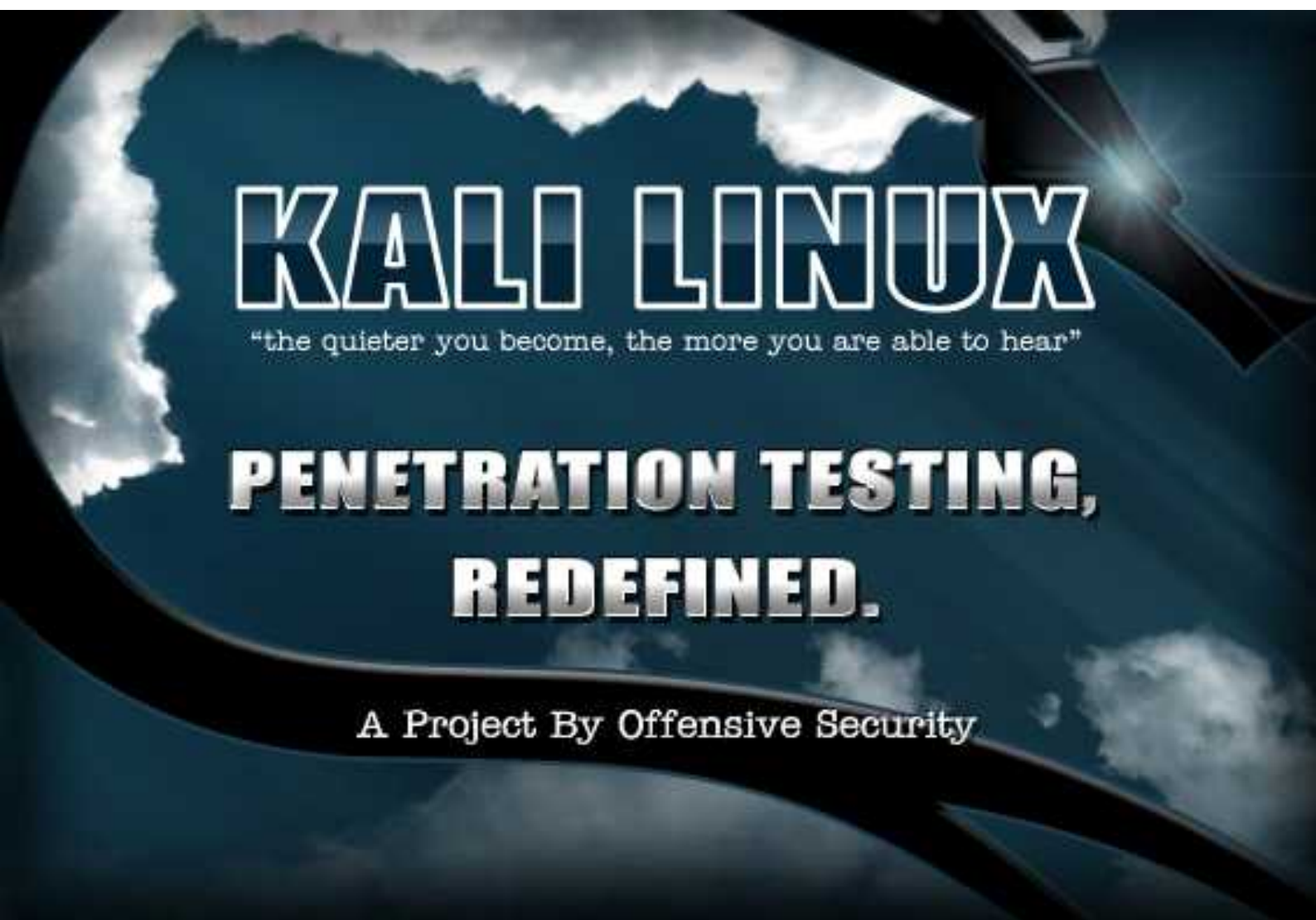


# KALI LINUX 中文指南 0.1



2013/3/14

欢迎点击这里的链接进入精彩的[Linux公社](http://www.Linuxidc.com) 网站

Linux公社（[www.Linuxidc.com](http://www.Linuxidc.com)）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

[Linux公社](http://www.Linuxidc.com)是专业的Linux系统门户网站，实时发布最新Linux资讯，包括Linux、Ubuntu、Fedora、RedHat、红旗Linux、Linux教程、Linux认证、SUSE Linux、Android、Oracle、Hadoop、CentOS、MySQL、Apache、Nginx、Tomcat、Python、Java、C语言、OpenStack、集群等技术。

Linux公社（[LinuxIDC.com](http://www.LinuxIDC.com)）设置了有一定影响力的Linux专题栏目。

包括：[Ubuntu 专题](#) [Fedora 专题](#) [Android 专题](#) [Oracle 专题](#) [Hadoop 专题](#) [RedHat 专题](#) [SUSE 专题](#) [红旗 Linux 专题](#) [CentOS 专题](#)



[www.linuxidc.com](http://www.linuxidc.com)

01. Kali Linux 介绍 .....	3
一、    Kali Linux 与 Debian 的区别 .....	3
二、    Kali Linux 商标策略 .....	3
三、    Kali Linux 适合你么? .....	5
四、    Kali Linux 特性 .....	5
五、    Kali Linux 镜像 .....	6
02. Kali Linux 安装 .....	7
一、    硬盘安装 Kali Linux (可选择是否加密) .....	7
二、    用 Live U 盘安装 Kali Linux .....	19
三、    Kali 和 Windows 双引导 .....	22
四、    Kali Mini ISO 网络安装 .....	28
五、    Kali Linux PXE 网络安装 .....	33
03. Kali Linux 一般应用 .....	35
一、    Kali Linux 电子取证模式 .....	35
二、    Kali 虚拟机安装 VMware Tools .....	37
三、    运行 Metasploit Framework .....	38
四、    建立你自己的卡利 ISO .....	39
五、    更改卡利桌面环境 .....	41
六、    解决无线驱动程序问题 .....	42
04. Kali Linux ARM 应用 .....	43
一、    准备 Kali Linux ARM chroot .....	43
二、    在 ODROID U2 安装 Kali ARM .....	47
三、    在三星 Chromebook 安装 Kali ARM .....	49
四、    在 Raspberry Pi 安装 Kali ARM .....	52
05. Kali Linux 开发 .....	53
一、    ARM 交叉编译 .....	53
二、    重新编译 Kali Linux 内核 .....	54
三、    从源代码编译包 .....	55
06. Kali Linux 社区 .....	57
一、    Kali Linux 漏洞跟踪 .....	57
二、    Kali Linux 官方网站 .....	57

# 01. Kali Linux 介绍

## 一、Kali Linux 与 Debian 的区别

Kali Linux 面向专业的渗透测试和安全审计。因此，Kali Linux 已经进行了如下的多处核心的修改：

1. **单用户，设计成 root 权限登录：**由于安全审计的本质，Kali Linux 被设计成使用[单用户，root 权限](#)“方案。”
2. **默认禁用网络服务：**Kali Linux 包含了默认[禁用网络服务](#)的 sysvinit hooks。它们允许用户在 Kali Linux 安装各种的服务，允许用户安装各种包，同时仍然确保我们默认的发行版安全。附加的服务，例如蓝牙也会被默认列入黑名单。
3. **定制的内核：**Kali Linux 使用打过无线注入补丁的上游内核。

Kali Linux 1.0 基于 [Debian Wheezy](#)。因此，大部分的 Kali 包都是从 Debian 源原封不动的导入过来。还有些比较新的包是从不稳定版或实验版导入，或因为这样可以提升用户体验，或因为那是必要修复的 BUGS。

### 分离包

为了实现一些 Kali 特有的功能，一些包明显的必须被分离。但 Kali 在可能时尽可能靠提高上游包的数量来保持包的数量最小化(或直接整合功能，或添加必要的钩子使其化繁为简而实际上并没有修改上游包)。

每个被 Kali 分离的包放在 Git 源的 debian 分支里，用一个 *Git 的 debian 分支* 混合在主分支使得更新一个被分离的包变得很容易。

### 新包

此文前面提到，Kali 引入了很多新的用于渗透测试和安全审计领域的 Debian 包。根据 Debian's Free Software Guidelines，这些包大部分都是免费的。Kali 打算贡献它们给 Debian 并且直接在 Debian 里维护他们。

因此，Kali 包努力遵循 Debian 策略并且在 Debian 里表现良好。

## 二、Kali Linux 商标策略

Kali Linux 和 Offensive Security 希望促进我们的商标在互联网社会的广泛认同，但是也要确保我们的商标对应我们的公司和产品。我们的商标策略核心是**信任**—我们要避免当用户不是在和 Kali Linux 和/或 Offensive Security 交涉时，却认为是在和 Kali Linux 和/或 Offensive Security 交涉。这对**可信任**的渗透测试发行版的开发和分发(例如 Kali Linux)很重要。

这份文档辨认和描述我们的商标，并提供合理使用它们的指南。我们很乐意公平和诚实地使用我们的商标。如果你有意向的话，详细咨询请随时与我们联系。

## 我们的一些商标



## 用于打印，网页，媒体和公开展示

保持商标的外形和拼写很重要。请勿修改商标。例如包含使用缩写名，添加 LOGO，或与其它词汇捆绑。我们建议你像我们使用商标一样正确的使用它们。

Offensive Security 商标标明源自我们的产品和服务。只要商标是用于辨认 Offensive Security 的产品和服务，我们鼓励使用。我们不希望在用户不是在和我们一起交涉时，却认为他们是在和我们一起交涉。

首先提到 Offensive Security 的商标应该伴随标志符号，已注册的商标用®，未注册的商标用™。如果有疑虑，请参考上面列表使用™的正确符号。

使用 Offensive Security 商标应该与周围的大写，斜体，粗体或下划线文本分开。Offensive Security 商标标明源自我们的产品和服务。

当使用 Offensive Security 商标于书面材料时，你应该提供一个表示[此商标]是 Offensive Security 商标的声明。例如：

“KALI LINUX ™是 Offensive Security 的商标。这个声明可以正确的放在你的文本，或脚注或者尾注里。

Offensive Security 商标用于你的域名是禁止的，因为这样使用将导致客户困惑。在商标政策范围以外不得未经 Offensive Security 明确的书面许可使用。

你可以印制 T 恤，做电脑桌面，或制作别的有 Offensive Security 商标的制品，仅限你本人和朋友(未从中获得回报)。不能把商标用于商业生产(无论是否盈利)-至少在没有书面允许情况下不允许。

## 联系

如果你有任何问题或者评论，或者想举报滥用 Offensive Security 商标，请联系我们。

## 三、 Kali Linux 适合你么？

作为发行版的开发者，可能有人认为我们建议所有人都使用 Kali Linux。事实上，Kali 是一个面向专业的渗透测试和安全审计的发行版，所以不推荐那些不熟悉 Linux 的人使用。

此外，在你的网络里滥用安全工具，特别是未经许可时，可能会导致不可挽回的损失和严重的后果。

如果你在寻找一个学习 Linux 基础的发行版，你需要一个好的起点，Kali Linux 并不是你理想的发行版。你可能应该用 Ubuntu 或者 Debian。

## 四、 Kali Linux 特性

Kali Linux 是一个高级渗透测试和安全审计 Linux 发行版。

Kali 是 BackTrack Linux 完全遵循 Debian 开发标准彻底的完全重建。全新的目录框架，复查并打包所有工具，我们还为 VCS 建立了 Git 树。

- **超过 300 个渗透测试工具：** 复查了每一个 BackTrack 里的工具之后，我们去掉了一部分不再有效或者是功能重复的工具。
- **永久免费：** Kali Linux 一如既往的免费。你永远无需为 Kali Linux 付费。

欢迎点击这里的链接进入精彩的[Linux公社](http://www.Linuxidc.com) 网站

Linux公社（[www.Linuxidc.com](http://www.Linuxidc.com)）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

[Linux公社](http://www.Linuxidc.com)是专业的Linux系统门户网站，实时发布最新Linux资讯，包括Linux、Ubuntu、Fedora、RedHat、红旗Linux、Linux教程、Linux认证、SUSE Linux、Android、Oracle、Hadoop、CentOS、MySQL、Apache、Nginx、Tomcat、Python、Java、C语言、OpenStack、集群等技术。

Linux公社（[LinuxIDC.com](http://www.LinuxIDC.com)）设置了有一定影响力的Linux专题栏目。

包括：[Ubuntu 专题](#) [Fedora 专题](#) [Android 专题](#) [Oracle 专题](#) [Hadoop 专题](#) [RedHat 专题](#) [SUSE 专题](#) [红旗 Linux 专题](#) [CentOS 专题](#)





- **开源 Git 树：**我们是开源软件忠实的拥护者，所有人都可以浏览我们的[开发树](#)，那些想调整或重建包的人可以得到所有源代码。
- **遵循 FHS：**Kali 被开发成遵循 [Filesystem Hierarchy Standard](#)，Linux 用户可以方便的找到命令文件，帮助文件，库文件等。
- **大量支持无线设备：**我们构建 Kali Linux 使其尽可能的支持更多的无线设备，在各种各样的硬件上正常运行，兼容大量 USB 和其它无线设备。
- **集成注入补丁的内核：**作为渗透测试者或开发组经常需要做无线安全评估。所以我们的内核包含了最新的注入补丁。
- **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。
- **包和源有 GPG 签名：**所有 Kali 的包都在它们编译和被提交时被每个开发者签名，而源在其后也对其签名。
- **多语言：**虽然渗透工具趋向于用英语，但我们确保 Kali 有多语言支持，可以让用户使用本国语言定位到他们工作时需要的工具。
- **完全的可定制：**我们完全理解，不是每个人都赞同我们的设计决定，所以我们让更多有创新精神的用户[定制 Kali Linux](#) (甚至定制内核) 成他们喜欢的样子变得尽可能的容易。
- **ARMEL 和 ARMHF 支持：**自从基于 ARM 的设备变得越来越普遍和廉价，我们就知道我们将竭尽全力的做好 [Kali 的 ARM 支持](#)。因此有了现在的 [ARMEL 和 ARMHF](#) 系统。Kali Linux 有完整的主线发行版的 ARM 源，所以 ARM 版的工具将会和别的版本同时更新。Kali 现在可以运行在如下的 ARM 设备：
  - [rk3306 mk/ss808](#)
  - [Raspberry Pi](#)
  - [ODROID U2/X2](#)
  - [MK802/MK802 II](#)
  - [Samsung Chromebook](#)

Kali 特别针对渗透测试，因此本站所有文档假设读者事先有 Linux 操作系统知识。

## 五、Kali Linux 镜像

### ISO 文件

Kali Linux 提供了 32 位和 64 位的可引导 ISO

**警告！**请确认你从官方源下载的 Kali Linux 与官方提供的 MD5 校验码一致。因为在二次封装的时候往 Kali Linux 植入恶意代码并通过非官方渠道发布是件很容易的事情。

- [下载 Kali ISO](#)

### VMware 镜像

Kali 提供了 32 位和 64 位的预装了 Vmware Tools 的 VMware 虚拟机镜像。



- [下载 Kali VMware 镜像文件](#)

## ARM 镜像

由于 ARM 的架构性质，单一的一个镜像不能通用于所有 ARM 设备运行。我们提供了如下设备的 Kali Linux ARM 镜像：

- rk3306 mk/ss808
- Raspberry Pi
- ODROID-U2/X2
- MK802/MK802 II
- Samsung Chromebook

## 验证下载的镜像的 MD5 校验码

验证你下载的文件 MD5 校验码与官方提供的校验码是否一致很重要。

### 在 Linux 验证 MD5 校验码

`md5sum kali-i386.iso` 2455da608852a7308e1d3a4dad34d3ce kali-i386.iso

### 在 OSX 验证 MD5 校验码

`md5 kali-i386.iso` MD5 (kali-i386.iso) = 2455da608852a7308e1d3a4dad34d3ce

### 在 Windows 验证 MD5 校验码

Windows 本身不能计算 MD5 校验码，所以你需要 MD5summer 这类软件来验证 MD5 校验码。

# 02. Kali Linux 安装

## 一、 硬盘安装 Kali Linux（可选择是否加密）

有时我们希望采用全盘加密的方式来加密我们的敏感信息。你可以使用 Kali 安装程序把它安装到硬盘或是 U 盘的加密 LVM 逻辑卷。安装过程除了加密 LVM 逻辑卷部分以外，与常规的 Kali Linux 硬盘安装非常类似。

### 安装条件

- 安装 Kali Linux 需要最少 8G 硬盘可用空间。
- i386 和 amd64 架构，最低 512MB 内存。
- CD-DVD 光驱/支持 USB 引导

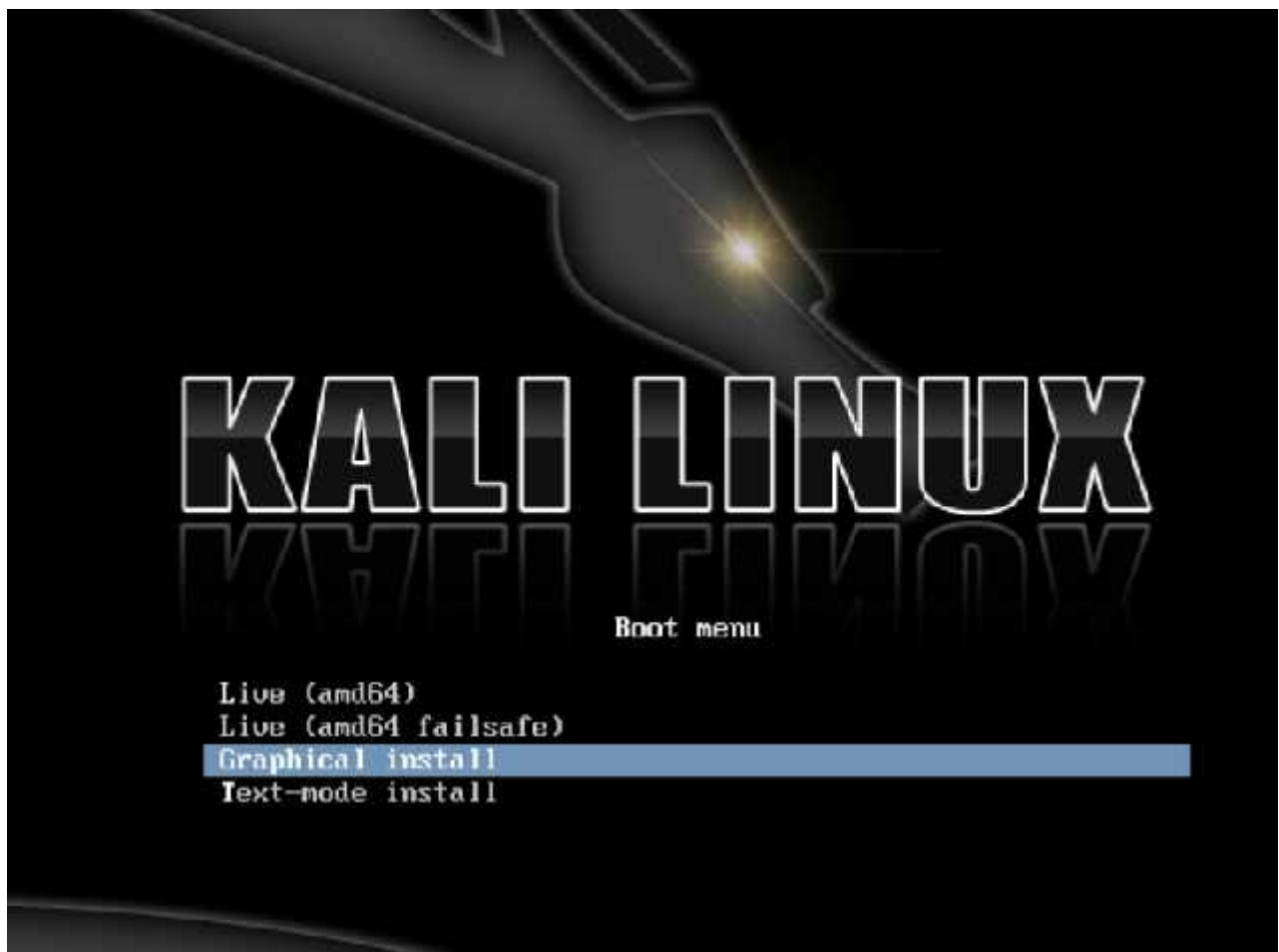
安装 Kali Linux 到你的电脑过程很简单。首先你需要兼容的电脑硬件。最低硬件要求如下，更好的硬件性能会更好。i386 镜像默认使用 PAE 内核，所以你能在大于 4GB 内存的机器运行它。下载 Kali Linux 然后刻录 DVD 盘，或准备好一块 Kali Linux Live U 盘作为安装媒介。

## 准备安装

1. [下载 Kali Linux](#)。
2. 把 Kali Linux 刻录到 DVD 盘或[制作 Kali Linux 镜像 U 盘](#)。
3. 确认你电脑的 BIOS 设置了从 CD/USB 引导。

## Kali Linux 安装步骤

1. 开始安装，从你选择的安装媒介启动。你会看到 Kali 的引导界面。选择图形界面或文本模式安装。此处，我们选择图形界面安装。



2. 选择你的首选语言和国家。你会被提示为你的键盘配置适当的 Keymap。



3. 安装器会复制镜像到你的硬盘，探测你的网络接口，然后提示你为你的系统输入主机名。此例，我们输入 Kali 作为主机名。

欢迎点击这里的链接进入精彩的[Linux公社](http://www.Linuxidc.com) 网站

Linux公社（[www.Linuxidc.com](http://www.Linuxidc.com)）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

[Linux公社](http://www.Linuxidc.com)是专业的Linux系统门户网站，实时发布最新Linux资讯，包括Linux、Ubuntu、Fedora、RedHat、红旗Linux、Linux教程、Linux认证、SUSE Linux、Android、Oracle、Hadoop、CentOS、MySQL、Apache、Nginx、Tomcat、Python、Java、C语言、OpenStack、集群等技术。


Linux公社（[LinuxIDC.com](http://www.LinuxIDC.com)）设置了有一定影响力的Linux专题栏目。

包括：[Ubuntu 专题](#) [Fedora 专题](#) [Android 专题](#) [Oracle 专题](#) [Hadoop 专题](#) [RedHat 专题](#) [SUSE 专题](#) [红旗 Linux 专题](#) [CentOS 专题](#)





4. 为 root 账户输入一个强健的密码



### Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the 'sudo' command.

Note that you will not be able to see the password as you type it.

Root password:

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

Screenshot

Go Back

Continue

5. 下一步设置时区。



6. 安装器会检测硬盘,并提供 4 个选项。加密 LVM 安装应选择 **Guided – use entire disk and set up encrypted LVM(使用全盘 LVM 加密卷)**“, 一般安装选择第一个选项即可。如下图所示。

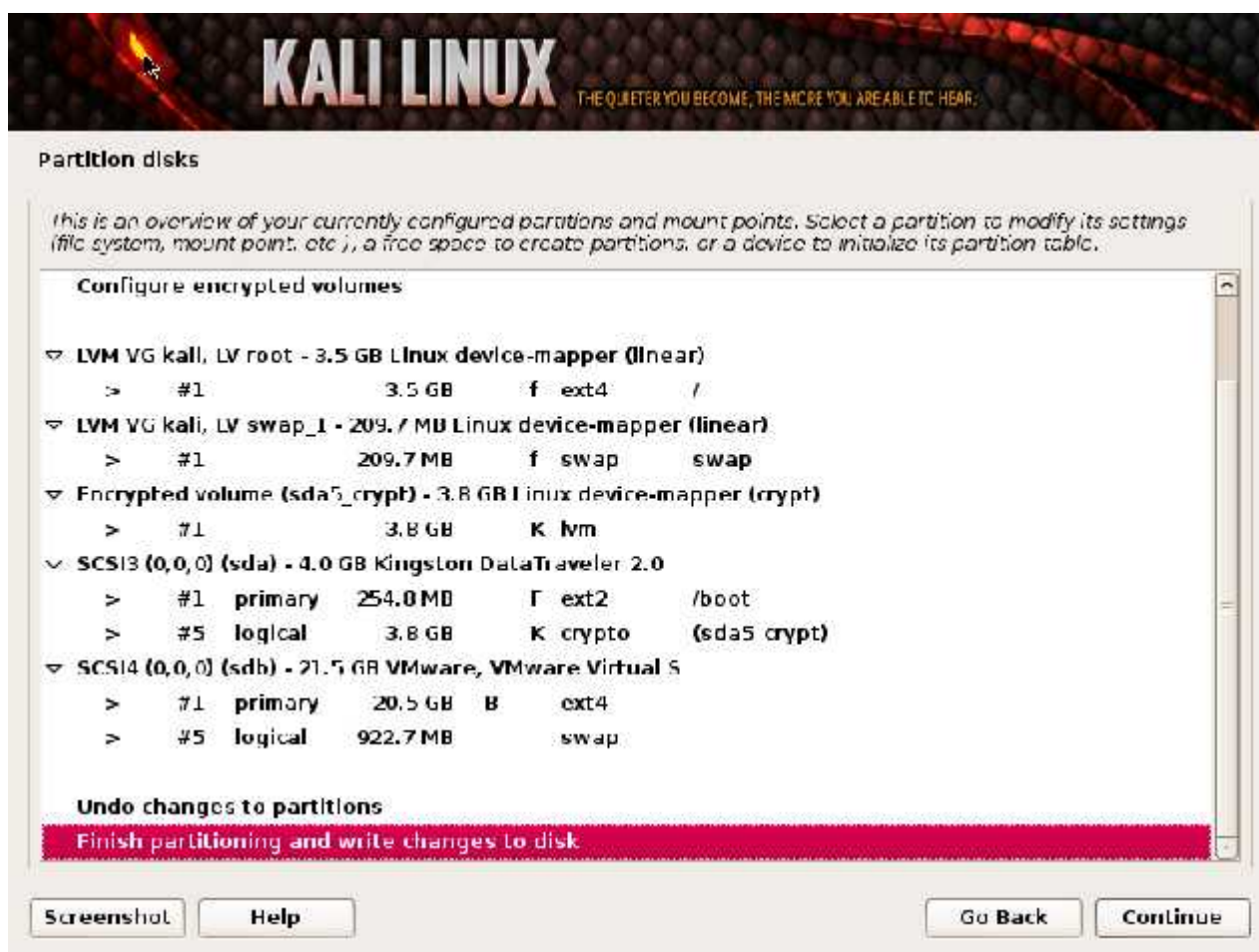




7. 选择安装 Kali 的目标驱动器。在此例中我们选择一块 U 盘作为目标驱动器。我们将用这块 U 盘来启动加密的 Kali。



8. 确认你的分区结构并继续安装。



9. 然后, 你将被要求输入一个加密密码。你必须记住此密码并在每次启动 Kali 时输入。



10. 配置网络 Mirrors。Kali 使用中心源发布软件。在必要的时候你需要输入适当的代理信息。

**注意！** 如果你选择了 NO，你将不能从 Kali 源安装软件。



11. 下一步安装 GRUB。



12. 最后，点击 *Continue*(继续)来重启系统，进入全新安装的 Kali。如果你安装的目标驱动器是 U 盘，确认 BIOS 中已设置为从 U 盘启动。你将在每次启动时输入先前设置的加密密码。





## 完成安装

现在你已经完成了 Kali Linux 的安装，是时候定制你的系统了。官方网站上的 Kali 常见问题里有更多信息，你还会在用户论坛里找到更多的小技巧。

## 二、用 Live U 盘安装 Kali Linux

从 U 盘启动然后安装 Kali 是我们最喜欢并且是获得并运行 Kali 最快的方法。为此，我们首先要在 U 盘创建 Kali ISO 的镜像。如果你想长久使用 Kali Linux U 盘，请在创建镜像前阅读完整的文档。

### 准备 USB 镜像

1. [下载 Kali linux](#)。
2. 如果你用到的是 Windows，下载 [Win32 Disk Imager](#)。
3. \*nix 类系统不需要任何别的软件。



欢迎点击这里的链接进入精彩的[Linux公社](http://www.Linuxidc.com) 网站

Linux公社（[www.Linuxidc.com](http://www.Linuxidc.com)）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

[Linux公社](http://www.Linuxidc.com)是专业的Linux系统门户网站，实时发布最新Linux资讯，包括Linux、Ubuntu、Fedora、RedHat、红旗Linux、Linux教程、Linux认证、SUSE Linux、Android、Oracle、Hadoop、CentOS、MySQL、Apache、Nginx、Tomcat、Python、Java、C语言、OpenStack、集群等技术。

Linux公社（[LinuxIDC.com](http://www.LinuxIDC.com)）设置了有一定影响力的Linux专题栏目。

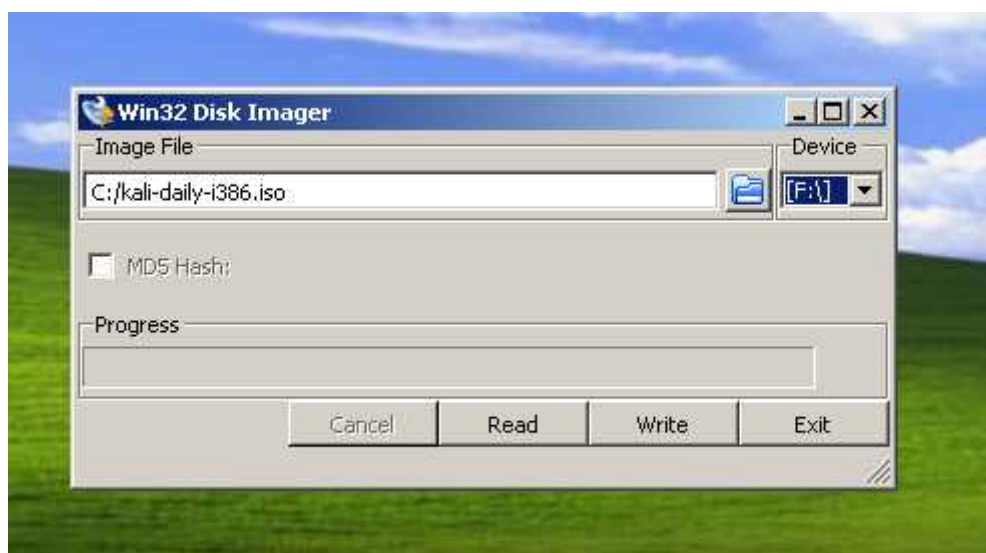
包括：[Ubuntu 专题](#) [Fedora 专题](#) [Android 专题](#) [Oracle 专题](#) [Hadoop 专题](#) [RedHat 专题](#) [SUSE 专题](#) [红旗 Linux 专题](#) [CentOS 专题](#)



4. 一块 U 盘(至少 2GB 容量)。

## 在 Windows 机器上镜象 Kali

1. 插入 U 盘。运行 Win32 Disk Imager。
2. 选择 Kali Linux ISO 文件作为被镜象文件然后核实被改写的是正确的那块 U 盘。



3. 镜象完成后，从 Windows 机器安全弹出 U 盘。现在你可以用 U 盘启动 Kali Linux 了。

## 在 Linux 机器上镜象 Kali

在 Linux 环境下制作可启动的 Kali Linux U 盘很容易。下载好 Kali ISO 文件后，你可以用 **dd** 把它复制到 U 盘：

警告！虽然在 U 盘上镜象 Kali 过程很简单，但是如果你不懂你正在用 **dd** 做什么很容易破坏引导分区。

1. 插入 U 盘。
2. 用 **dmesg** 确认你的 U 盘设备块名。
3. 开始在 U 盘镜象 Kali ISO 文件(谨慎操作！)：

```
dd if=kali.iso of=/dev/sdb bs=512k
```

就这样！你现在可以用 U 盘启动到 Kali Live/Installer 环境了。

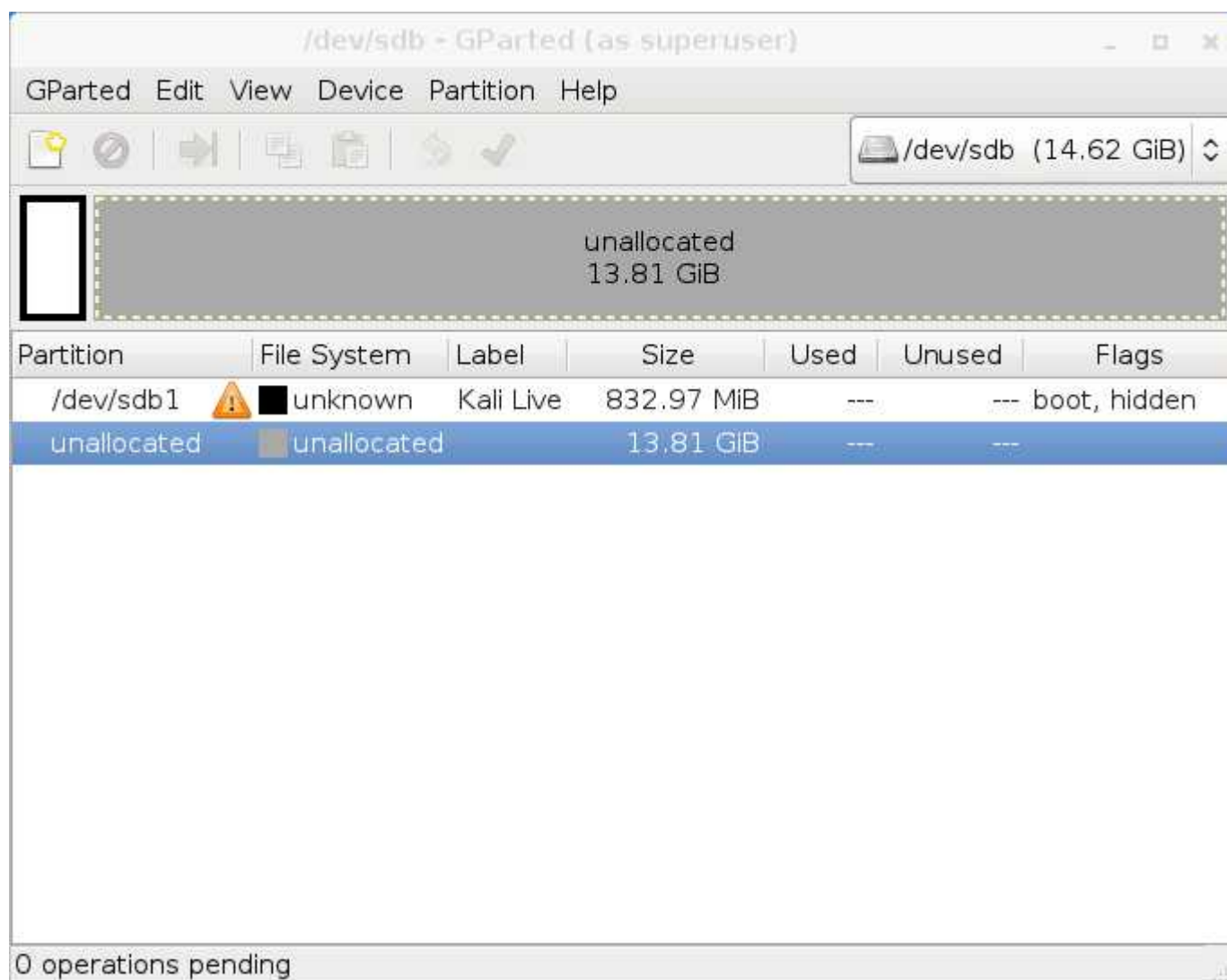
## 为你的 U 盘添加 Persistence 功能

在某些情况下。为你的 Kali Linux 镜像添加 persistence 功能(在 Live 启动的时候可以保存和修改文件)非常有用。为了给你的 Kali Linux U 盘启动 persistent 功能，按照以下步骤。在此例，我们假设我们的设备块名是 `/dev/sdb`。如果你想添加 persistence 功能，需要一块比上面提到的要求更大容量的 U 盘。

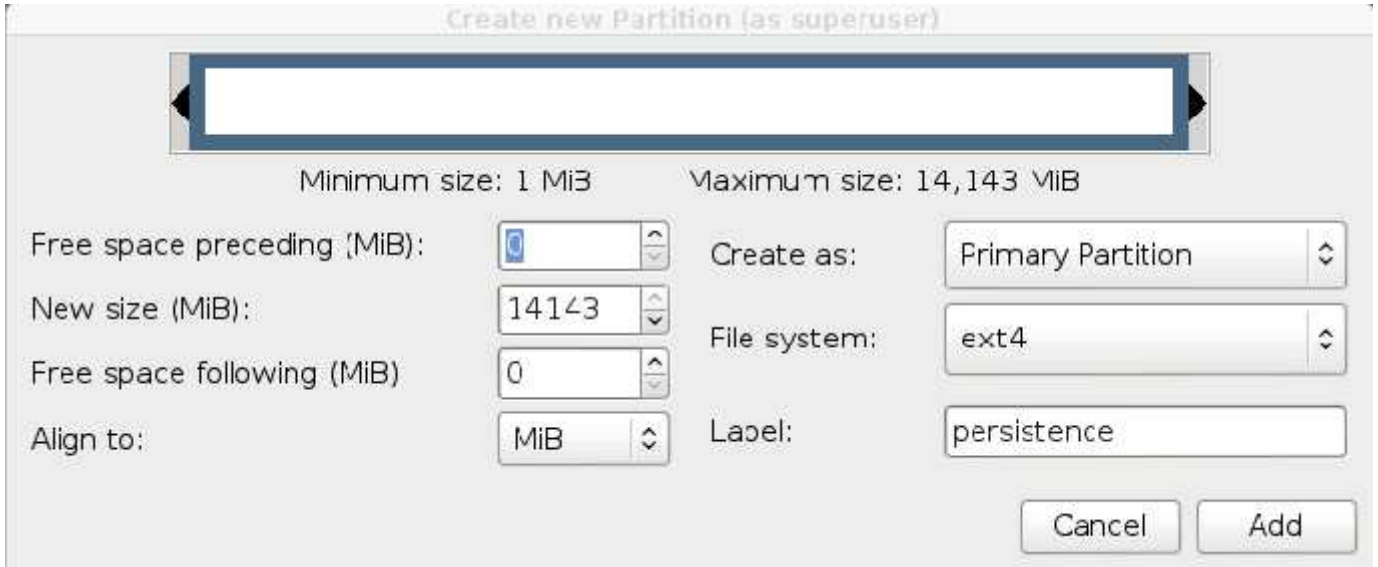
1. 镜像 Kali Linux ISO 到 U 盘和上面讲解的一样，用在 Linux 机器上的方法和 **dd**。
2. 在 U 盘创建并格式化额外的分区。在此例我们用 **gparted** by invoking:

```
gparted /dev/sdb
```

3. 你现在的分区方案应该和下图类似:



4. 着手于格式化一个你要用于 `persistence` 功能的理想大小的新分区。在此例，我们使用所有剩余可用空间。确保新创建的分区卷名是 `persistence` 然后格式化成 `ext4` 文件系统。



5. 这步完成后，用以下命令挂载用于 `persistence` 功能的 U 盘分区：

```
mkdir /mnt/usb
mount /dev/sdb2 /mnt/usb
echo "/ union" && /mnt/usb/persistence.conf
umount /mnt/usb
```

6. 插入 U 盘到你要启动的电脑。务必设置 BIOS 从 USB 设备启动。当显示 Kali Linux 启动画面时，从菜单选择“Live boot(不要按下回车)，然后按下 Tab 键。这将允许你编辑启动参数，在每次你想挂载你的 `persistent` 存储时添加“`persistence`”到 `boot` 参数行的最后。

### 三、Kali 和 Windows 双引导

把 Kali 和 Windows 装在一起很有用。然而，你要谨慎的安装。首先确保你已经备份了你电脑里的重要数据。因为我们要修改你的硬盘，所以你应该把数据备份到别的媒介。一旦你完成了备份，我们推荐你阅读硬盘安装 Kali Linux，以了解 Kali 的基础安装过程。

此例，我们将把 Kali Linux 和硬盘唯一的 Windows 7 系统装在一起。我们开始重新给 Windows 分区划分分区大小，缩小 Windows 分区的容量，以便把 Kali Linux 安装到新建的空分区。

下载 Kali Linux 刻录到 DVD 光盘，或者准备一块 Kali linux Live U 盘作为安装媒介。如果你的电脑没有 DVD 光驱或 USB 端口，请参考网络安装 Kali Linux。硬件要求：

- Windows 至少有 8G 的剩余空间
- 支持 CD-DVD / USB 引导

## 准备安装

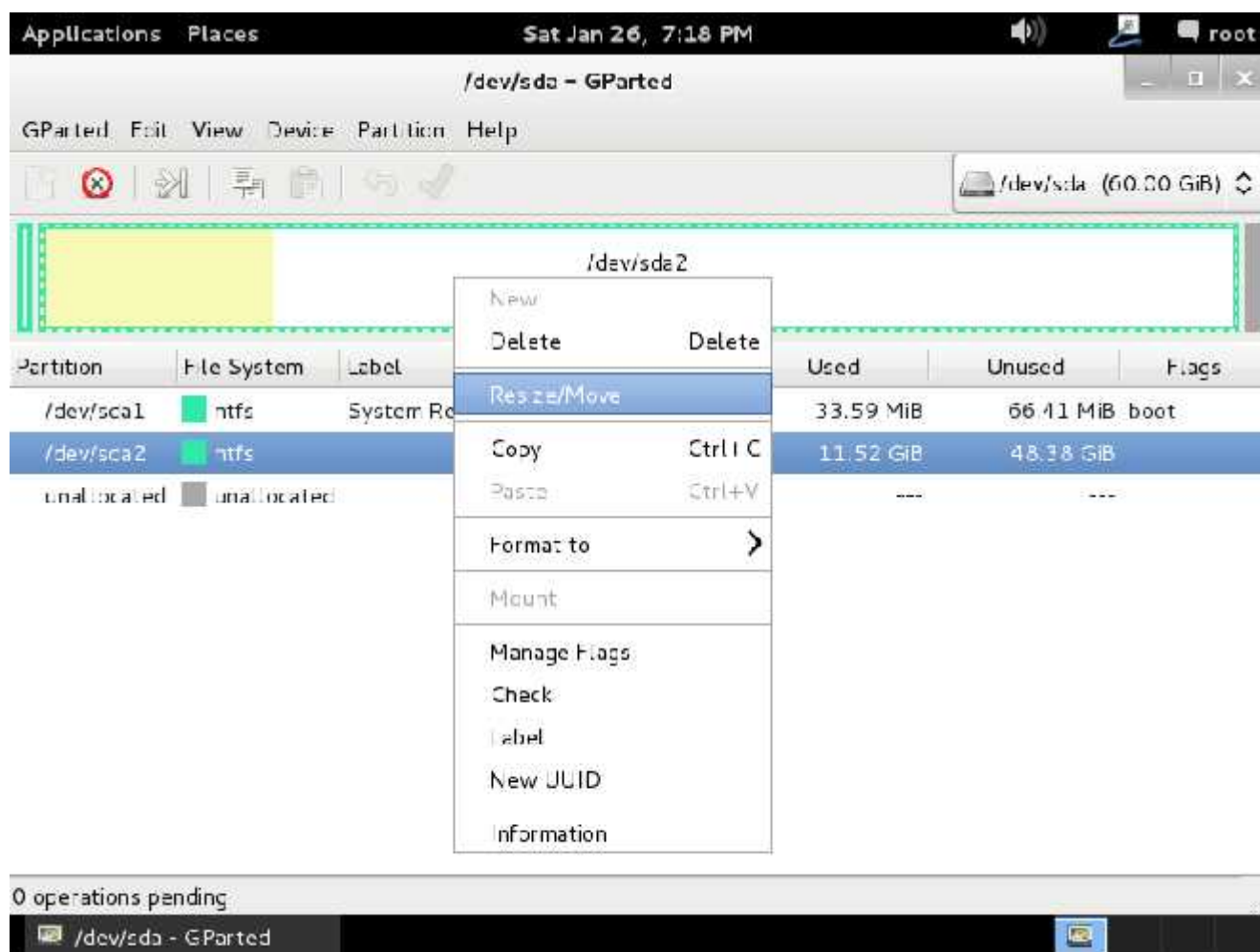
1. [下载 Kali Linux](#)。
2. 刻录 Kali Linux DVD 盘或[制作 Kali Linux Live U 盘](#)。
3. 确保你的电脑 BIOS 设置了从 CD/USB 引导。

## 双系统安装过程

1. 开始安装，从你选择的安装媒介启动。你会看到 Kali 的引导界面。选择 *Live*，然后你会进入到 Kali Linux 桌面。
2. 使用用户名 **root**，和密码 **toor** 登录。下一步运行 **gparted** 程序。我们将用 **gparted** 缩小 windows 分区的大小以提供足够的空间安装 Kali。

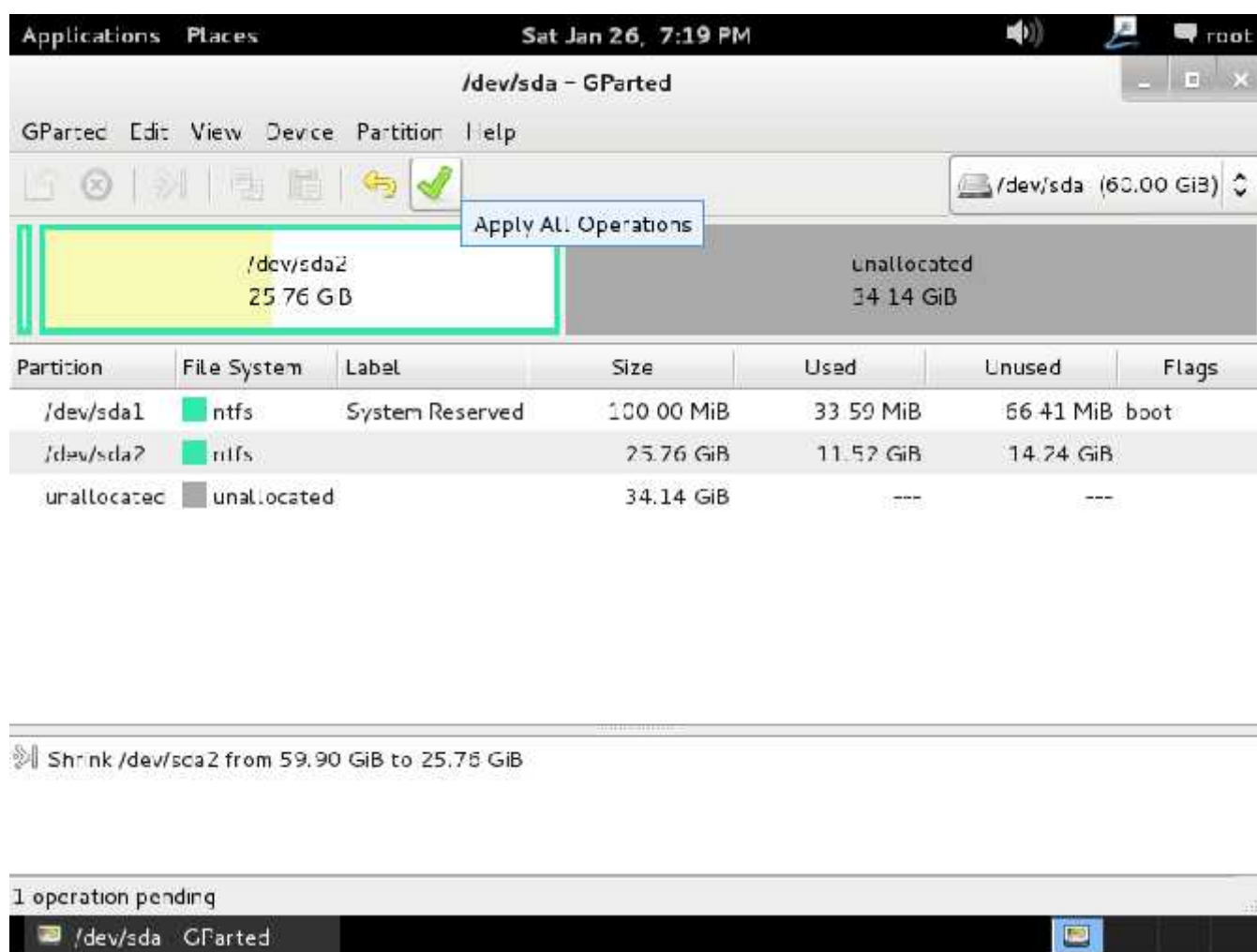


3. 选择 Windows 分区。根据你的系统情况选择，此例选择较大的第二个分区。此例中有两个分区，第一个分区是系统恢复分区，实际上 Windows 安装在/dev/sda2.重新调整 Windows 分区的大小预留(最小 8GB)空间给 Kali Linux。



4. 重新分区之后。确保点击了硬盘的 Apply All Operations(应用所有操作)。退出 **gparted** 并重启。





## Kali Linux 安装步骤

1. 安装步骤和之前的[硬盘安装 Kali Linux](#)，类似，除了分区的时候选 Guided - use the largest continuous free space(上文中用 gparted 创建的分区)。



2. 安装完毕，重启。你会看见 GRUB 的启动菜单有 Kali 和 Windows 启动项。



安装完成

## 四、Kali Mini ISO 网络安装

The Kali mini ISO is a convenient way to install a minimal Kali system and install it “from scratch. The mini install ISO will download all required packages from our repositories, meaning you need to have a fast Internet connection to use this installation method.

### 安装先决条件

- A minimum of 8 GB disk space for the Kali Linux install.
- For i386 and amd64 architectures, a minimum of 512MB RAM.
- CD-DVD Drive / USB boot support

## 准备安装

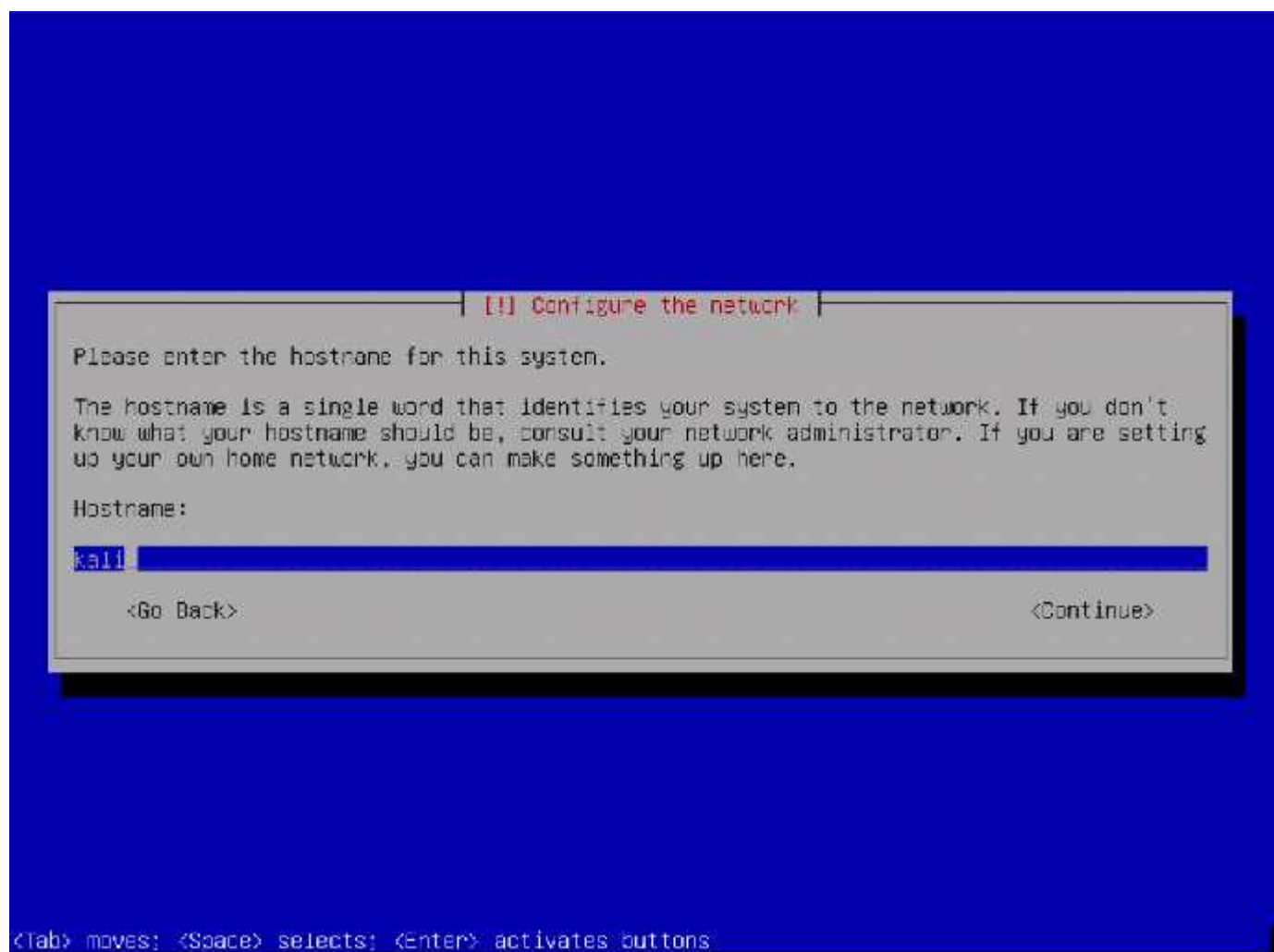
1. [Download the Kali mini ISO](#)。
2. Burn The Kali Linux ISO to DVD or [Image Kali Linux Live to USB](#)。
3. Ensure that your computer is set to boot from CD / USB in your BIOS。

## Kali Linux 安装步骤

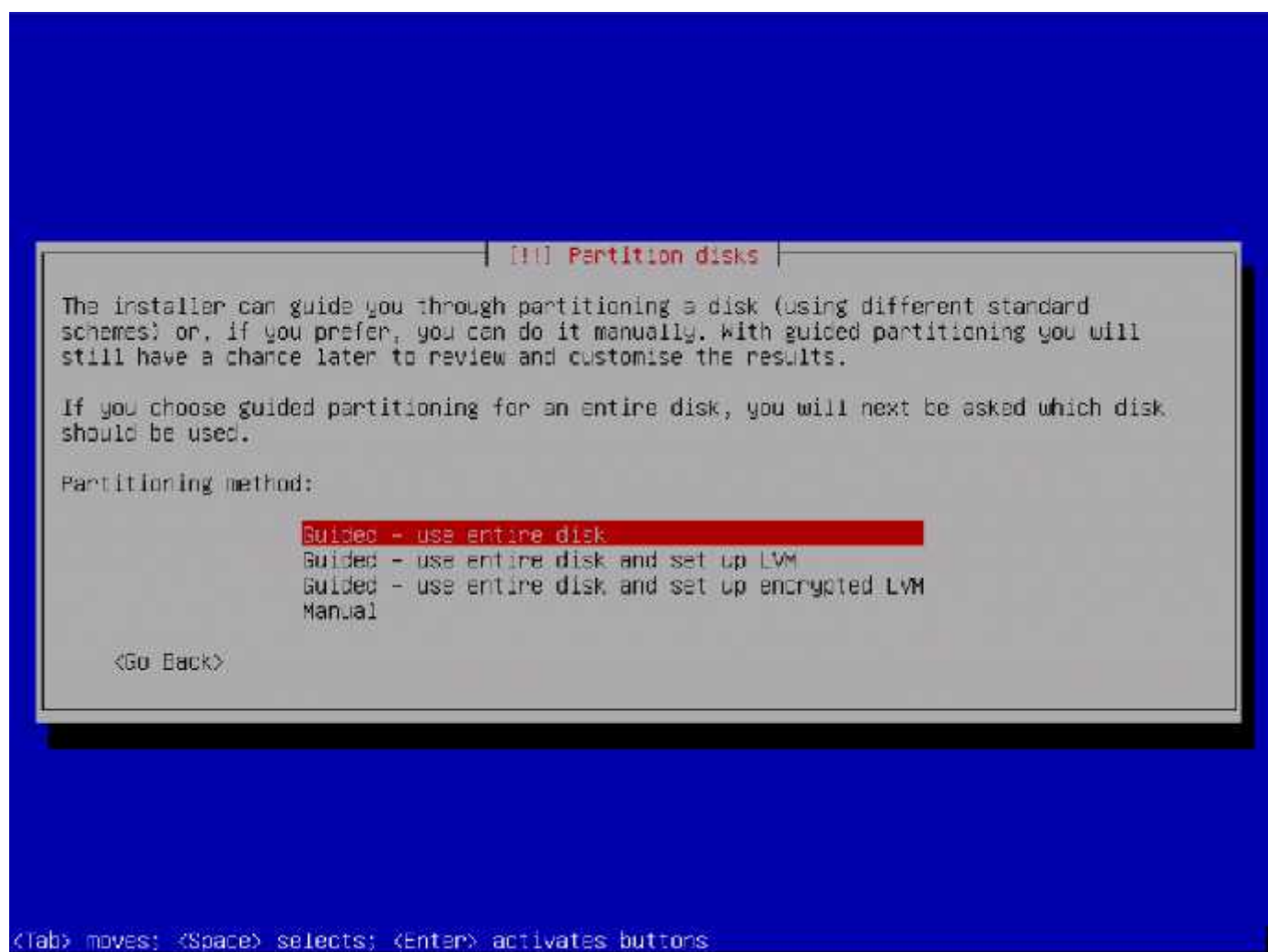
When you first boot the mini ISO, you will be presented with a small boot menu with various options. For this article, we will simply be doing a basic install.



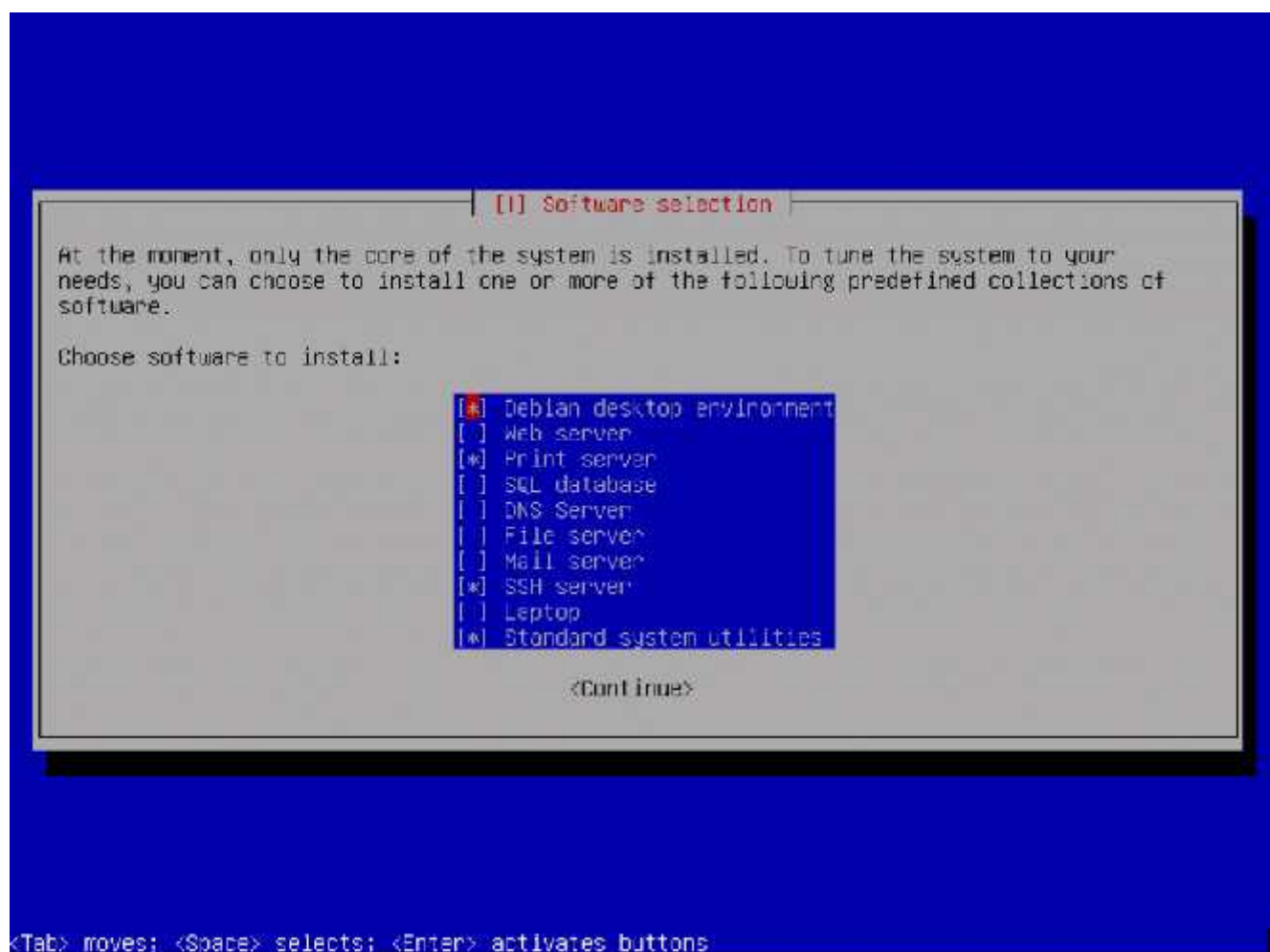
You will next be prompted for various things such as your language and keyboard type, then you will need to select a hostname for your installation. We will stick with the default of *kali*.



Next, you will need to select your time zone, then you'll be shown the partition options. To get up and running quickly, we will use 'Guided - use entire disk' and follow the prompts all the way through to create the new partitioning setup.

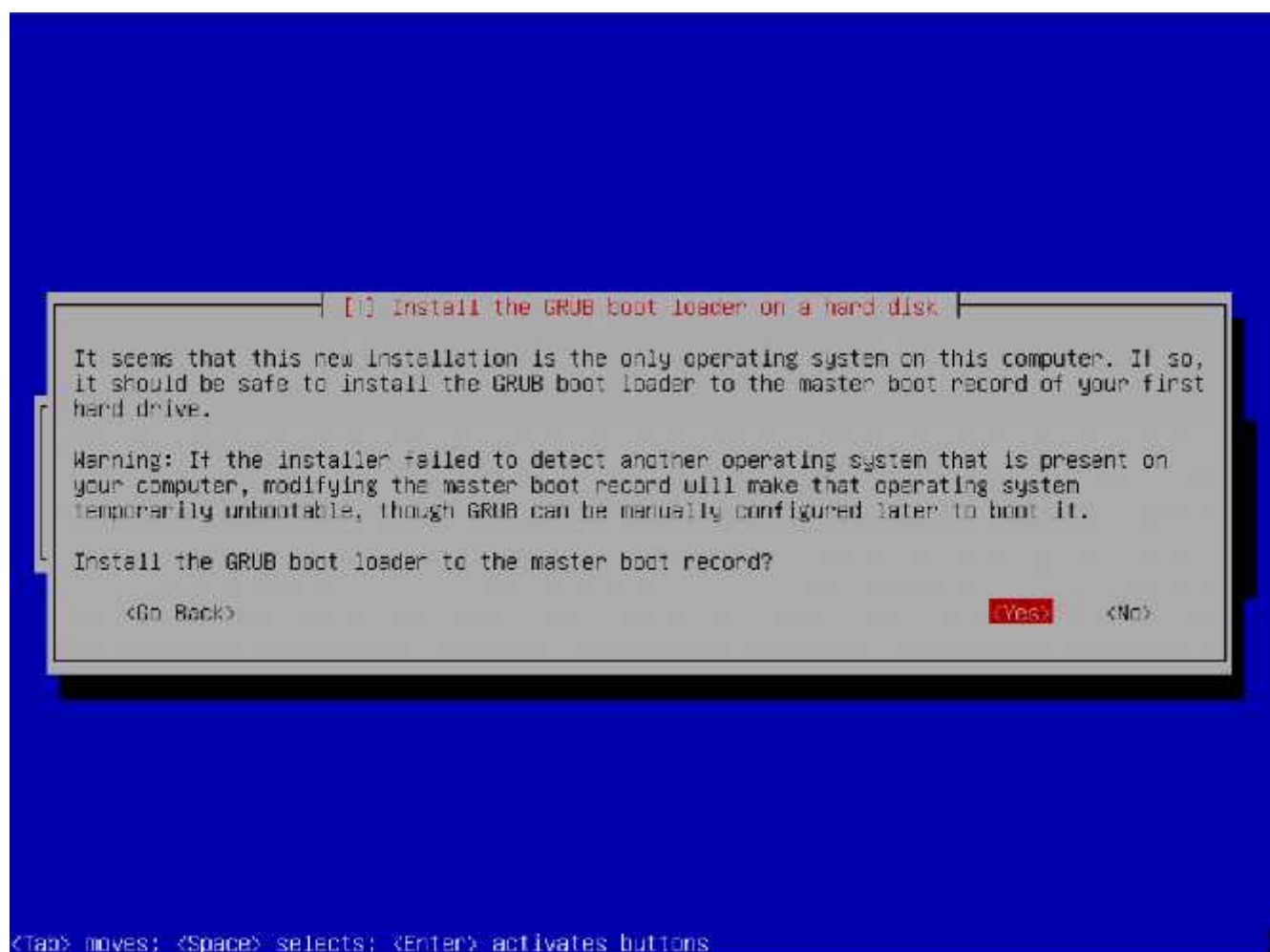


In order to reduce network bandwidth, a small subset of packages will be selected by default. If you wish to add different services or features, this is the area you would make your selections.



At this point, the installer will download all of the packages it requires and install them on the system. Depending on your Internet connectivity speed, this could take some time. Eventually, you will finally be prompted to install GRUB to finish the installation.





安装完成

## 五、Kali Linux PXE 网络安装

### 配置 PXE 服务

Booting and installing Kali over the network ([PXE](#)) can be useful from a single laptop install with no CDROM or USB ports, to enterprise deployments supporting pre-seeding of the Kali installation.

First, we need to install *dnsmasq* to provide the DHCP/TFTP server and then edit the *dnsmasq.conf* file.

```
apt-get install dnsmasq
nano /etc/dnsmasq.conf
```

In *dnsmasq.conf*, enable DHCP, TFTP and PXE booting as shown below, changing the *dhcp-range* to match your environment:

```
interface=eth0
dhcp-range=192.168.8.100, 192.168.8.254, 12h
dhcp-boot=pxelinux.0
enable-tftp
tftp-root=/tftpboot/
```

With the edits in place, the dnsmasq service needs to be restarted in order for the changes to take effect.

```
service dnsmasq restart
```

## Download Kali PXE Netboot Images

Now, we need to create a directory to hold the Kali Netboot image and download the image we wish to serve from the Kali repos.

```
mkdir -p /tftpboot
cd /tftpboot
# for 64 bit systems:
wget http://repo.kali.org/kali/dists/kali/main/installer-amd64/current/images/netboot/netboot.tar.gz
# for 32 bit systems:
wget http://repo.kali.org/kali/dists/kali/main/installer-i386/current/images/netboot/netboot.tar.gz
tar xzpf netboot.tar.gz
rm netboot.tar.gz
```

## Configure Target to Boot From Network

With everything configured, you can now boot your target system and configure it to boot from the network. It should get an IP address from your PXE server and begin booting Kali.

## 03. Kali Linux 一般应用

### 一、Kali Linux 电子取证模式

BackTrack Linux 引入了 Forensic Boot 启动选项, BackTrack 5 里也有, 现在 Kali Linux 里依然有这个选项。基于 backtracklinux 的广泛传播, Forensic Boot 也被证明是非常的流行。许多人都备着 Kali Linux, 以便在需要取证时方便的用上。它集成了流行的开源取证工具, Kali 是在你需要做开源取证工作时非常趁手的工具。



启动到 forensic boot 模式后，你会发现这个模式有一些非常重要的改变。

1. 首先，不会触及到内部硬盘。这意味着 SWAP 分区和内部硬盘分区不会被自动挂载。为了验证这一点，我们找来一个标准系统然后拆掉硬盘。用商业的取证软件获取这块硬盘的 Hash。然后再把它接回到电脑上用 Kali 的取证启动模式启动。在使用了 Kali 一段时间后，我们关机，再次拆除硬盘并获取它的 Hash。两个 Hash 一直，表明了硬盘没有任何改变。
2. 其次，很重要的一点，我们修改了自动挂载任意可卸载媒体为禁用。所以插入 U 盘，光盘，等等时将不会被自动挂载。这个想法的由来很简单：用户不操作不会改变任何媒介。有改变都是用户所为。

如果你有兴趣在现实中用 Kali 任意类型的取证，我们希望你不要以为我们只是在危言耸听。不管在什么情况下使用取证工具都应该确保知道它们在做什么。

## 二、Kali 虚拟机安装 VMware Tools

我们建议你自己创建一台 Kali Linux 的 VMware 虚拟机，而不是使用我们预先提供的 VMware 镜像，进行如下的操作以便在 Kali 虚拟机成功安装 VMware Tools。你可以选择安装 `open-vm-tools`，或自带的 `VMware tools`。

### 安装 open-vm-Tools

这可能是在 Kali 虚拟机里实现 VMware Tools 功能最容易的方法。

```
apt-get install open-vm-tools
```

### 在 Kali 里安装 VMware Tools

如果 `open-vm-tools` 不能用，或者你更偏向于使用 VMware Tools，开始安装一些 VMware Tools 安装器需要的包：

```
apt-get install gcc make linux-headers-$(uname -r)
ln -s /usr/src/linux-headers-$(uname -r)/include/generated/uapi/linux/version 0 h
/usr/src/linux-headers-$(uname -r)/include/linux/
```

下一步，通过点击菜单里的 Install VMware Tools 挂载 VMware Tools 的 ISO。虚拟机的光驱连接到 VMware Tools ISO 后，我们挂载驱动器然后复制 VMware Tools 安装器到 `/tmp/` 目录下。

```
mkdir /mnt/vmware
mount /dev/cdrom /mnt/vmware/
cp -rf /mnt/vmware/VMwareTools* /tmp/
```

最后，进到 `/tmp/` 目录，解压缩然后开始安装：

```
cd /tmp/
tar xzpf VMwareTools-*.tar.gz
cd vmware-tools-distrib/
./vmware-tools-install
```

照着上面的命令，VMware Tools 就安装好了。

## VMware 里鼠标移动很慢

如果在 Kali Linux 的 VMware 虚拟机里，你的鼠标移动很慢或者反应很迟钝。尝试在 Kali 虚拟机里安装 `xserver-xorg-input-vmouse` 这个包。

```
apt-get install xserver-xorg-input-vmouse
reboot
```

## VMWare Tools 不能编译！

这是个经常折磨我们不幸的事实，例如 Kali Linux 用了 VMware 还没有支持的太新的内核。有时，可能需要在 VMware 社区寻找兼容的 VMware Tools 补丁。

## 已知问题

截至 2013 年 3 月 2 日为止。VMware Tools 已经在 3.7 内核编译通过，除了共享文件夹模块不能正常工作外。已经有[补丁](#)可以解决这个问题。

## 三、运行 Metasploit Framework

依照 Kali Linux 网络服务策略，Kali 没有自动启动的网络服务，包括数据库服务在内。所以为了让 Metasploit 以支持数据库的方式运行有些必要的步骤。

### 启动 Kali 的 PostgreSQL 服务

Metasploit 使用 [PostgreSQL](#) 作为数据库，所以必须先运行它。

```
service postgresql start
```

你可以用 `ss -ant` 的输出检验 PostgreSQL 是否在运行，然后确认 5432 端口处于 listening 状态。

```
State Recv-Q Send-Q Local Address: Port Peer Address: Port
LISTEN 0 128 ::: 22 ::: *
LISTEN 0 128 *: 22 *: *
LISTEN 0 128 127.0.0.1: 5432 *: *
LISTEN 0 128 :: 1: 5432 ::: *
```

## 启动 Kali 的 Metasploit 服务

随着 PostgreSQL 的启动和运行，接着我们要运行 Metasploit 服务。第一次运行服务会创建一个 msf3 数据库用户和一个叫 msf3 的数据库。还会运行 Metasploit RPC 和它需要的 WEB 服务端。

```
service metasploit start
```

## 在 Kali 运行 msfconsole

现在 PostgreSQL 和 Metasploit 服务都运行了，可以运行 **msfconsole**，然后用 **db\_status** 命令检验数据库的连通性。

```
msfconsole
msf > db_status
[*] postgresql connected to msf3
msf >
```

## 配置 Metasploit 随系统启动运行

如果你想 PostgreSQL 和 Metasploit 在开机时运行，你可以使用 **update-rc.d** 启用服务。

```
update-rc.d postgresql enable
update-rc.d metasploit enable
```

## 四、 建立你自己的卡利 ISO

Building a customized Kali ISO is easy, fun, and rewarding. You can configure virtually every aspect of your custom Kali ISO build using the Debian [live-build](#) scripts. These scripts allow one to easily build live system images by providing a framework that uses a configuration set to automate and customize all aspects of building the image. We have adopted these scripts and use them for the official Kali ISO releases.

### Prerequisites

Ideally, you should build your custom Kali ISO from within a pre-existing Kali environment. However, if this is not the case for you, make sure



you are using the latest version of live-build (in the 3.x branch which targets Debian wheezy)。

## Getting Ready

We first need to prepare the Kali ISO build environment with the following commands:

```
apt-get install git live-build cdebootstrap
git clone git://git.kali.org/cdimage.kali.org
cd cdimage.kali.org/live/
lb config
```

## Configuring the Kali ISO Build (Optional)

Through the **config** directory, your ISO build supports significant customization options, which are well documented on the Debian [live build 3.x](#) page. However, for the impatient, the following configuration files are of particular interest:

**config/package-lists/kali.list.chroot** - contains the list of packages to install in the Kali ISO. You can choose specific packages to be installed, while dropping others. This is also where you can [change your Kali ISO Desktop Environment](#) (KDE, Gnome, XFCE, LXDE, etc)。

**hooks/** - The hooks directory allows us to hook scripts in various stages of the Kali ISO live build. For more information about hooks, refer to the [live build manual](#). As an example, Kali adds its forensic menu this way:

```
$ cat config/hooks/forensic-menu.binary
#!/bin/sh
```

```
cat >>binary/isolinux/live.cfg <<END
```

```
label live-forensic
    menu label ^Live (forensic mode)
    linux /live/vmlinuz
    initrd /live/initrd.img
    append boot=live noconfig username=root hostname=kali noswap noautomount
END
```

欢迎点击这里的链接进入精彩的[Linux公社](http://www.Linuxidc.com) 网站

Linux公社（[www.Linuxidc.com](http://www.Linuxidc.com)）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

[Linux公社](http://www.Linuxidc.com)是专业的Linux系统门户网站，实时发布最新Linux资讯，包括Linux、Ubuntu、Fedora、RedHat、红旗Linux、Linux教程、Linux认证、SUSE Linux、Android、Oracle、Hadoop、CentOS、MySQL、Apache、Nginx、Tomcat、Python、Java、C语言、OpenStack、集群等技术。

Linux公社（[LinuxIDC.com](http://www.LinuxIDC.com)）设置了有一定影响力的Linux专题栏目。

包括：[Ubuntu 专题](#) [Fedora 专题](#) [Android 专题](#) [Oracle 专题](#) [Hadoop 专题](#) [RedHat 专题](#) [SUSE 专题](#) [红旗 Linux 专题](#) [CentOS 专题](#)



## Building the ISO

Before you generate your ISO, you can specify your required architecture, choosing either amd64 or i386. Also note that “lb build requires root rights.

```
lb config --architecture amd64 # for 64 bit
# ... or...
lb config --architecture i386 # for 32 bit
```

```
lb build
```

The last command will take a while to complete, as it downloads all of the required packages needed to create your ISO. Good time for a coffee.

## 五、更改卡利桌面环境

Although Kali Linux uses Gnome for its default desktop environment, we recognize that not all users wish to use Gnome so we have made it simple to change to a WM of your choosing. To build your own Kali ISO image with a custom Desktop Environment, start by following the [Live Build a Custom Kali ISO guide](#). Before building your ISO, edit the last section of **config/package-lists/kali.list.chroot** to contain the entries related to the desktop environment of your choice. The section starts with this comment:

```
# Graphical desktops depending on the architecture
#
# You can replace all the remaining lines with a list of the
# packages required to install your preferred graphical desktop
# or you can just comment everything except the packages of your
# preferred desktop.
```

- [KDE](#)
- [Gnome](#)
- [LXDE](#)
- [XFCE](#)
- [E17](#)
- [MATE](#)

```
kali-defaults
kali-root-login
```

`desktop-base`  
`kde-plasma-desktop`

## 六、 解决无线驱动程序问题

Troubleshooting wireless driver issues in Linux can be a frustrating experience if you don't know what to look for. This article is meant to be used as a general guideline to better help you find the information you need to solve your wireless issues.

Carefully read carefully ANY error message as they will VERY OFTEN tell you what's wrong and how to fix it. If not, then use your Google-Fu.

### 1. 找不到网卡

- Stupid question: Is it a wireless card? (We've seen that several times)
- Is the device plugged in?
- Does it show up on **lsusb** or **lspci** (with the exception of phones)? You might want to update pci ids and usb ids
- Does **dmesg** contain any information about the driver loading and/or failing
- Is Kali a VM? Then, unless your card is USB, it will not be useable (VMWare/VirtualBox/QEMU will virtualize EVERY PCI device). Is it attached to the VM?
- If there is nothing in **dmesg** and it's not in a VM, then you might want to try the latest *compat-wireless* (and sometimes, you'll need firmware) -> check on Linux-Wireless drivers

### 2. 找到网卡但不能进行任何操作

- Read error messages
- If there are no error messages, then run **dmesg | tail** and it will most likely tell you what's wrong
- Firmware might be missing
- Check rfkill and any hardware switches and BIOS options

### 3. 网卡没监听模式

- STA drivers (Ralink, Broadcom) and every other manufacturer's provided driver doesn't support monitor mode
- ndiswrapper doesn't support monitor mode AND NEVER WILL.

- Airodump-ng/Wireshark don't show any packets: check rfkill and any hardware switches and BIOS options

## 4. 网卡不能注入

- Test with aireplay-ng -9 (Make sure the card is in monitor mode with airmon-ng)
- Airmon-ng doesn't display chipset information: It's not a big issue as it just didn't get that information from the card and doesn't change the abilities of your card
- No injection but monitor mode: Check rfkill and any hardware switches and BIOS options
- Network managers sometimes interfere with Aircrack tools. run **airmon-ng check kill** to kill these processes.

## 其他有用链接

- [Will my card work with Aircrack-ng?](#)
- [Compat-wireless](#)

# 04. Kali Linux ARM 应用

## 一、准备 Kali Linux ARM chroot

虽然你能从下载区[下载 Kali ARM 镜像](#)但是有人更热衷于定制他们的 Kali rootfs。如下展示一个制作 Kali armhf rootfs 的例子。

## 安装需要的软件和依赖

```
apt-get install debootstrap qemu-user-static
```

## 定义架构和定制包

这里定义一些你需要 ARM 架构 (armel 或 armhf) 的环境变量, 下列的包将会安装到你的镜像里。这是全文要用到的, 所以务必根据你的需要修改它们。

```
export packages="xfce4 kali-menu kali-defaults nmap openssh-server"
export architecture="armhf"
#export disk="/dev/sdc"
```

## 建立 Kali rootfs

我们创建一个标准的目录结构并从 Kali Linux 的源用 bootstrap 获得 ARM rootfs。然后我们从我们的主机复制 `qemu-arm-static` 到 rootfs, 以便进行第 2 步。

```
cd ~
mkdir -p arm-stuff
cd arm-stuff/
mkdir -p kernel
mkdir -p rootfs cd rootfs
debootstrap --foreign --arch $architecture kali kali-$architecture http://repo.kali.org/kali
cp /usr/bin/qemu-arm-static kali-$architecture/usr/bin/
LANG=C chroot kali-$architecture
/debootstrap/debootstrap --second-stage
```

## 第 2 步 chroot

这里我们配置基本的镜像设置, 例如 keymaps, 源, 默认网络接口特性 (有需要的话请修改) 等..

```
cat << EOF > kali-$architecture/debconf.set
console-common console-data/keymap/policy      select Select keymap from full list
console-common console-data/keymap/full        select en-latin1-nodeadkeys
EOF
```

```
cat << EOF > kali-$architecture/etc/apt/sources.list
deb http://repo.kali.org/kali kali main contrib non-free
deb http://repo.kali.org/security kali/updates main contrib non-free
EOF
```

```
echo "kali" > kali-$architecture/etc/hostname
```

```
cat << EOF >    kali-$architecture/etc/network/interfaces
auto lo
iface lo inet loopback
auto usbmon0
iface usbmon0 inet dhcp
EOF
```

### 第 3 步 chroot

这里开始定制。\$Packages 变量表示这个包将会被安装，默认 root 的密码将被设置为 toor，以及修改和修复其它配置。

```
mount -t proc proc kali-$architecture/proc mount -o bind /dev/ kali-$architecture/dev/ mount -o
bind /dev/pts kali-$architecture/dev/pts
cat << EOF >    kali-$architecture/third-stage
#!/bin/bash debconf-set-selections /debconf。set
rm -f /debconf。set
apt-get update
apt-get -y install git-core binutils ca-certificates
apt-get -y install locales console-common less nano git
echo "root: toor" | chpasswd
sed -i -e 's/KERNEL! ="eth*/KERNEL! ="/' /lib/udev/rules.d/75-persistent-net-generator.rules
rm -f /etc/udev/rules.d/70-persistent-net.rules
apt-get --yes --force-yes install $packages
rm -f /third-stage
EOF
```

```
chmod +x kali-$architecture/third-stage
LANG=C chroot kali-$architecture /third-stage
```

### 在 chroot 环境中手动配置

如果有需要，你可以手工在 rootfs 环境里进行最终和必要的修改。

```
LANG=C chroot kali-$architecture
{ 在 chroot 环境里做额外的修改 }
exit
```



## 清理 chroot 环境里的被锁文件

事实上在 rootfs 里一些你已经安装的包可能会产生被锁文件(例如在 chroot 环境里运行中的服务)，需要在我们能关闭 chroot 时释放。在你 umount 之前可能需要在 chroot 环境里停止一些服务。umount proc 和 dev 的命令：

```
umount kali-$architecture/proc umount kali-$architecture/dev/pts umount kali-$architecture/dev/
```

然而，如果仍然有服务在 chroot 里运行，将会出现这样的错误提示：

```
root@rootfs-box: ~ umount kali-$architecture/proc
root@rootfs-box: ~ umount kali-$architecture/dev/pts
root@rootfs-box: ~ umount kali-$architecture/dev/
umount: kali-armhf/dev: device is busy. (In some cases useful info about processes that use the
device is found by lsof(8) or fuser(1)) root@rootfs-box: ~
```

如果出现这种情况，请用如下命令检查哪个文件/服务锁住了 chroot：

```
root@rootfs-box: ~/arm-stuff/rootfs: ~ lsof |grep kali-armhf
..。
dbus-daem 4419 messagebus mem REG 8,1 236108 15734602 dbus-daemon
dbus-daem 4419 messagebus mem REG 8,1 93472 17705250 ld-2.13.so ..。
dbus-daem 4419 messagebus mem REG 8,1 100447 17705251 libpthread-2.13.so
dbus-daem 4419 messagebus mem REG 8,1 22540 17705240 librt-2.13.so
dbus-daem 4419 messagebus mem REG 8,1 893044 17705232 libc-2.13.so ..。
```

从输出信息我们看到 dbus 守护进程仍在 chroot 环境里运行。在继续之前，我们需要在 chroot 环境里停止它。如果你已经成功 umount 了 proc 或 dev，请用之前给出的命令重新挂载他们，chroot 到 rootfs 里，然后停止 dbus 服务(或别的可能需要停止的服务)：

```
# mount -t proc proc kali-$architecture/proc
# mount -o bind /dev/ kali-$architecture/dev/pts
LANG=C chroot kali-$architecture /etc/init.d/dbus stop exit
```

一旦释放了所有的服务和被锁文件，你就可以 umount proc 和 dev 了：

```
root@rootfs-box: ~/arm-stuff/rootfs~ umount kali-$architecture/proc
root@rootfs-box: ~/arm-stuff/rootfs~ umount kali-$architecture/dev/pts
root@rootfs-box: ~/arm-stuff/rootfs~ umount kali-$architecture/dev/
root@rootfs-box: ~/arm-stuff/rootfs~
```

## 清理

最后我们运行在 chroot 里的清理脚本释放缓存文件占用的空间,还有需要的清理工作:

```
cat << EOF > kali-$architecture/cleanup
#!/bin/bash rm -rf /root/.bash_history
apt-get update apt-get clean
rm -f cleanup
EOF

chmod +x kali-$architecture/cleanup
LANG=C chroot kali-$architecture /cleanup
/etc/init.d/dbus stop
umount kali-$architecture/proc
umount kali-$architecture/dev/pts
umount kali-$architecture/dev/
cd ..
```

恭喜! 你定制的 Kali ARM rootfs 就在 kali-\$architecture 目录里。你可以为往后的工作打包这个目录, 或复制到一个镜像文件。

## 二、 在 ODRROID U2 安装 Kali ARM



## Odroid U2 / X2

ODROID U2 棘手的部分是没有终端输出。理论上，购买 ODROID 时，你还应该买一根 USB UART 线，用于串口调试引导过程。话说，这些机器(目前)最引人注目的是他们的尺寸，功率和可用内存。

### ODROID U2 上的 Kali – 用户指南

如果你想在超棒的 ODROID 上安装 Kali，按照下列步骤：

1. 一张至少 8G 的高速 SD 卡，最好是 Class 10 的。
2. 在我们的[下载区](#)下载 ODROID U2 镜像。
3. 用 **dd** 命令把镜像文件写入到 SD 卡。本例中，假设存储设备的设备块名是/dev/sdb。  
如果有变，自行更改。

**警告！** 这步将会擦除 SD 卡内的数据，如果选择了错误的存储设备，会导致硬盘数据丢失。

```
dd if=kali-ordoidu2.img of=/dev/sdb bs=1M
```

这步需要的时间取决于你的 USB 存储设备的速度和镜像大小. dd 命令完成, 把插入 SD 卡到 Odroid 再启动。你将可以在 Gnome 登录页面用 (root/toor) 登录。就这样, 完成了!

## 疑难排解

要排除 Odroid 引导过程的故障, 你需要连接 UART 串口线到 odroid。连上线之后, 你可以发出如下命令连接终端:

```
screen /dev/ttySAC1 115200
```

## ODROID U2 上的 Kali – 开发者指南

如果你是个开发者, 并且想鼓捣 Kali 的 ODROID 镜像, 包括修改内核配置。查阅我们的文章[定制 Kali ODROID 镜像](#)。

## 三、 在三星 Chromebook 安装 Kali ARM



## Samsung ARM Chromebook

三星 ARM chromebook 是一台超级本。很具挑战性，但我们有在 Chromebook 运行良好的 Kali 镜像。

我们的 Chromebook Kali 镜像包含两个引导分区，其中一个的内核强制从 SD 卡引导，另一个的内核强制从 USB 引导。根据你使用的 USB 存储媒介的类型，确保在你用 dd 把镜像克隆到你的 USB 设备后用更高的优先级标记相应的引导分区，本指南的最后阶段将会提及。

### Kali 在 Chromebook 上 – 用户指南

如果你想安装 Kali 到你的 Samsung ARM Chromebook，按照下列步骤：

1. 准备一块高速的 8G SD 卡或 U 盘。
2. 把 Chromebook 设置成开发者模式。

3. 从我们的 [downloads](#) 下载 Kali 的 Samsung ARM Chromebook 镜像。
4. 用 **dd** 命令把镜像文件克隆到 SD 卡。本例中，假设存储设备的设备块名是/dev/sdb。  
如果有变，自行更改。

**警告！** 这步将会擦除 SD 卡内的数据，如果选择了错误的存储设备，会导致硬盘数据丢失..

**dd if=kali-chromebook. img of=/dev/sdb bs=512k**

这步需要的时间取决于你的 USB 存储设备的速度和镜像大小。

就是这里，你要标记分区 1 或者分区 2 有更高的优先权。更高优先权的数字将先启动。如下的例子将把第一个分区(用-i 参数)的优先权设置成 10，因此将从 SD 卡引导成功。

**cgpt repair /dev/sdb**

**cgpt add -i 1 -S 1 -T 5 -P 10 -l KERN-A /dev/sdb**

**cgpt add -i 2 -S 1 -T 5 -P 5 -l KERN-B /dev/sdb**

使用 **cgpt show** 命令查看分区的列表和引导顺序。

```
root@kali: ~# cgpt show /dev/sdb
```

start	size	part	contents
0	1		PMBR
1	1		Pri GPT header
2	32		Pri GPT table
8192	32768	1	Label: "KERN-A" Type: ChromeOS kernel UUID: 63AD6EC9-AD94-4B42-80E4-798BBE6BE46C Attr: <b>priority=10 tries=5 successful=1</b>
40960	32768	2	Label: "KERN-B" Type: ChromeOS kernel UUID: 37CE46C9-0A7A-4994-80FC-9C0FFCB4FDC1 Attr: <b>priority=5 tries=5 successful=1</b>
73728	3832490	3	Label: "Linux filesystem" Type: 0FC63DAF-8483-4772-8E79-3D69D8477DE4 UUID: E9E67EE1-C02E-481C-BA3F-18E721515DBB
125045391	32		Sec GPT table
125045423	1		Sec GPT header

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

dd 命令操作完成后，插入 SD 卡/U 盘启动 Chromebook(不要插在蓝色的 USB 口！)。在开发者引导提示里按 CTRL + ALT + U 引导进入到 Kali Linux。用(root / toor)登录到 Kali，然后运行 **startx**。就这样，大功告成！！

## Kali 在 Chromebook 上 – 开发指南

如果你是一个开发者，想鼓捣 Kali Samsung Chromebook 的镜像，包括修改内核配置或更具冒险精神的尝试，请查阅我们的文章[定制 Chromebook 内核/镜像](#)。

## 四、在 Raspberry Pi 安装 Kali ARM



# Raspberry Pi

树莓 Pi 是个低端，低成本的 ARM 电脑。忽略它的不是很显著的配置，它的廉价使它成为 Tiny Linux 系统的首选，并且他能做的远远不止媒体 PC 而已。



## 存储 Kali 在树莓 Pi – 简单版

如果你想安装 Kali 到你的树莓 Pi，按照下列步骤：

1. 一张至少 8G 的高速 SD 卡，最好是 Class 10 的。
2. 在我们的[下载区](#)下载 Kali Linux 树莓 Pi 镜像。
3. 用 **dd** 命令把镜像文件写入到 SD 卡。本例中，假设存储设备的设备块名是/dev/sdb。  
如果有变，自行更改。

**警告！** 这步将会擦除 SD 卡内的数据，如果选择了错误的存储设备，会导致硬盘数据丢失。

```
root@kali: ~ dd if=kali-pi.img of=/dev/sdb bs=512k
```

这步需要的时间取决于你的 USB 存储设备的速度和镜像大小。dd 命令完成，把插入 SD 卡到树莓 Pi 再启动。你将可以用 (root/toor) 登录，然后用 **startxstartx** 启动图形界面。就这样，完成了！

## 存储 Kali 在树莓 Pi – 复杂版

如果你是个开发者，你想修改 Kali Linux 树莓 Pi 的镜像，包括修改内核配置，查阅我们的文章定制树莓 Pi 镜像(敬请期待)。 内容待定。

# 05. Kali Linux 开发

## 一、 ARM 交叉编译

本文档说明如何在 kali linux 上配置 ARM 交叉编译环境，是我们多份关于定制 ARM 镜像的文档的起点。

## 开发机的配置

编译内核生成镜像通常需要大量硬盘空间。确保你的开发机至少有 50G 可用硬盘空间以及足够的内存，CPU 不要太差。

## 安装依赖

先安装 ARM 交叉编译所需的依赖。

```
apt-get install git-core gnupg flex bison gperf libbsd0-dev build-essential  
zip curl libncurses5-dev zlib1g-dev libncurses5-dev gcc-multilib g++-multilib
```

如果你是 64 位的 Kali Linux 系统，用如下命令添加 i386 架构支持到你的开发环境。

```
dpkg --add-architecture i386  
apt-get update  
apt-get install ia32-libs
```

## 下载 Linaro 工具链

从我们的 Git 源下载 Linaro 交叉编译器。

```
cd ~  
mkdir -p arm-stuff/kernel/toolchains  
cd arm-stuff/kernel/toolchains  
git clone git://github.com/offensive-security/arm-eabi-linaro-4.6.2.git
```

## 设置环境变量

为了能使用 Linaro 交叉编译器，你需要在你的 session 里设置如下的环境变量。

```
export ARCH=arm  
export CROSS_COMPILE=~/.arm-stuff/kernel/toolchains/arm-eabi-linaro-4.6.2/bin/arm-eabi-
```

现在你的 ARM 交叉编译环境完成了，可以编译属于你自己的 ARM 内核了。

## 二、重新编译 Kali Linux 内核

有时你可能想添加必要的驱动，补丁，或者不包含在 Kali Linux 里的内核功能。如下的教程描述如何快速修改和编译 Kali Linux 内核为你所需。请注意目前默认的 Kali Linux 内核已经打了大量的无线注入补丁。

### 安装编译所需的依赖

```
apt-get install kernel-package ncurses-dev fakeroot bzip2
```

## 下载 Kali Linux 内核源代码

```
apt-get install linux-source
cd /usr/src/
tar jxpf linux-source-3.7.tar.bz2
cd linux-source-3.7/
```

## 配置内核

复制 Kali 默认的内核配置文件然后修改为你所需。这一步你需要应用各种驱动，补丁，等等...在此例中，我们重新编译一个 64 位内核。

```
cp /boot/config-3.7-trunk-amd64 .config
make menuconfig
```

## 编译内核

编译你修改过的内核。需要花的时间和硬件配置有关。

```
CONCURRENCY_LEVEL=$(cat /proc/cpuinfo|grep processor|wc -l)
make-kpkg clean
fakeroot make-kpkg kernel_image
```

## 安装新内核

内核编译成功后。继续以安装新内核，然后重启。请注意内核版本号可能会变。在此例中，当前的内核版本是 3.7.2，你需要根据情况做相应的修改。

```
dpkg -i ../linux-image-3.7.2-3.7.2-10.00.Custom_amd64.deb
update-initramfs -c -k 3.7.2
update-grub2
reboot
```

重启后，你的新内核应该运行了。如果出错了导致你的内核不能启动，你仍然可以通过启动官方的 Kali Linux 内核来解决问题。

## 三、从源代码编译包

有时，我们需要从源代码重新编译一个 Kali 包。幸运的是用 APT 下载源代码包，进行必要的修改后再用 Debian 工具重新编译是如此的简单。此例中，为了添加额外的 Mifare Key 硬编码到 mifare 格式化工具，我们将重新编译 [libfreefare](#) 这个包。

## 下载包的源代码

```
# Get the source package
apt-get source libfreefare
cd libfreefare-0.3.4~svn1469/
```

## 修改包的源代码

按需修改包里面的源代码文件，此例中，我们以修改 mifare-classic-format.c 为例。

```
nano examples/mifare-classic-format.c
```

## 检查编译所需的依赖

检查编译包所需的依赖。它们需要在编译包前被安装。

```
dpkg-checkbuilddeps
```

输出的结果和如下类似，在于你已经安装了什么包。如果 dpkg-checkbuilddeps 没有任何输出，说明你没有缺少依赖，可以继续编译。

```
dpkg-checkbuilddeps:  Unmet build dependencies:  dh-autoreconf libnfc-dev
```

## 安装编译所需的依赖

安装上面 dpkg-checkbuilddeps 输出的编译所需的依赖：

```
apt-get install dh-autoreconf libnfc-dev
```

## 编译修改过的包

所有安装依赖安装好后，调用 dpkg-buildpackage 来编译是件很容易的事。

```
dpkg-buildpackage
```

## 安装新编译的包

如果一切顺利，你就可以安装新编译的包了。

```
dpkg -i ../libfreefare*.deb
```

# 06. Kali Linux 社区

## 一、Kali Linux 漏洞跟踪

Kali Linux 有官方的[漏洞跟踪系统](#)，用户可以提交漏洞或者补丁给开发者，或者给我们建议新的工具包含到发行版里。任何人都可以在本站注册，但是我们建议你先看如下规则，以保证漏洞用正确的信息和适当的格式正确的提交给我们。

- 漏洞追踪系统不是问题解答。
- 使用真实的 email 以便我们在将来需要的时候能及时联系你。
- 使用明确的标题。
- 尽可能多的提供细节，包括终端输出，系统架构类型和准确的版本。
- 请求新增工具必须包含新增这个工具的理由和它的 URL。
- 不要把 BUG 分给任何人提交，开发者会判断是谁发现的 BUG。

## 二、Kali Linux 官方网站

[Kali Linux](#) 的一系列网站用于给我们的用户提供服务。下列的是 Kali 官方网站以及它们的用途。请注意这些是 Kali Linux 发布权威信息来源的[唯一的官方站点](#)。

下列网站是唯一的 **Kali Linux** 发行版官方网点。

- [www.kali.org](http://www.kali.org)
- [docs.kali.org](http://docs.kali.org)
- [forums.kali.org](http://forums.kali.org)
- [bugs.kali.org](http://bugs.kali.org)
- [git.kali.org](http://git.kali.org)

[Kali Linux 主站](#)主要用于发布 Kali Linux 相关新闻，基本信息，和一般相关项目的更新。在这里你会发现与 Kali Linux 相关的新工具，功能和技巧的博文。还有这应该是你[下载](#)发行版的唯一来源。

欢迎点击这里的链接进入精彩的[Linux公社](http://www.Linuxidc.com) 网站

Linux公社（[www.Linuxidc.com](http://www.Linuxidc.com)）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

[Linux公社](http://www.Linuxidc.com)是专业的Linux系统门户网站，实时发布最新Linux资讯，包括Linux、Ubuntu、Fedora、RedHat、红旗Linux、Linux教程、Linux认证、SUSE Linux、Android、Oracle、Hadoop、CentOS、MySQL、Apache、Nginx、Tomcat、Python、Java、C语言、OpenStack、集群等技术。

Linux公社（[LinuxIDC.com](http://www.LinuxIDC.com)）设置了有一定影响力的Linux专题栏目。

包括：[Ubuntu 专题](#) [Fedora 专题](#) [Android 专题](#) [Oracle 专题](#) [Hadoop 专题](#) [RedHat 专题](#) [SUSE 专题](#) [红旗 Linux 专题](#) [CentOS 专题](#)

