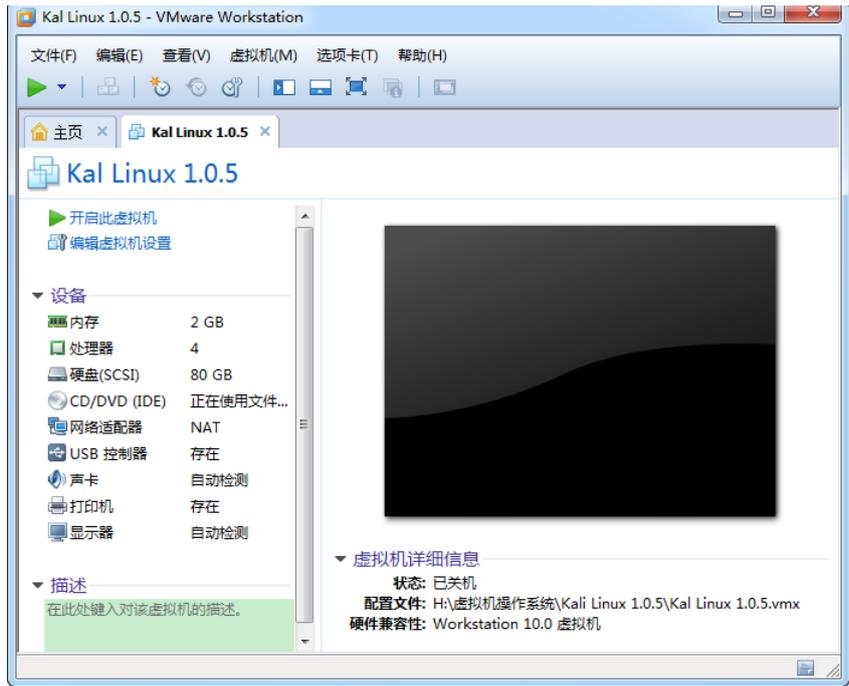


图 1.43 创建虚拟机

(11)该界面显示了新创建的虚拟机的详细信息。接下来就可以准备安装 Kali Linux1.0.5 操作系统了。但是，在安装 Kali Linux 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”，将显示如图 1.44 所示的界面。

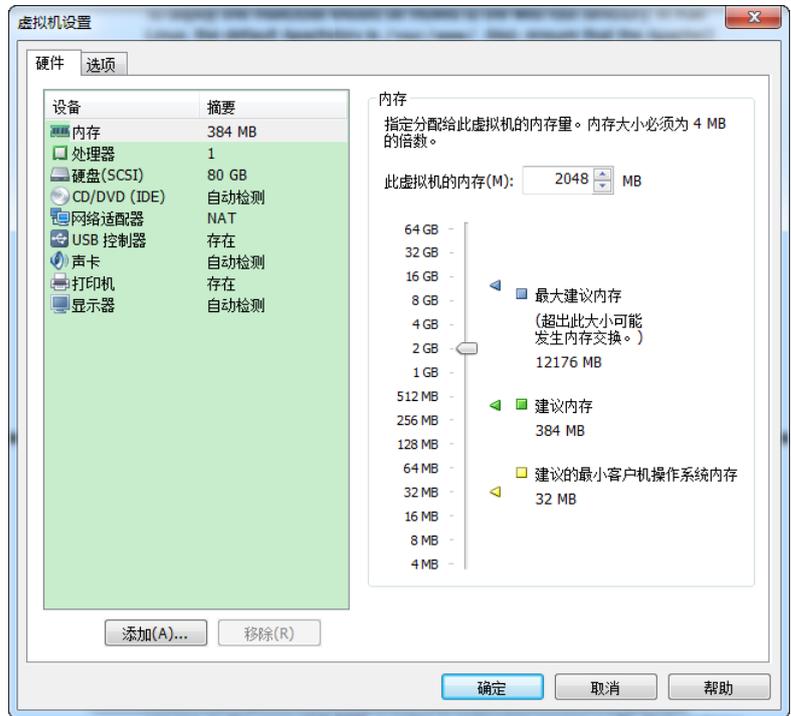


图 1.44 虚拟机设置

(12) 在该界面可以设置内存、处理器、网络适配器等。将这些硬件配置好后，选择“CD/DVD (IDE)”选项，将显示如图 1.45 所示的界面。

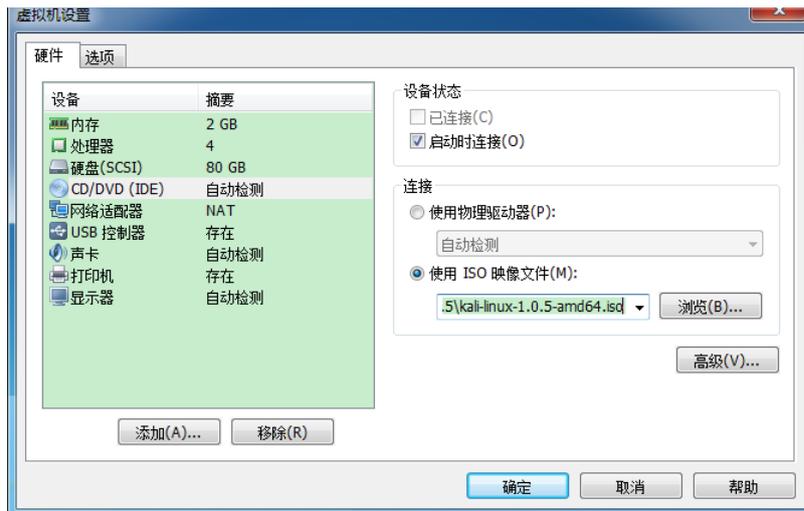


图 1.45 选择 ISO 映像文件

(13) 在该界面的右侧选择“使用 ISO 映像文件”复选框，并单击“浏览”按钮，选择 Kali Linux 1.0.5 的映像文件。然后单击“确定”按钮，将返回到图 1.43 所示的界面。此时，就可以开始安装 Kali Linux 操作系统。

(14) 在图 1.43 中单击“开启此虚拟机”命令，将显示一个新的窗口，如图 1.46 所示。



图 1.46 安装界面

(15) 此时，就可以在 VMware Workstation 上安装 Kali Linux 操作系统了。

### 1.2.3 安装 VMware tools

VMware Tools 是 VMware 虚拟机中自带的一种增强工具。它是 VMware 提供的增强虚拟显卡和硬盘性能，以及同步虚拟机与主机时钟的驱动程序。只有在 VMware 虚拟机中安装好 VMware Tools 工具，才能实现主机与虚拟机之间的文件共享，同时可支持自由拖拽的功能，鼠标也可在虚拟机与主机之间自由移动（不用再按 Ctrl+Alt）。下面将介绍安装 VMware Tools 的方法。

(1) 在 VMware Workstation 菜单栏中，依次选择“虚拟机”|“安装 VMware Tools...”命令，如图 1.47 所示。

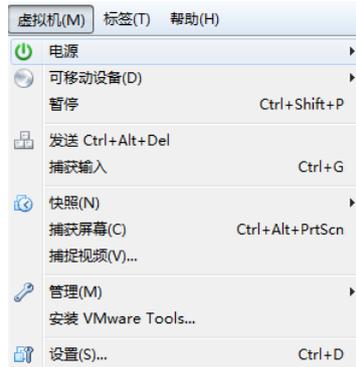


图 1.47 安装 VMware Tools

(2) 挂载 VMware Tools 安装程序到/mnt/cdrom/目录。执行命令如下所示：

```
root@kali:~# mkdir /mnt/cdrom/ #创建挂载点
root@kali:~# mount /dev/cdrom /mnt/cdrom/ #挂载安装程序
mount: block device /dev/sr0 is write-protected, mounting read-only
```

看到以上的输出信息，表示 VMware Tools 安装程序挂载成功了。

(3) 切换到挂载位置，解压安装程序 VMwareTools。执行命令如下所示：

```
root@kali:~# cd /mnt/cdrom/ #切换目录
root@kali:/mnt/cdrom# ls #查看当前目录下的文件
manifest.txt    VMwareTools-9.6.1-1378637.tar.gz  vmware-tools-upgrader-64
run_upgrader.sh  vmware-tools-upgrader-32
root@kali:/mnt/cdrom# tar zxvf VMwareTools-9.6.1-1378637.tar.gz -C /usr #解压 VMwareTools 安装程序
```

执行以上命令后，VMwareTools 程序将被解压到/usr 目录中，并生成一个名为 vmware-tools-distrib 文件夹。

(4) 切换到 VMwareTools 的目录，并运行安装程序。执行命令如下所示：

```
root@kali:/mnt/cdrom# cd /usr/vmware-tools-distrib/ #切换目录
root@kali:/usr/vmware-tools-distrib# ./vmware-install.pl #运行安装程序
```

执行以上命令后，会出现一些问题。这时按下“回车”键，接受默认值即可。如果当前系统中没有安装 Linux 内核头文件的话，在安装时出现以下问题时，应该输入 no。如下所示：

```
Enter the path to the kernel header files for the 3.14-kali1-amd64 kernel?
The path " " is not a valid path to the 3.14-kali1-amd64 kernel headers.
Would you like to change it? [yes] no
```

在以上输出的信息中，输入 no 后，将继续安装 VMware tools。如果在以上问题中按下回车键的话，将无法继续安装。

(5) 重新启动计算机。然后，虚拟机和物理机之间就可以实现复制、粘贴等操作。

## 1.2.4 升级操作系统

由于 Linux 是一个开源的系统，所以每天可能都会有新的软件出现。而且 Linux 发行套件和内核也在不断更新。这样通过对 Linux 进行软件包进行更新，就可以马上使用最新的软件。如果当前系统的版本较低时，通过更新软件可以直接升级到最新版操作系统。下面将介

绍如何更新操作系统。

在 Kali Linux 中，用户可以在命令行终端或图形界面两种方法来实施升级操作系统。下面分别介绍这两种方法。

### 1. 图形界面升级操作系统

在前面安装的操作系统版本是 1.0.5，下面将通过更新软件包的方法来升级操作系统。具体操作步骤如下所示：

(1) 查看当前操作系统的版本及内核。执行命令如下所示：

```
root@kali:~# cat /etc/issue          #查看操作系统的版本
Kali GNU/Linux 1.0 \n \l
root@kali:~# uname -a              #查看内核信息
Linux kali 3.7-trunk-amd64 #1 SMP Debian 3.7.2-0+kali8 x86_64 GNU/Linux
```

从输出的信息中，可以看到当前系统的版本为 1.0，内核为 3.7。

(2) 在图形界面依次选择“应用程序”|“系统工具”|“软件更新”命令，将显示如图 1.48 所示的界面。

(3) 该界面提示确认是否要以特权用户身份运行该应用程序。这里单击“确认继续”按钮，将显示如图 1.49 所示的界面。

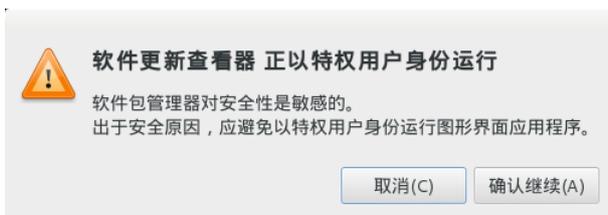


图 1.48 警告信息



图 1.49 软件更新

(4) 该界面显示了总共有 78 个软件包需要更新，单击“安装更新”按钮，将显示如图 1.50 所示的界面。

(5) 该界面显示了安装更新软件包依赖的软件包，单击“继续按钮”，将显示如图 1.51 所示的界面。



图 1.50 依赖软件包



图 1.51 软件更新过程

(6) 从该界面可以看到软件更新的一个进度。在该界面，可以看到各软件包的一个不同状态。其中，软件包后面出现图标，表示该软件包正在下载；如果显示为图标，表示软件包已下载；如果显示为图标，表示已准备等待安装；当下载好的软件包安装成功后，将显示为图标。如果同时出现和图标的话，表示安装完该软件包后，需要重新启动系统；在以上更新过程中，未下载的软件包会自动跳到第一列。此时，滚动鼠标是无用的。

(7) 当以上所有软件更新完，将弹出如图 1.52 所示的界面。

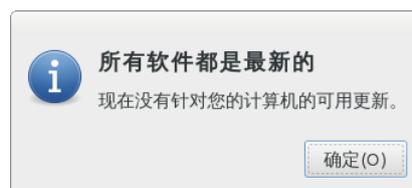


图 1.52 软件更新完成

(8) 从该界面可以看到，提示所有软件都是最新的。此时，单击“确定”按钮，将自

动退出软件更新程序。

(9) 这时候再次查看当前操作系统的版本及内核，将显示如下所示的信息：

```
root@kali:~# cat /etc/issue          #查看操作系统的版本
Kali GNU/Linux 1.0.9 \n \l
root@kali:~# uname -a              #查看内核信息
Linux kali 3.7-trunk-amd64 #1 SMP Debian 3.7.2-0+kali8 x86_64 GNU/Linux
```

从输出的信息中，可以看到当前系统的操作版本已经升级为 1.0.9，内核仍然为 3.7。这表明虽然通过更新软件包升级了操作系统的版本，但是原来的内核仍然保留。当用户重新启动系统时，将会发现有两个内核。这时候用户可以选择任意一个内核来启动系统，如图 1.53 所示。



图 1.53 选择启动系统的内核

从该界面可以看到升级后操作系统的内核是 3.14。用户不管选择哪个内核启动操作系统，操作系统的版本都 1.0.9，只是使用的内核不同。如选择使用 3.14 内核启动操作系统，启动后查看系统的版本和内核信息。显示结果如下所示：

```
root@kali:~# cat /etc/issue
Kali GNU/Linux 1.0.9 \n \l
root@kali:~# uname -a
Linux kali 3.14-kali1-amd64 #1 SMP Debian 3.14.5-1kali1 (2014-06-07) x86_64 GNU/Linux
```

从以上输出信息，可以看到该系统的版本是 1.0.9，内核为 3.14。

## 2. 命令行终端升级操作系统

在 Kali Linux 中提供了两个命令 `update` 和 `dist-upgrade`，它们分别对软件包进行更新或升级。这两个命令的区别如下所示：

- ❑ `update`: 更新软件列表信息。包括版本、依赖关系等。
- ❑ `dist-upgrade`: 会改变配置文件，改变旧的依赖关系，升级操作系统等。

【实例 1-1】使用 `update` 命令更新软件包列表。执行命令如下所示：

```
root@kali:~# apt-get update
执行以上命令后，将输出如下所示的信息：
获取：1 http://security.kali.org kali/updates Release.gpg [836 B]
获取：2 http://http.kali.org kali Release.gpg [836 B]
获取：3 http://security.kali.org kali/updates Release [11.0 kB]
获取：4 http://http.kali.org kali Release [21.1 kB]
```

```

获取： 5 http://security.kali.org kali/updates/main amd64 Packages [219 kB]
获取： 6 http://http.kali.org kali/main Sources [7,545 kB]
忽略 http://security.kali.org kali/updates/contrib Translation-zh_CN
忽略 http://security.kali.org kali/updates/contrib Translation-zh
忽略 http://security.kali.org kali/updates/contrib Translation-en
忽略 http://security.kali.org kali/updates/main Translation-zh_CN
忽略 http://security.kali.org kali/updates/main Translation-zh
忽略 http://security.kali.org kali/updates/main Translation-en
忽略 http://security.kali.org kali/updates/non-free Translation-zh_CN
命中 http://http.kali.org kali/contrib Sources
获取： 8 http://http.kali.org kali/main amd64 Packages [8,450 kB]
获取： 9 http://http.kali.org kali/non-free amd64 Packages [128 kB]
命中 http://http.kali.org kali/contrib amd64 Packages
下载 16.5 MB，耗时 4 分 53 秒 (56.2 kB/s)
正在读取软件包列表... 完成

```

以上输出的信息，就是更新 Kali Linux 系统软件包列表的一个过程。从以上输出信息中，可以发现在链接前的表示方法不同，包括获取、忽略和命中三种状态。其中，获取表示有更新并且正在下载；忽略表示无更新或者更新无关紧要，或者不需要；命中表示链接到该网站。

**【实例 1-2】**使用 `dist-upgrade` 命令将当前的操作系统进行升级。执行命令如下所示：

```

root@kali:~# apt-get dist-upgrade
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
正在对升级进行计算... 完成
下列软件包将被【卸载】：
  beef-xss-bundle
下列【新】软件包将被安装：
  hashid libhttp-parser2.1 python3 python3-minimal python3.2 python3.2-minimal
  ruby-ansi ruby-atomic ruby-buftok ruby-dataobjects ruby-dataobjects-mysql
  ruby-dataobjects-postgres ruby-dataobjects-sqlite3 ruby-dm-core
  ruby-dm-do-adapter ruby-dm-migrations ruby-dm-sqlite-adapter
  ruby-em-websocket ruby-equalizer ruby-execjs ruby-faraday ruby-http
  ruby-http-parser.rb ruby-librex ruby-libv8 ruby-memoizable
  ruby-msfrpc-client ruby-multipart-post ruby-naught ruby-parseconfig ruby-ref
  ruby-rubyzip ruby-simple-oauth ruby-therubyracer ruby-thread-safe
  ruby-twitter ruby-uglifier
下列软件包将被升级：
  apt apt-utils automater beef-xss chkrootkit dbus dbus-x11 dnsrecon dpkg
  dpkg-dev exploitdb ghost-phisher gnupg gpgv iceweasel iodine kali-linux
  kali-linux-full kali-linux-sdr kali-menu libapache2-mod-php5 libapt-inst1.5
  libapt-pkg4.12 libavcodec53 libavdevice53 libavformat53 libavutil51
  libdbus-1-3 libdpkg-perl libgnutls-openssl27 libgnutls26 libmozjs24d
  libpostproc52 libssl-dev libssl-doc libssl1.0.0 libswscale2
  linux-image-3.14-kali1-amd64 linux-libc-dev metasploit metasploit-framework
  mitmproxy openssl php5 php5-cli php5-common php5-mysql python-lxml
  python-scapy recon-ng responder ruby-eventmachine ruby-json ruby-msgpack
  ruby-rack-protection ruby-sinatra ruby-tilt spidermonkey-bin sslsplit w3af
  w3af-console wpasupplicant xulrunner-24.0 yersinia
升级了 64 个软件包，新安装了 37 个软件包，要卸载 1 个软件包，有 0 个软件包未被升级。
需要下载 406 MB 的软件包。
解压缩后将会空出 13.1 MB 的空间。
您希望继续执行吗？ [Y/n]

```

执行以上命令后，会对升级的软件包进行统计。提示有多少个包需要升级、安装、卸载等。这里输入 Y，继续升级软件。由于需要下载的软件包太多，所以该过程需要很长时间。

(3) 以上软件包都更新完后，即完成操作系统的升级。同样，重新启动系统时发现有两个内核可以启动操作系统

## 1.3 Kali Linux 的基本配置

当 Kali Linux 操作系统安装完成后，用户就可以使用了。但是，在使用过程中可能会安装一些软件或者需要输入中文字体。所以，在用户使用 Kali Linux 之前，建议进行一些基本配置，如配置软件源、安装中文输入法、更新系统等。这样，将会使用户在操作时更顺利。本节将介绍 Kali Linux 的一些基本配置。

### 1.3.1 配置软件源

软件源是一个应用程序安装库，大部分的应用软件都在这个库里面。它可以是网络服务器、光盘或硬盘上的一个目录。当用户安装某个软件时，可能发现在默认的软件源中没有。这时候，用户就可以通过配置软件源，然后进行安装。下面将介绍在 Kali Linux 中配置软件源的方法。

在 Kali Linux 操作系统中，默认只有 Kali 官方和一个 security 源。没有其它常用软件源，所以需要手动添加。下面介绍添加国内较快的一个更新源——中国科学技术大学的源。

Kali Linux 操作系统默认的软件源保存在 `/etc/apt/sources.list/` 文件中。在该文件中输入以下内容：

```
root@kali:~# vi /etc/apt/sources.list
deb http://mirrors.ustc.edu.cn/kali kali main non-free contrib
deb-src http://mirrors.ustc.edu.cn/kali kali main non-free contrib
deb http://mirrors.ustc.edu.cn/kali-security kali/updates main
contrib non-free
```

添加完以上源后，保存 `sources.list` 文件并退出。在该文件中，添加的软件源是根据不同的软件库分类的。其中，`deb` 指的是 DEB 包的目录；`deb-src` 指的是源码目录。如果自己不需要看程序或者编译的话，可以不指定 `deb-src`。因为 `deb-src` 和 `deb` 是成对出现的，在配置软件源时可以不指定 `deb-src`。但是当需要 `deb-src` 的时候，`deb` 是必须指定的。

配置完以上软件源后，需要更新软件包列表后才可以安装。更新软件包列表，执行命令如下所示：

```
root@kali:~# apt-get update
```

更新完软件列表后，会自动退出程序。这样，中国科学技术大学的软件源就添加成功了。当系统中没有提供有要安装的包时，会自动的通过该源下载并安装相应的软件。

注意：在以上过程中，操作系统必须要连接到互联网。否则，更新会失败。

### 1.3.2 安装中文输入法

在 Kali Linux 操作系统中，默认没有安装有中文输入法。在很多情况下，可能需要使用

中文输入法。为了方便用户的使用，下面将介绍在 Kali Linux 中安装小企鹅中文输入法。

**【实例 1-3】**安装小企鹅中文输入法。执行命令如下所示：

```
root@kali:~# apt-get install fcitx-table-wbpy ttf-wqy-microhei ttf-wqy-zenhei
```

执行以上命令后，安装过程中没有出现任何错误的话，该软件包就安装成功了。安装成功后，需要启动该输入法才可以使用。启动小企鹅输入法。执行命令如下所示：

```
root@kali:~# fcitx
```

执行以上命令后，会输出大量的信息。这些信息都是启动 fcitx 时加载的一些附加组件配置文件。默认启动 fcitx 后，可能在最后出现一行警告信息“请设置环境变量 XMODIFIERS”。这是因为 XMODIFIERS 环境变量设置不正确所导致的。这时候只需要重新设置一下 XMODIFIERS 环境变量就可以了。该信息只是一个警告，用户不做其它设置也不会影响小企鹅输入法的使用。为了用户不受该警告信息的影响，这里介绍下设置 XMODIFIERS 环境变量的方法。其语法格式如下所示：

```
export XMODIFIERS="@im=YOUR_XIM_NAME"
```

语法中的 YOUR\_XIM\_NAME 是 XIM 程序在系统注册时的名字。应用程序启动时会根据该变量查找相应的 XIM 服务器。因此，即使系统中同时运行了若干个 XIM 程序，一个应用程序在某个时刻也只能使用一个 XIM 输入法。

fcitx 缺省注册的 XIM 名为 fcitx，但如果 fcitx 启动时 XMODIFIERS 已经设置好，fcitx 会自动以系统的设置来注册合适的名字。如果没有设置好，使用以下方法设置。通常情况下是配置 ~/.bashrc 文件，在该文件中添加以下内容。如下所示：

```
export XMODIFIERS="@im=fcitx"
export XIM=fcitx
export XIM_PROGRAM=fcitx
```

添加并保存以上内容后，重新登录当前用户，fcitx 输入法将自动运行。如果没有启动，则在终端执行如下命令：

```
root@kali:~# fcitx
```

小企鹅输入法成功运行后，将会在屏幕的右上角弹出一个键盘。该输入法默认支持汉语、拼音、双拼和五笔拼音四种输入法，这几种输入法默认使用 Ctrl+Shift 键切换。

如果想要修改输入法之间的切换键，右击桌面右上角的键盘，将弹出如图 1.54 所示的界面。

在该界面单击“配置”命令，将显示如图 1.55 所示的界面。在该界面单击“全局配置”标签，将显示如图 1.56 所示的界面。



图 1.54 fcitx 界面

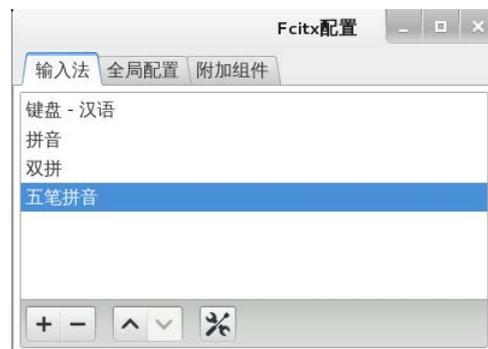


图 1.55 Fcix 配置



图 1.56 全局配置

从该界面可以看到各种快捷键的设置，根据自己习惯用的快捷键进行设置。设置完后，单击“应用”按钮。

### 1.3.3 虚拟机中使用 USB 设备

通常情况下，用户会在虚拟机中连接一些 USB 设备，如 USB 无线网卡、U 盘等。如果虚拟机运行正常的话，这些 USB 设备插入后可能马上就会被识别。但是，如果虚拟机的某个服务被停止了，这时候插入的 USB 设备无法被虚拟机识别。所以，用户有时候发现自己插入的 USB 无线网卡没有被识别出。下面将介绍如何在虚拟机中使用 USB 设备。

这里将介绍在 Windows 7 中，VMware Workstation 虚拟机中 USB 设备的使用方法。安装 VMware Workstation 后，在 Windows 7 系统中会被创建几个相关的服务。用户可以在 Windows 7 的服务管理界面查看到。具体方法如下所示：

(1) 在 Windows 7 的桌面选择计算机图标，然后单击右键并选择“管理”命令，将打开如图 1.57 所示的界面。

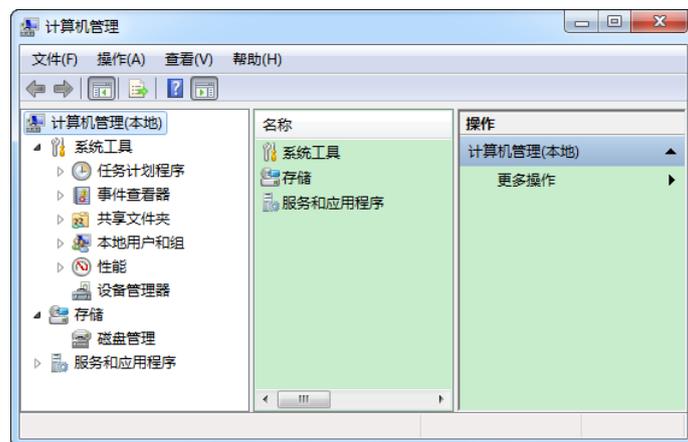


图 1.57 计算机管理

(2) 在该界面左侧栏中依次选择“服务和应用程序”|“服务”选项，将打开服务管理界面，如图 1.58 所示。

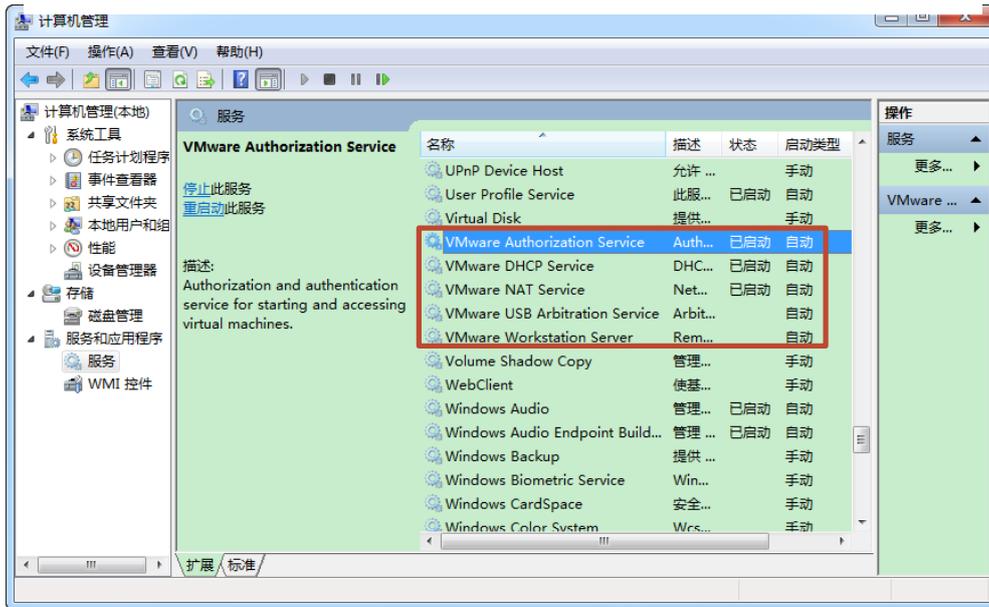


图 1.58 服务

(3) 在该界面的中间栏中，将看到当前系统中安装的所有服务。其中名称以 VMware 开头的服务，都是用于管理虚拟机的相关服务。从该界面可以看到，包括五个相关的服务。这几个服务分别用来，认证、自动获取地址、网络地址转换、USB 设备管理及远程访问。从该界面中间栏的状态列，可以看到每个服务是否启动。如果用户发现自己的 USB 设备无法被识别时，应该是 VMware USB Arbitration Service 服务没有启动。这时候用户在名称列选择该服务，然后单击右键将弹出一个菜单栏，如图 1.59 所示。

(4) 在该菜单栏中单击“启动”按钮，该服务即可被成功启动。然后，返回到虚拟机界面，即可连接所要连接的 USB 设备。如果虚拟机可以识别 USB 设备的话，通常情况下插入 USB 设备后，将会弹出一个对话框。如图 1.60 所示。



图 1.59 启动服务

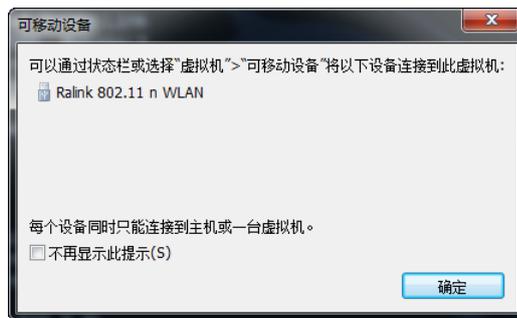


图 1.60 连接的移动设备

(5) 从该界面可以看到，当前系统插入一个名称为 Ralink 802.11 n WLAN 的 USB 设备。用户可以通过选择“虚拟机”|“可移动设备”选项，将该设备连接到虚拟机。此时，在虚拟机菜单栏中依次选择“虚拟机”|“可移动设备”选项，将看到当前系统中插入的所有移动设备，如图 1.61 所示。

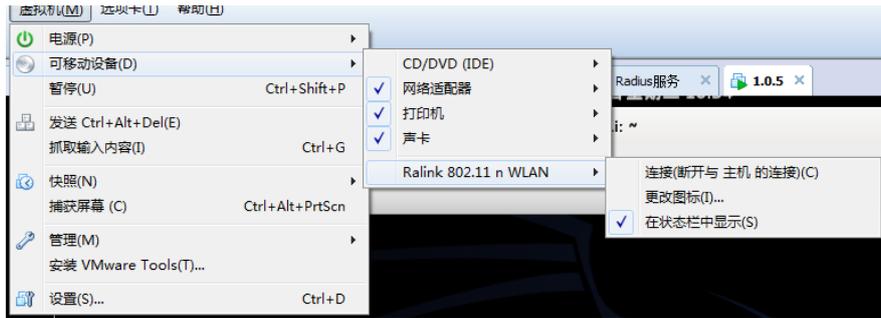


图 1.61 选择 USB 设备

(5) 在该界面的可移动设备选项中，可以看到插入的 USB 设备名称“Ralink 802.11 n WLAN”。从该界面可以看到该无线网卡，目前已经与主机建立连接。所以，如果想让该设备连接到虚拟机，选择“连接(断开与主机的连接(C))”选项，将显示如图 1.62 所示的界面。



图 1.62 提示对话框

(6) 该界面是一个提示对话框，这里单击“确定”按钮，该 USB 设备将自动连接到虚拟机操作系统中。这里插入的 USB 设备是一个无线网卡。所以，用户可以使用 ifconfig 命令查看该设备的连接状态。执行命令如下所示：

```

root@kali:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:13:5e:8e
          inet addr:192.168.1.105  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe13:5e8e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9688 (9.4 KiB)  TX bytes:3044 (2.9 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:820 (820.0 B)  TX bytes:820 (820.0 B)

wlan1     Link encap:Ethernet  HWaddr 00:c1:41:26:0e:f9
          inet6 addr: fe80::2c1:41ff:fe26:ef9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:528 (528.0 B)

```

从输出的信息中，可以看到有一个名称为 wlan1 的接口。当前操作系统中，只有一块有线网卡。在 Linux 系统中，默认的接口名称为 eth0。所以，wlan1（该接口名称不是固定的）

就是插入的无线网卡接口。如果输出的信息中，没有 wlan1 接口的话，可能接入的设备没有启动。用户可以使用 `ifconfig -a` 命令查看，即可看到接入的无线网卡。此时，用户需要手动启动该无线网卡。执行命令如下所示：

```
root@kali:~ # ifconfig wlan1 up
```

执行以上命令后，没有任何信息输出。用户可以再次使用 `ifconfig` 命令查看，以确定该无线网卡被启动。