

KALI LINUX 中文指南 0.2



2013/4/9

01. Kali Linux 介绍	4
一、 Kali Linux 与 Debian 的区别	4
二、 Kali Linux 商标策略	4
三、 Kali Linux 适合你么?	6
四、 Kali Linux 特性	6
五、 Kali Linux 镜像	7
六、 Kali Linux 默认密码	8
02. Kali Linux 安装	9
一、 Virtual Box 安装 Kali	9
二、 硬盘安装 Kali Linux (可选择是否加密)	11
三、 用 Live U 盘安装 Kali Linux	24
四、 Kali 和 Windows 双引导	27
五、 Kali Mini ISO 网络安装	33
六、 Kali Linux PXE 网络安装	38
七、 PXE 预启动执行环境	39
03. Kali Linux 一般应用	41
一、 Kali Linux 电子取证模式	41
二、 Kali 虚拟机安装 VMware Tools	43
三、 运行 Metasploit Framework	44
四、 封装最新的 Kali ISO	45
五、 建立你自己的卡利 ISO	46
六、 更改卡利桌面环境	47
七、 解决无线驱动程序问题	48
04. Kali Linux ARM 应用	49
一、 准备 Kali Linux ARM chroot	49
二、 在 Galaxy Note 10.1 安装 Kali ARM	53
三、 在 ODROID U2 安装 Kali ARM	55
四、 在三星 Chromebook 安装 Kali ARM	57
五、 在 Raspberry Pi 安装 Kali ARM	60
六、 在 MK/SS808 上安装 Kali ARM	62
05. Kali Linux 开发	63
一、 定制 Raspberry Pi 镜像	63
二、 定制 Chromebook 镜像	65
三、 定制 ODROID X2 U2 镜像	71
四、 定制 MK/SS808 Kali 镜像	77
五、 ARM 交叉编译	79
六、 重新编译 Kali Linux 内核	80
七、 从源代码编译包	81
06. Kali Linux 策略	83
一、 Kali Linux 工具策略	83
二、 Kali Linux Root 用户策略	83
三、 Kali Linux 开源软件策略	84
四、 Kali Linux 安全更新策略	84

五、	Kali Linux 网络服务策略	84
07.	Kali Linux 社区	85
一、	Kali Linux 漏洞跟踪	85
二、	Kali Linux IRC 频道	85
三、	Kali Linux 社区论坛	88
四、	Kali Linux 官方镜像	89
五、	Kali Linux 官方网站	92
六、	提交 Kali 的技术问题	94
七、	Kali Linux 招聘信息	104
1.	Debian 系 Linux 安全工程师	104
2.	渗透测试工程师	104
3.	脚本漏洞挖掘工程师	104
4.	逆向工程师	105
5.	各类安全培训讲师	105

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。

- **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。

六、Kali Linux 默认密码

安装 Kali 期间可以给 *root* 用户设置一个密码。但如果你用的是 live、i386、amd64、VMware 或 ARM 镜像时，*root* 的默认密码是 **toor**。

02. Kali Linux 安装

一、Virtual Box 安装 Kali

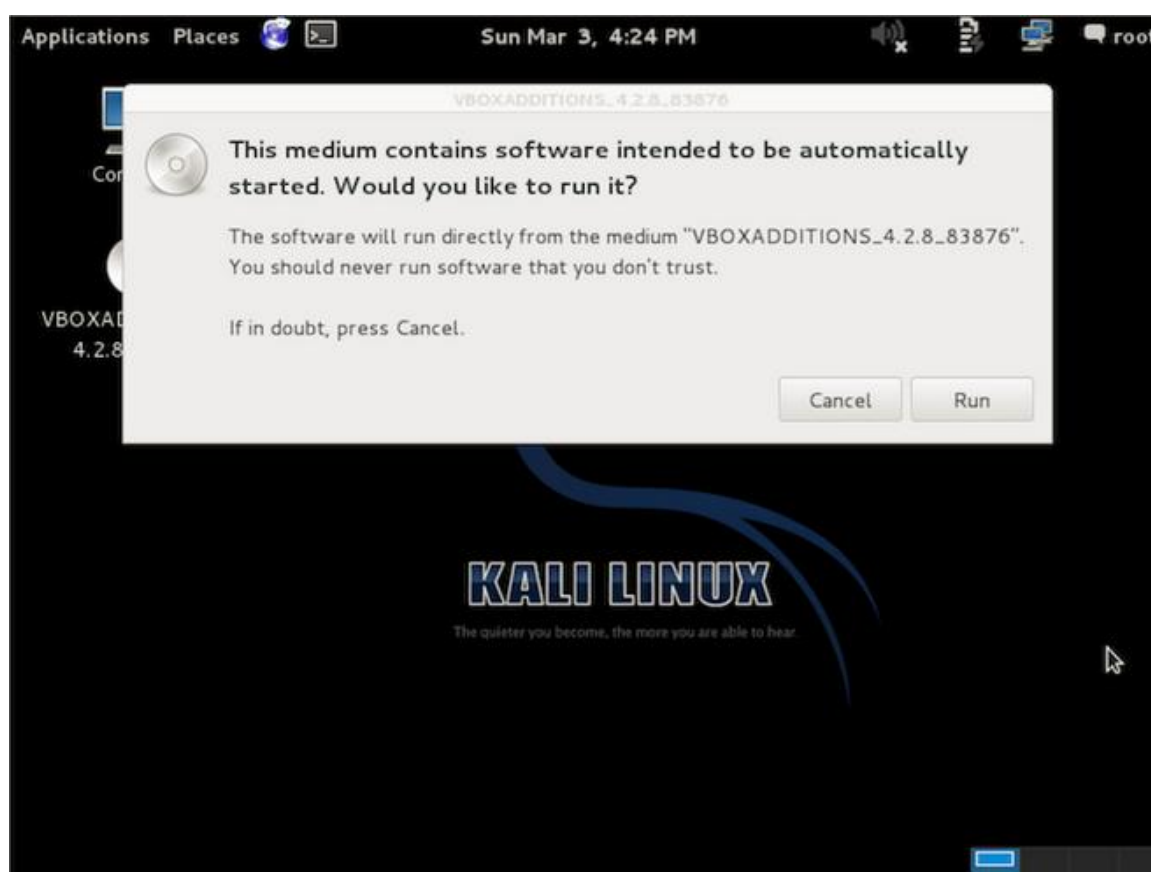
建议使用最新版的 VirtualBOX, 因为可以提升用户体验, 包括兼容性的提高, 软件核心和客户端功能增强工具的稳定性的增强.

为了整合鼠标和屏幕以及和你的宿主机共享目录, 你应该安装 VirtualBox 增强功能工具.

启动 Kali Linux 虚拟机后, 打开一个终端然执行如下命令来安装 Linux 内核头文件.

```
apt-get update && apt-get install -y linux-headers-$(uname -r)
```

安装完后, 从 VirtualBox 菜单的” Install Guest Additions” 选择’ Devices’ 来挂载客户端功能增强的 ISO 到虚拟机的 CD 光驱. 提示自动运行 CD 时, 点击取消按钮.



在终端窗口, 复制虚拟机 CD-Rom 里的 VboxLinuxAdditions.run 这个文件到本地目录, 确认有可执行权限, 然后运行该文件开始安装.

```
cp /media/cd-rom/VBoxLinuxAdditions.run /root/  
chmod 755 /root/VBoxLinuxAdditions.run
```

```
cd /root
./VBoxLinuxAdditions.run
```



```
Applications Places Sun Mar 3, 4:37 PM root
root@kali: ~
File Edit View Search Terminal Help
-r-xr-xr-x 1 root root 8181195 Mar 3 16:36 VBoxLinuxAdditions.run
root@kali:~# ./VBoxLinuxAdditions.run
Verifying archive integrity... All good.
Uncompressing VirtualBox 4.2.8 Guest Additions for Linux.....
VirtualBox Guest Additions installer
Copying additional installer modules ...
Installing additional modules ...
Saving modules configuration ...
Removing existing VirtualBox non-DKMS kernel modules ...done.
Building the VirtualBox Guest Additions kernel modules
The headers for the current running kernel were not found. If the following
module compilation fails then this could be the reason.

Building the main Guest Additions module ...done.
Building the shared folder support module ...done.
Building the OpenGL support module ...done.
Doing non-kernel setup of the Guest Additions ...done.
Starting the VirtualBox Guest Additions ...done.
Installing the Window System drivers
Installing X.Org Server 1.12 modules ...done.
Setting up the Window System to use the Guest Additions ...done.
You may need to restart the hal service and the Window System (or just restart
the guest system) to enable the Guest Additions.

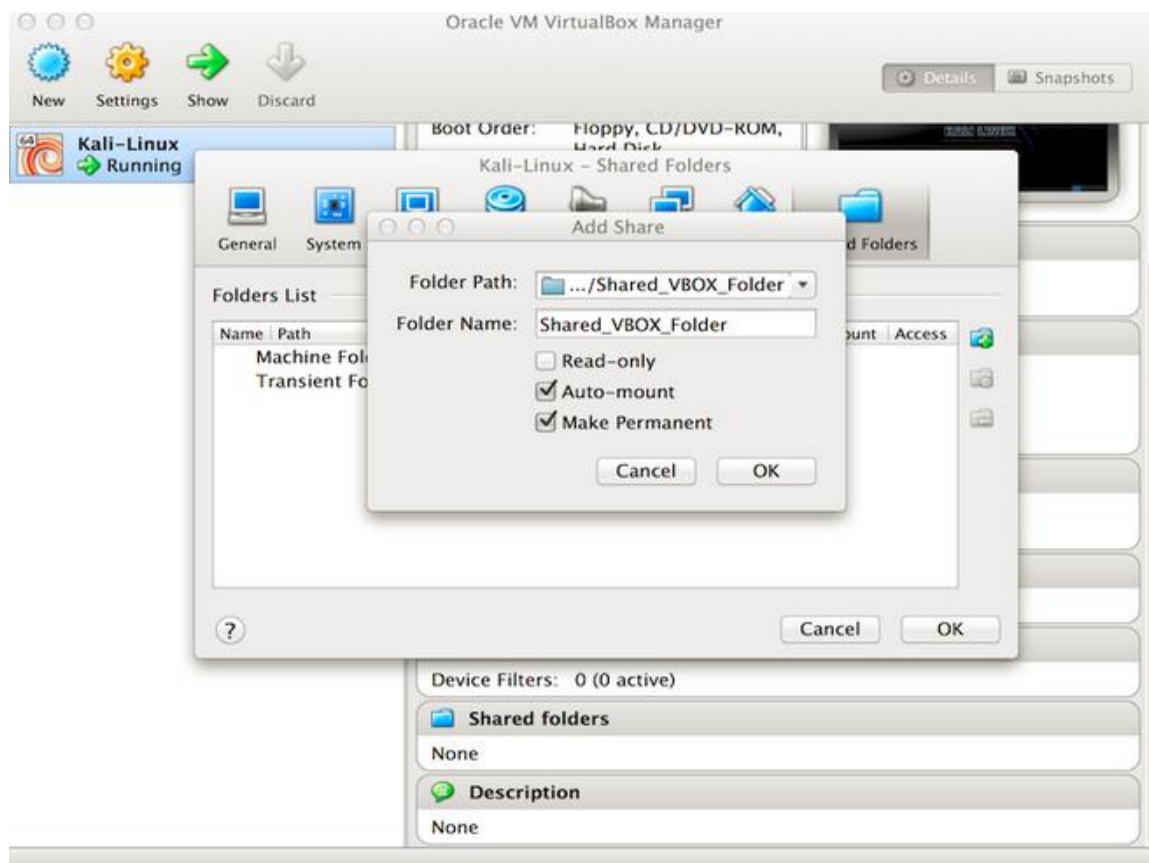
Installing graphics libraries and desktop services components ...done.
root@kali:~#
```

功能增强工具安装好后重启 Kali Linux 虚拟机。鼠标和屏幕整合好了,也可以与宿主机共享目录了。

为了共享宿主机上的目录给你的 Kali Linux 虚拟机,有一些步骤要完成。

在虚拟机管理器,选择你的 Kali Linux 虚拟机然后点击右键菜单的' Shared Folders'。会弹出一个用于添加共享目录的窗口。在这个窗口里点击图标来添加一个目录。

在 Folder Path 文本框,显示着共享文件夹的路径,或点击下拉菜单箭头来浏览宿主机的系统。勾选 Auto-mount (自动挂载)' 和' Make Permanent (永久)' 复选框,当有提示时点击 OK 按钮。



现在共享目录会出现在 media 目录里. 为了可以方便的进入到这个目录你可以创建一个书签或者链接.

二、 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

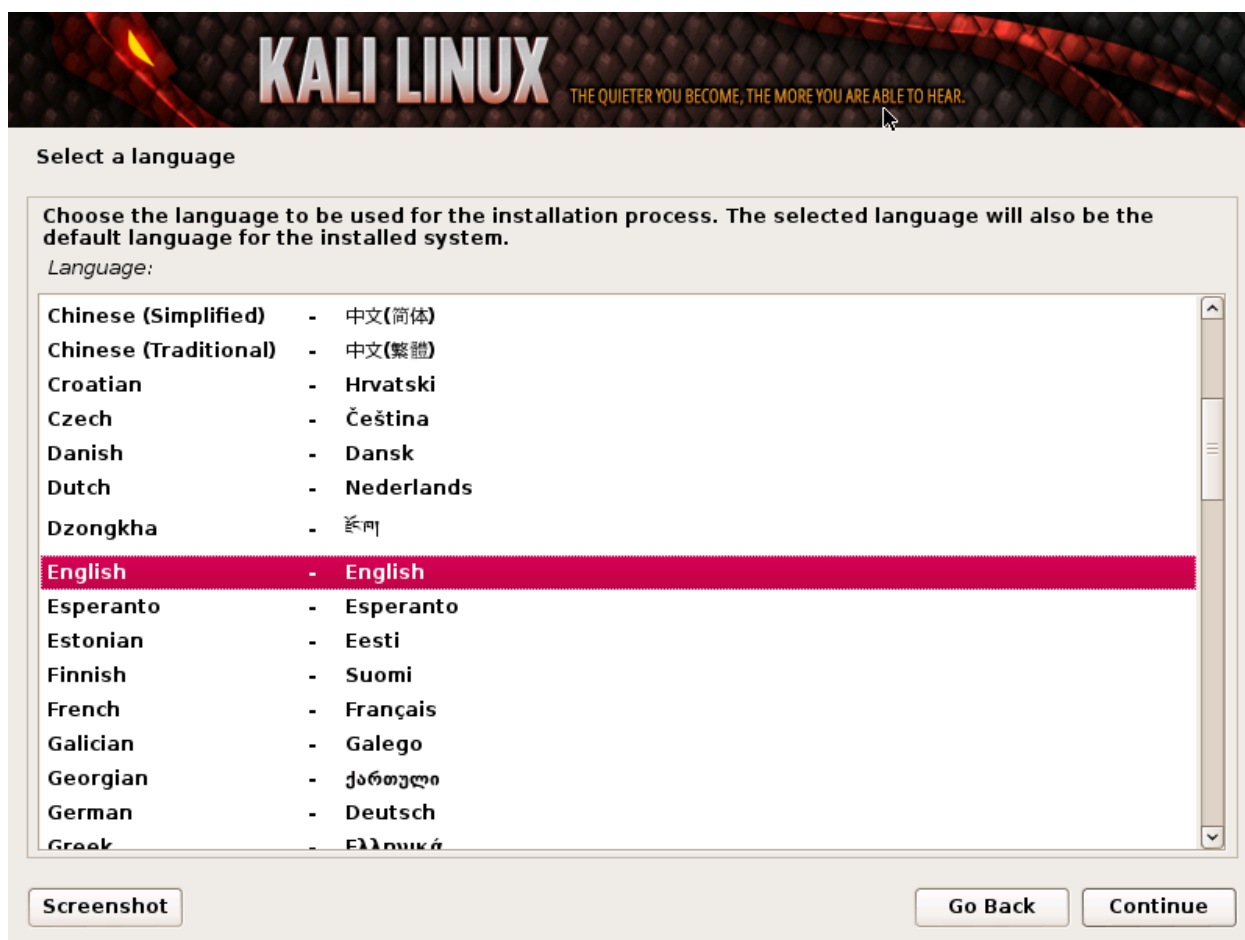
1. [下载 Kali Linux](#)。
2. 把 Kali Linux 刻录到 DVD 盘或[制作 Kali Linux 镜像 U 盘](#)。
3. 确认你电脑的 BIOS 设置了从 CD/USB 引导。

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。



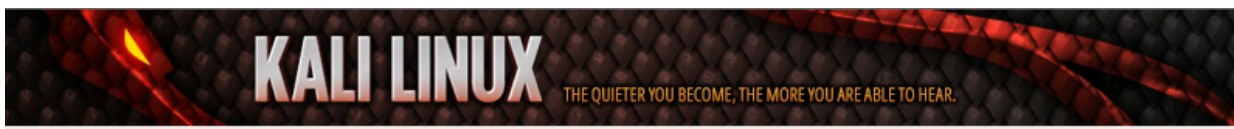
Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

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.

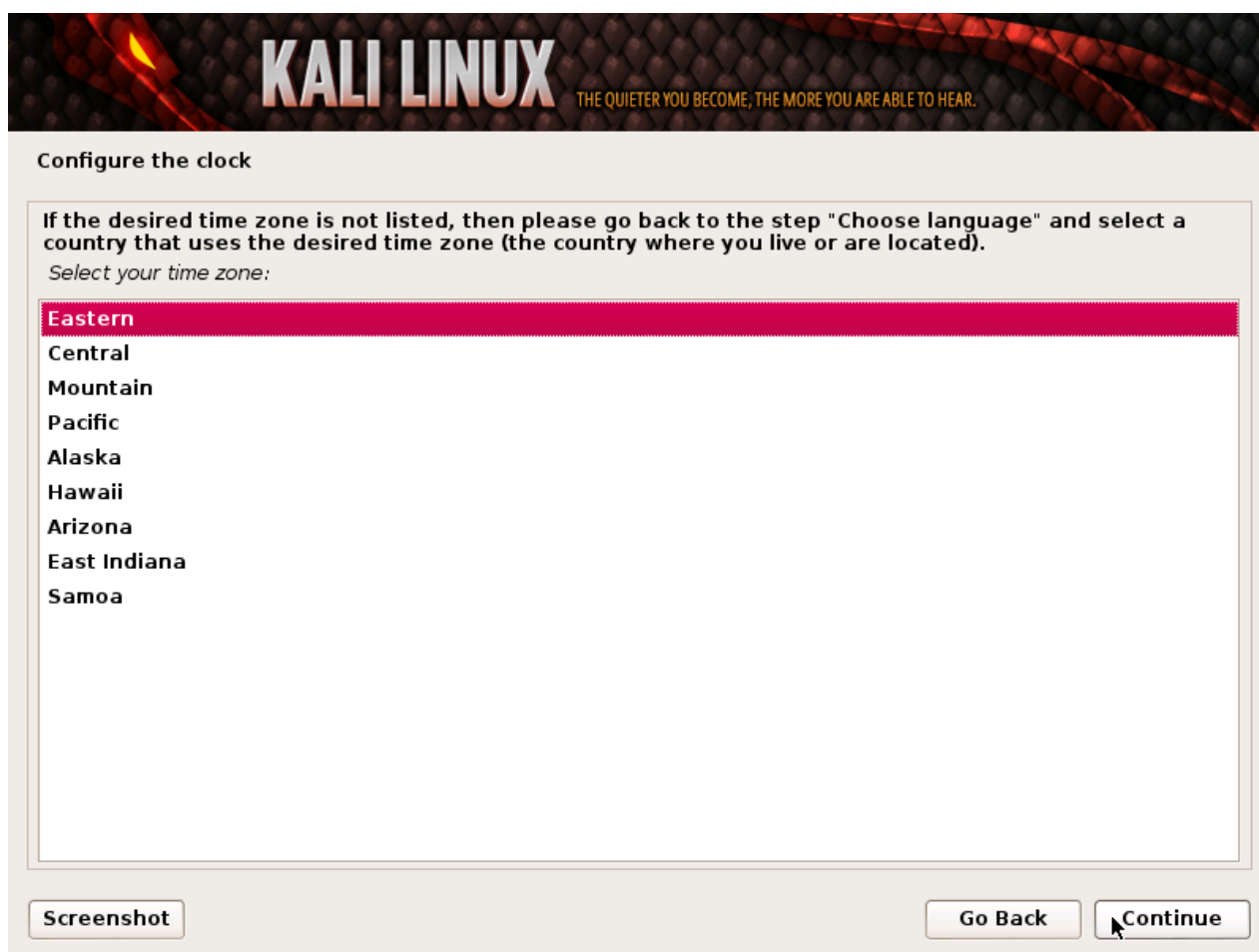
Re-enter password to verify:

[Screenshot](#)

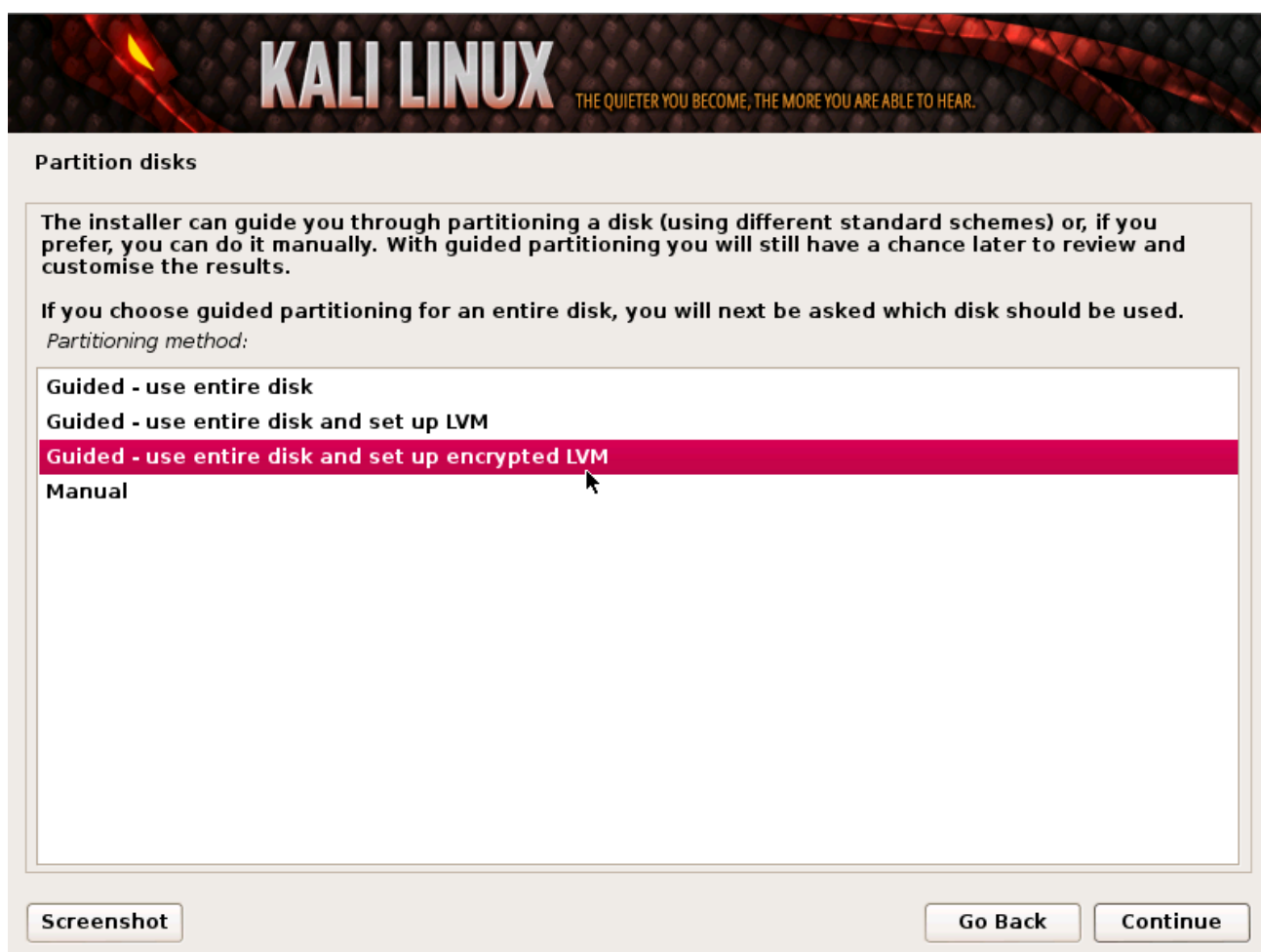
[Go Back](#)

[Continue](#)

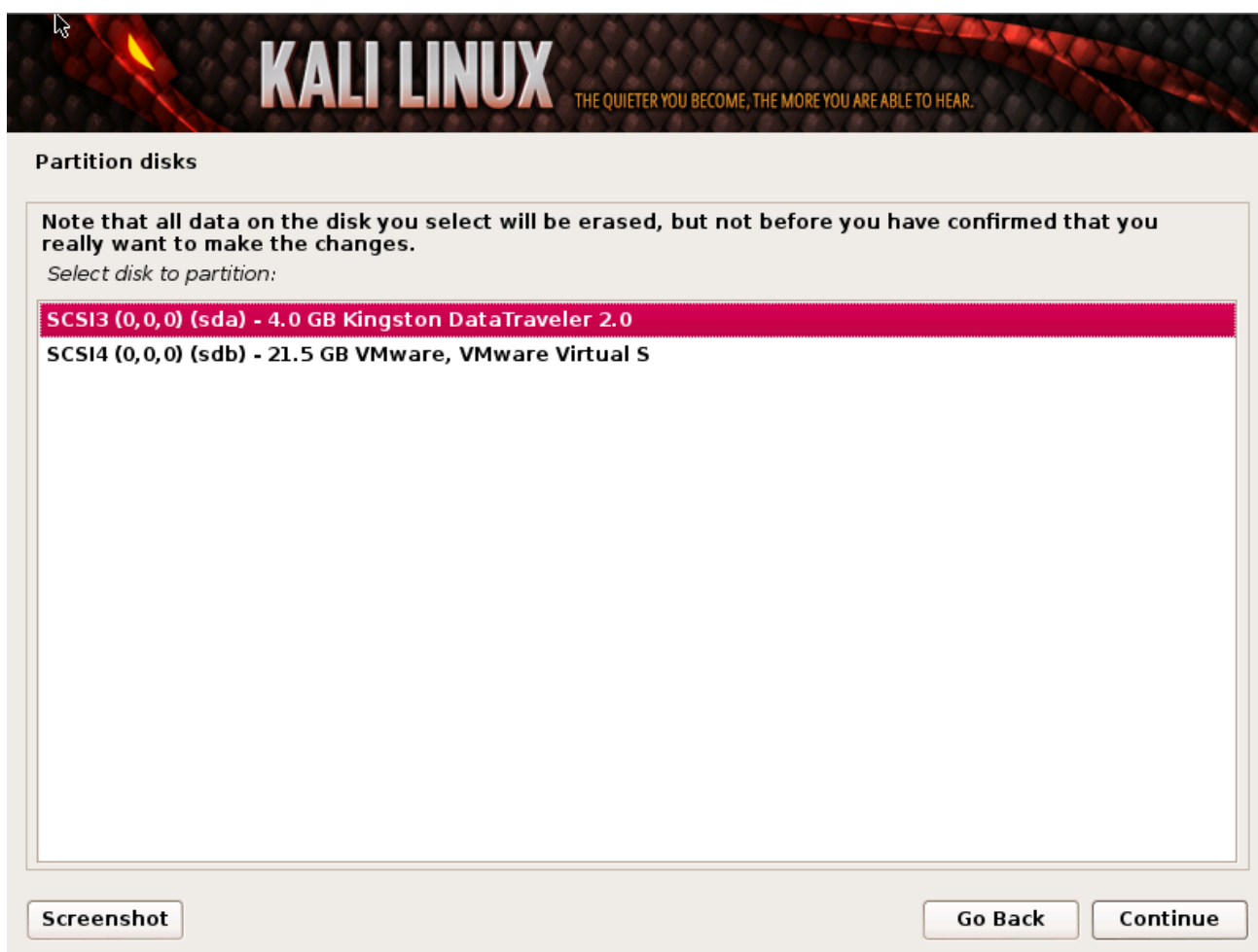
5. 下一步设置时区。



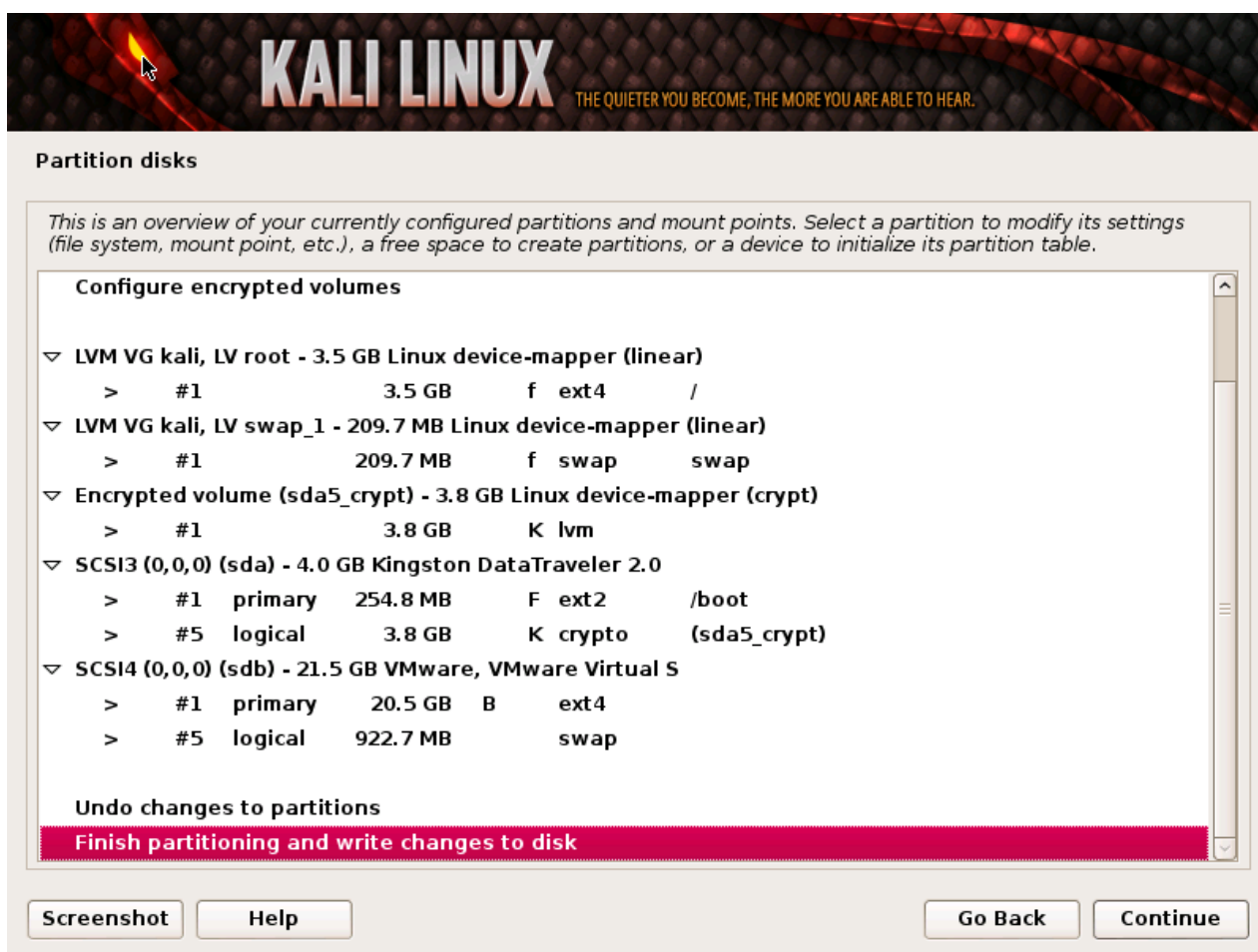
6. 安装器会检测硬盘, 并提供 4 个选项。加密 LVM 安装应选择 **Guided – use entire disk and set up encrypted LVM(使用全盘 LVM 加密卷)**“, 一般安装选择第一个选项即可。如下图所示。



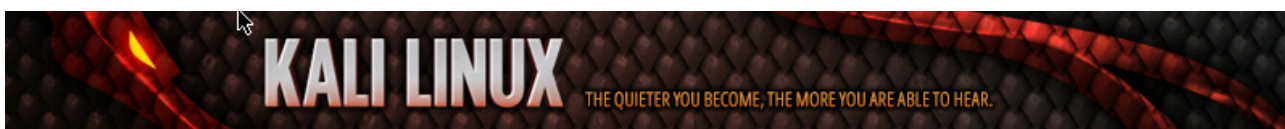
7. 选择安装 Kali 的目标驱动器。在此例中我们选择一块 U 盘作为目标驱动器。我们将用这块 U 盘来启动加密的 Kali。



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。



Partition disks

You need to choose a passphrase to encrypt SCSI3 (0,0,0), partition #5 (sda).

The overall strength of the encryption depends strongly on this passphrase, so you should take care to choose a passphrase that is not easy to guess. It should not be a word or sentence found in dictionaries, or a phrase that could be easily associated with you.

A good passphrase will contain a mixture of letters, numbers and punctuation. Passphrases are recommended to have a length of 20 or more characters.

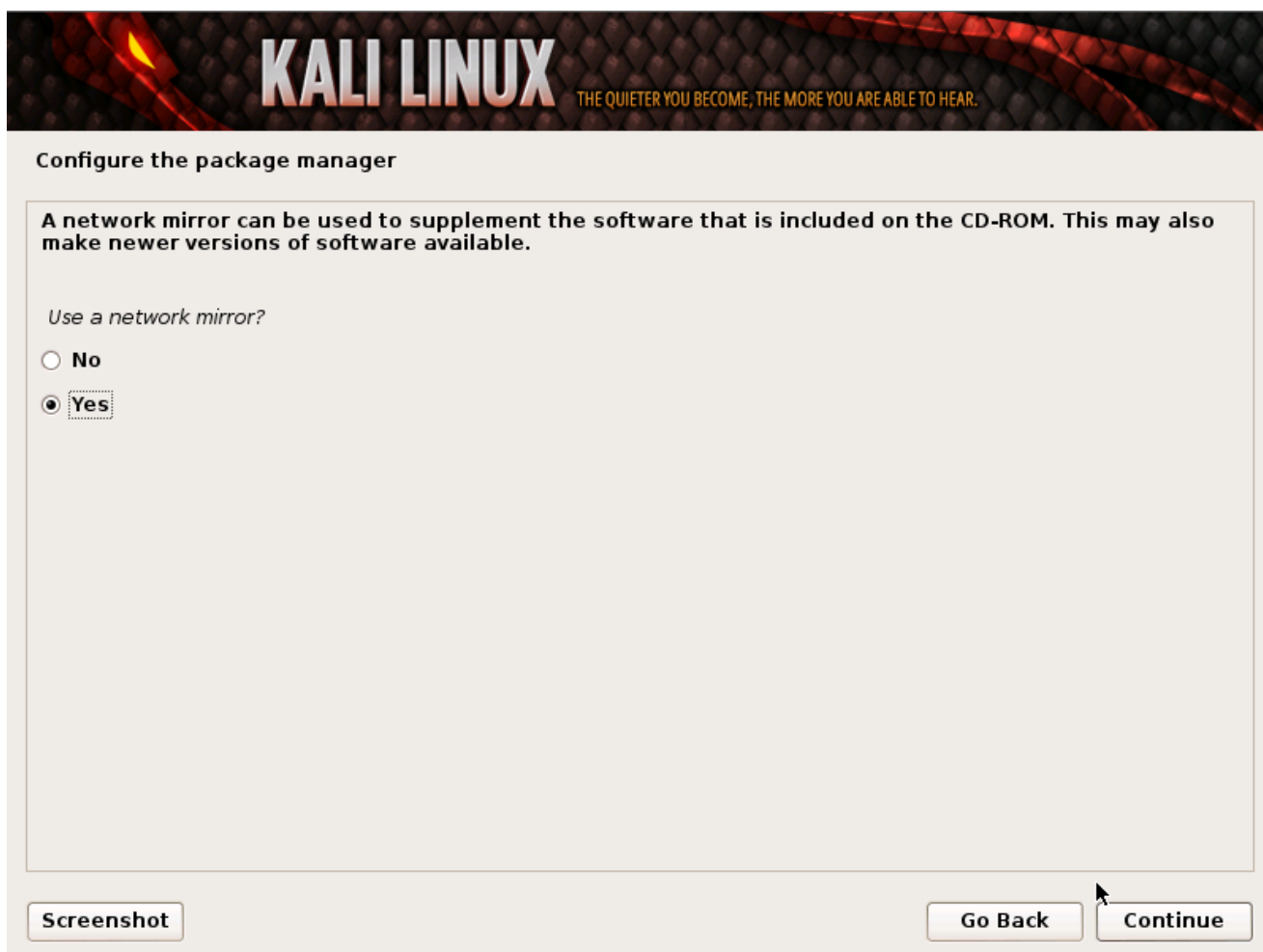
Encryption passphrase:

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

Re-enter passphrase to verify:

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。

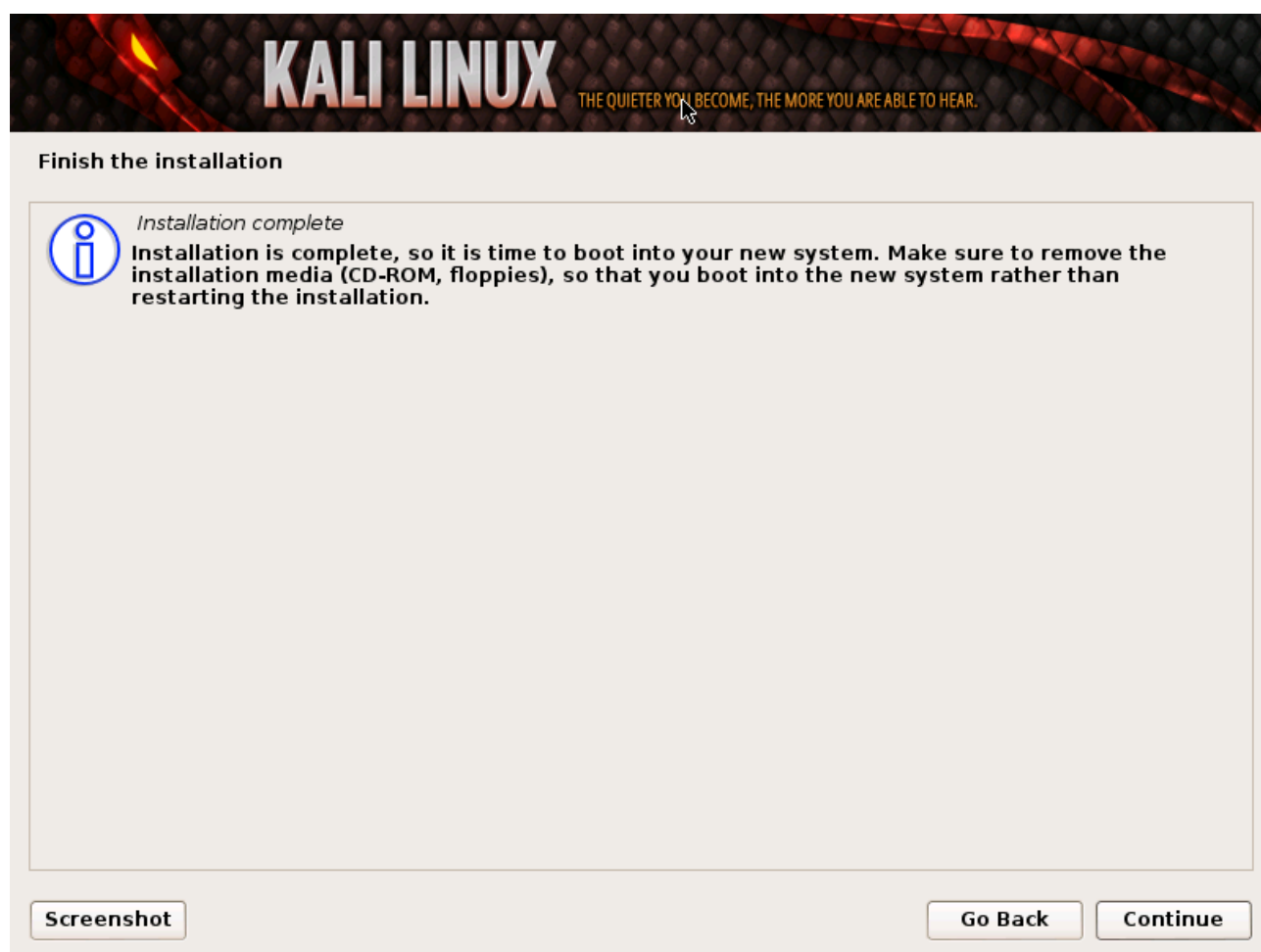
注意！ 如果你选择了 NO，你将不能从 Kali 源安装软件。



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。

三、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。

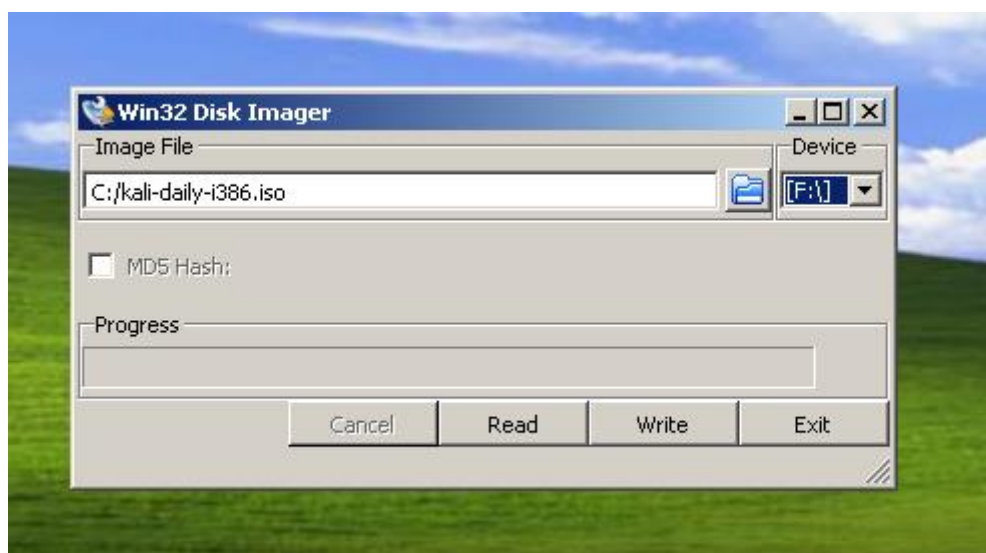
准备 USB 镜像

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。

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。

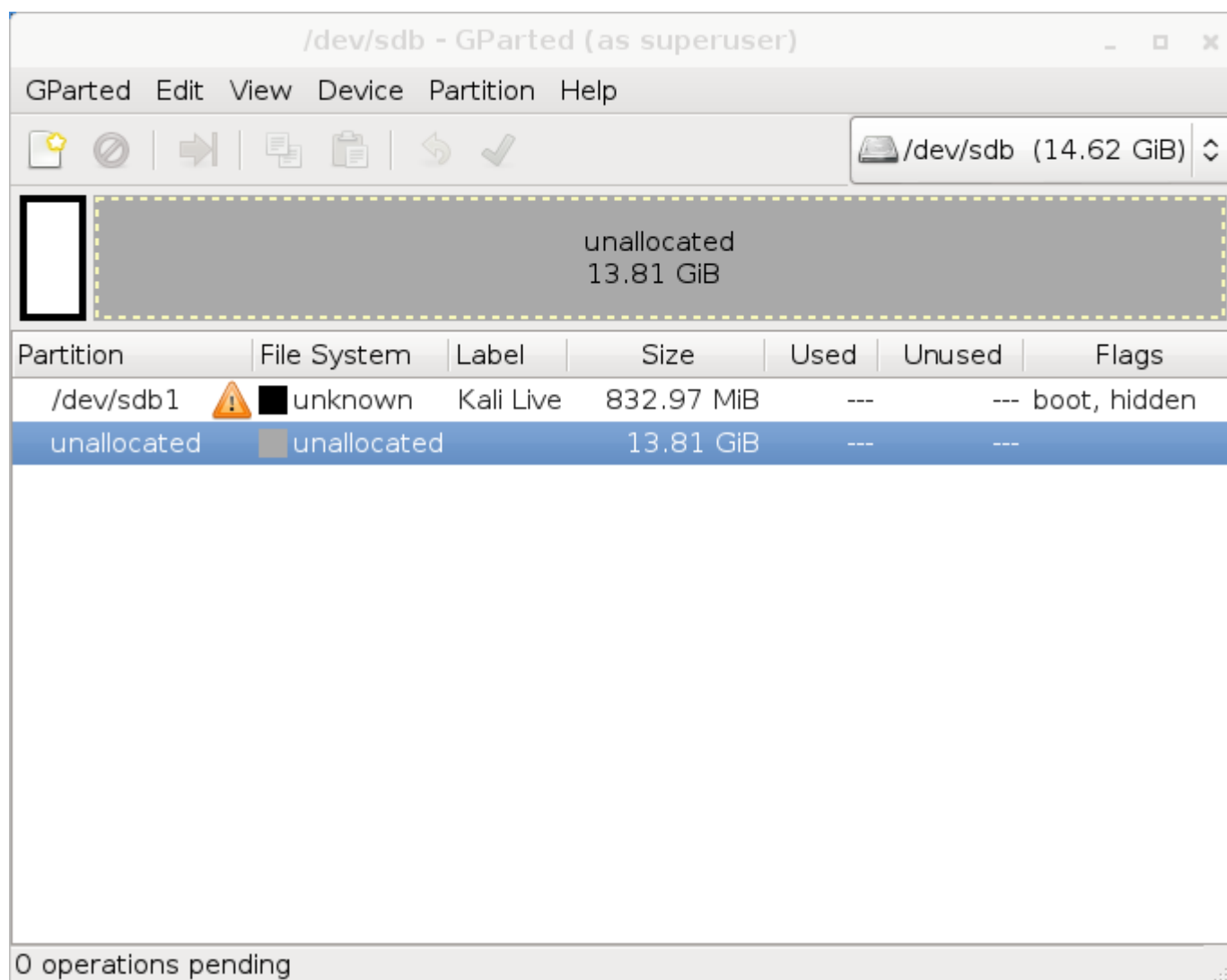
为你的 U 盘添加 Persistence 功能

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。

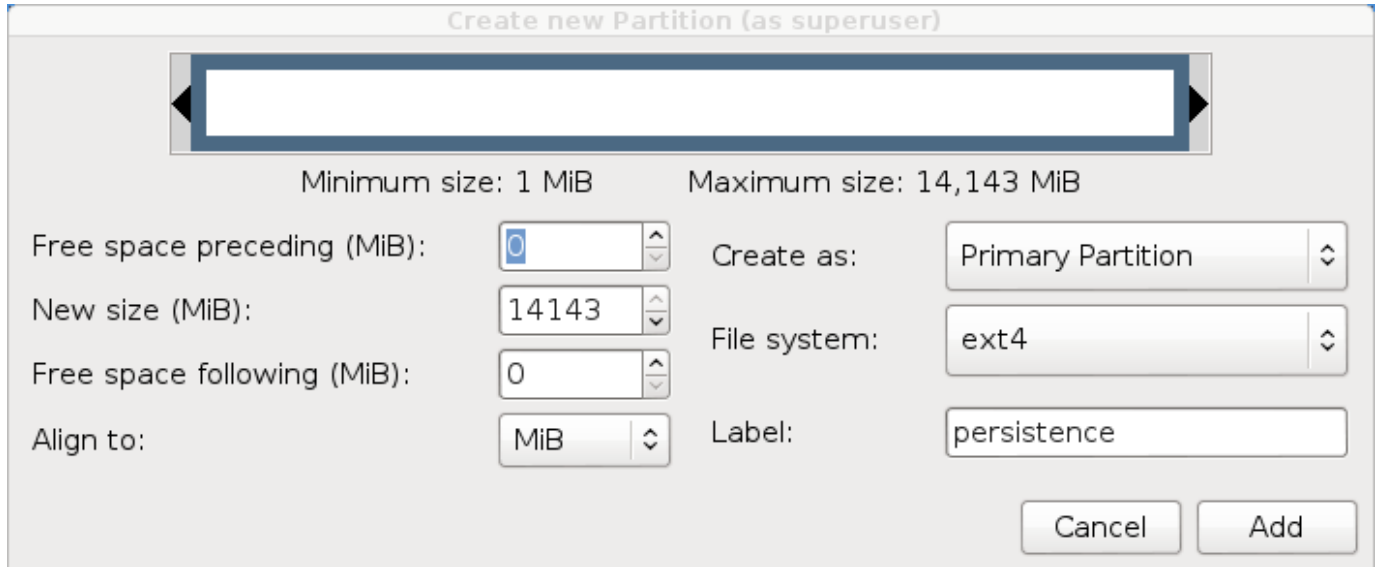
1. 镜像 Kali Linux ISO 到 U 盘和上面讲解的一样，用在 Linux 机器上的方法和 `dd`。
2. 在 U 盘创建并格式化额外的分区。在此例我们用 `gparted` by invoking:

```
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。

四、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：

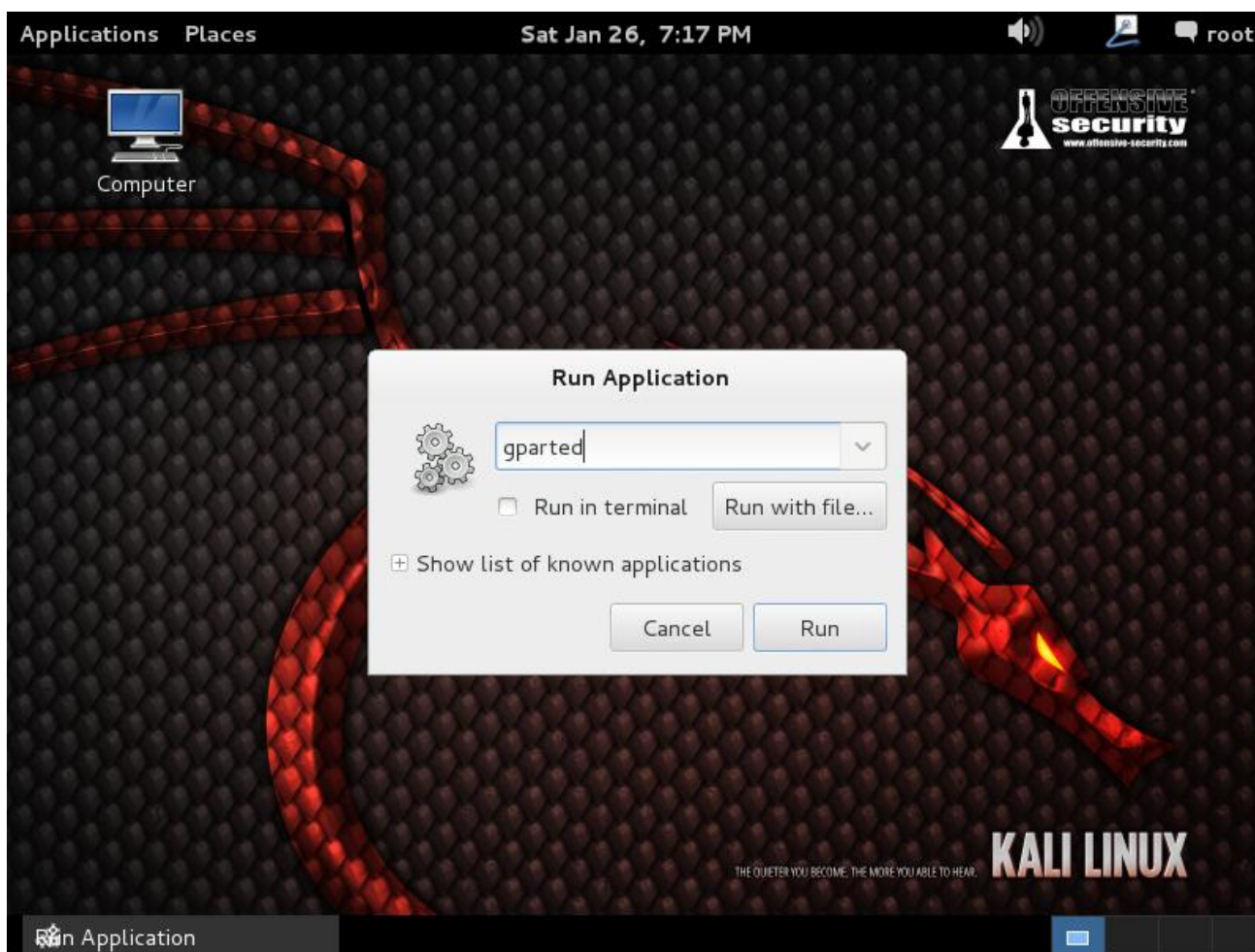
- Windows 至少有 8G 的剩余空间
- 支持 CD-DVD / USB 引导

准备安装

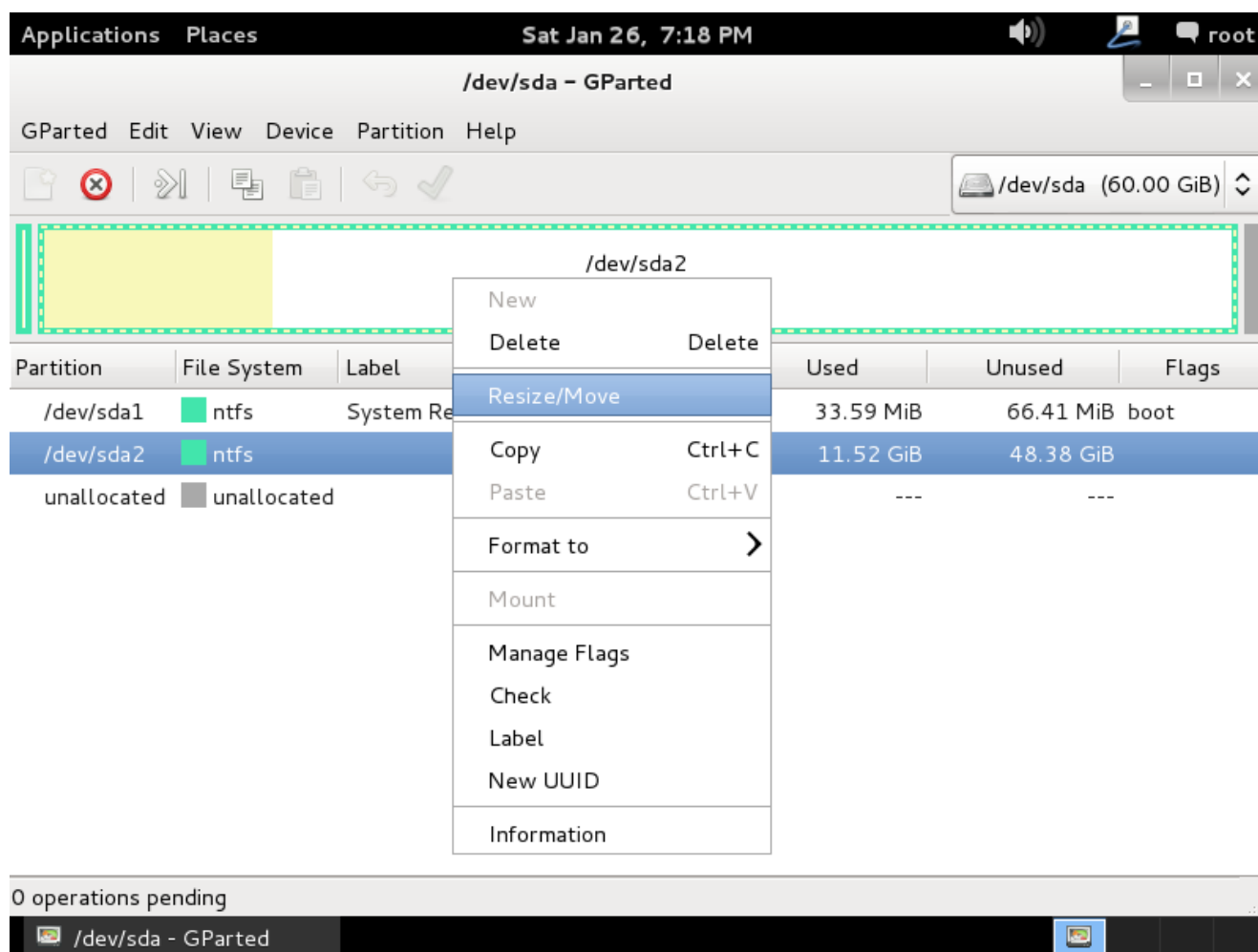
1. [下载 Kali Linux](#)。
2. 刻录 Kali Linux DVD 盘或[制作 Kali Linux Live U 盘](#)。
3. 确保你的电脑 BIOS 设置了从 CD/USB 引导。

双系统安装过程

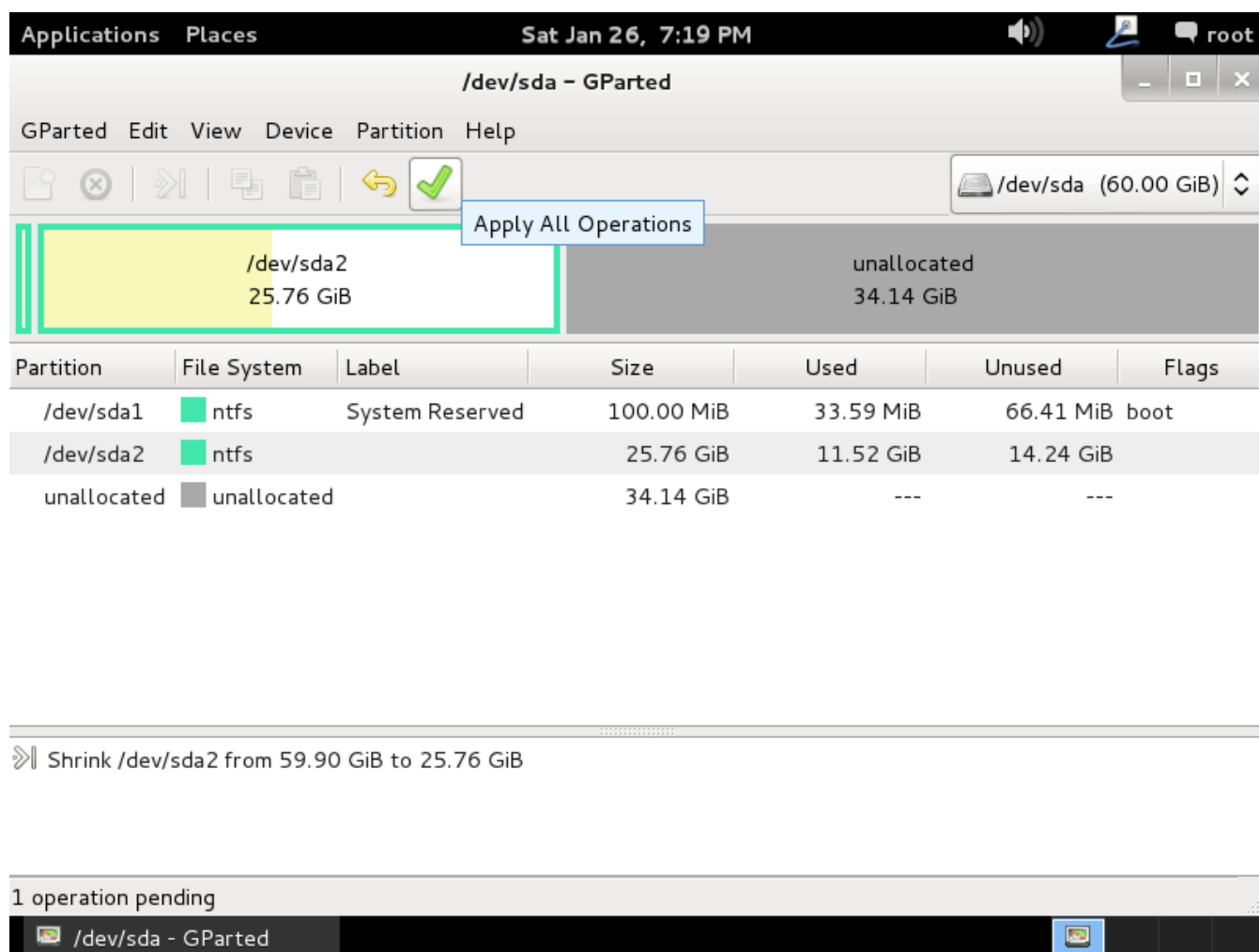
1. 开始安装，从你选择的安装媒介启动。你会看到 Kali 的引导界面。选择 *Live*，然后你会进入到 Kali Linux 桌面。
2. 使用用户名 **root**，和密码 **toor** 登录。下一步运行 **gparted** 程序。我们将用 **gparted** 缩小 windows 分区的大小以提供足够的空间安装 Kali。



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。

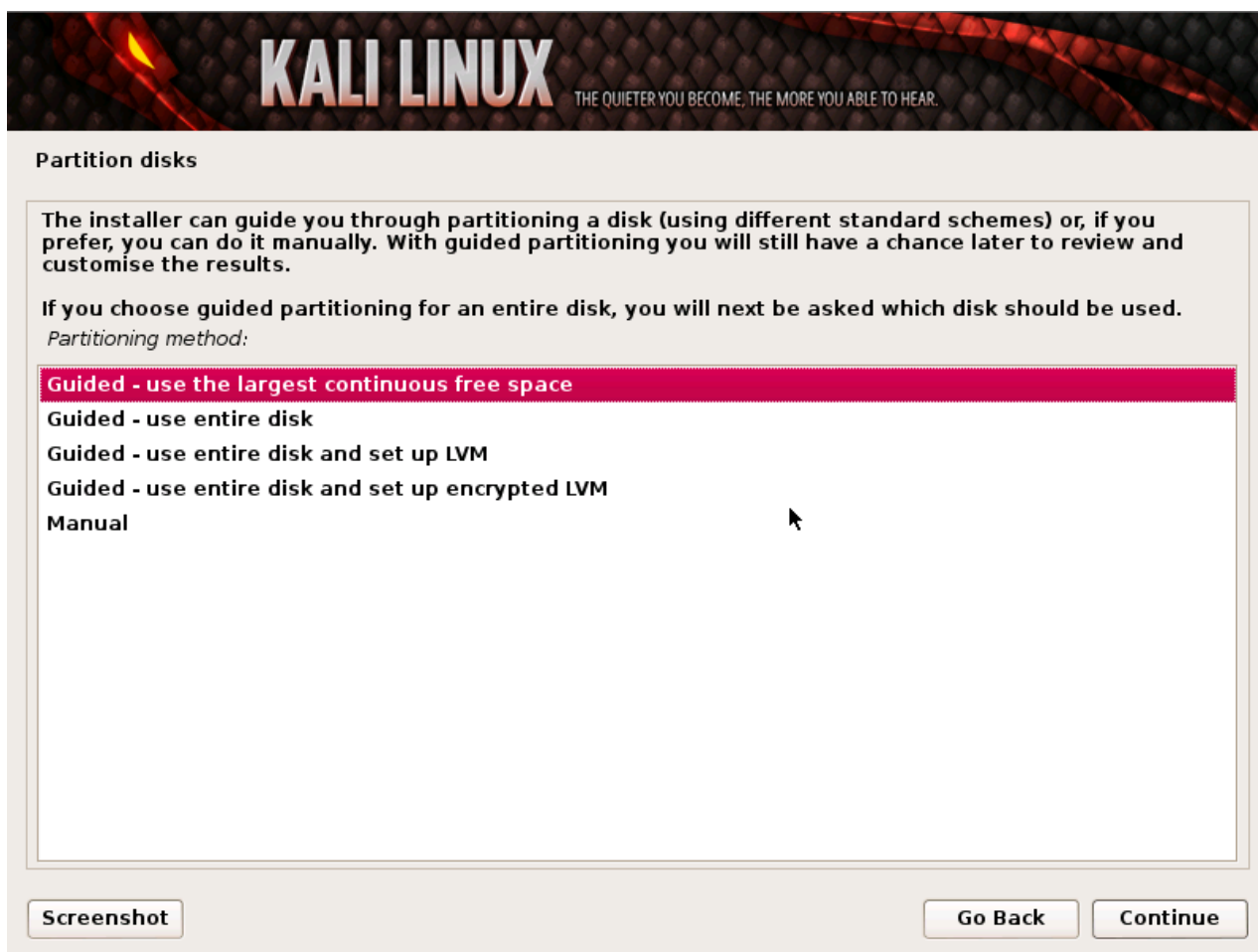


4. 重新分区之后。确保点击了硬盘的 Apply All Operations(应用所有操作)。退出 **gparted** 并重启。

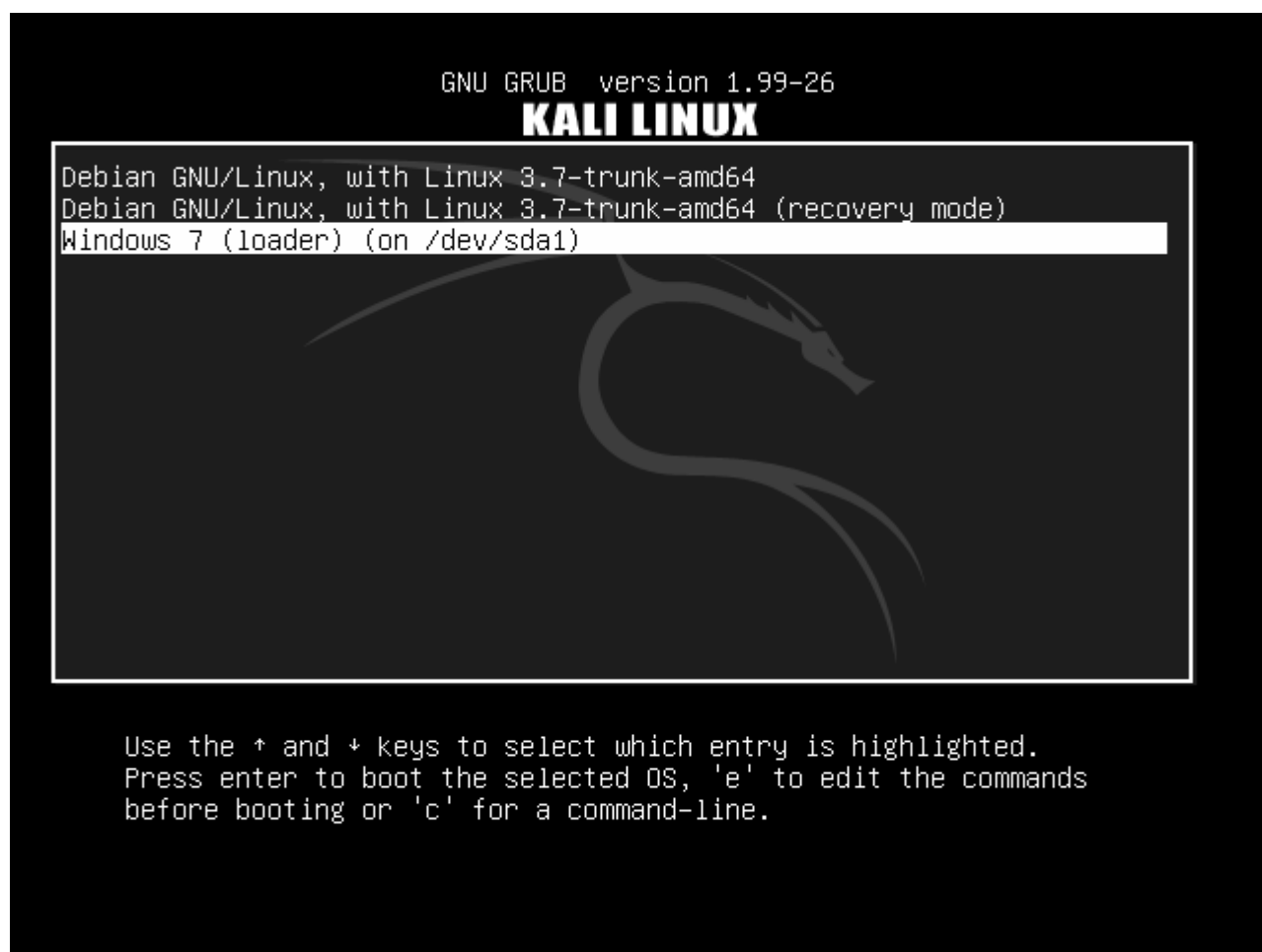


Kali Linux 安装步骤

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

五、Kali Mini ISO 网络安装

卡利迷你 ISO 可以很方便地从零开始安装一个最小的卡利系统, 迷你 ISO 安装文件会从我们的软件仓库下载所有需要的软件包, 这意味着你需要有一个快速的互联网连接, 就可以使用此安装方法。

安装先决条件

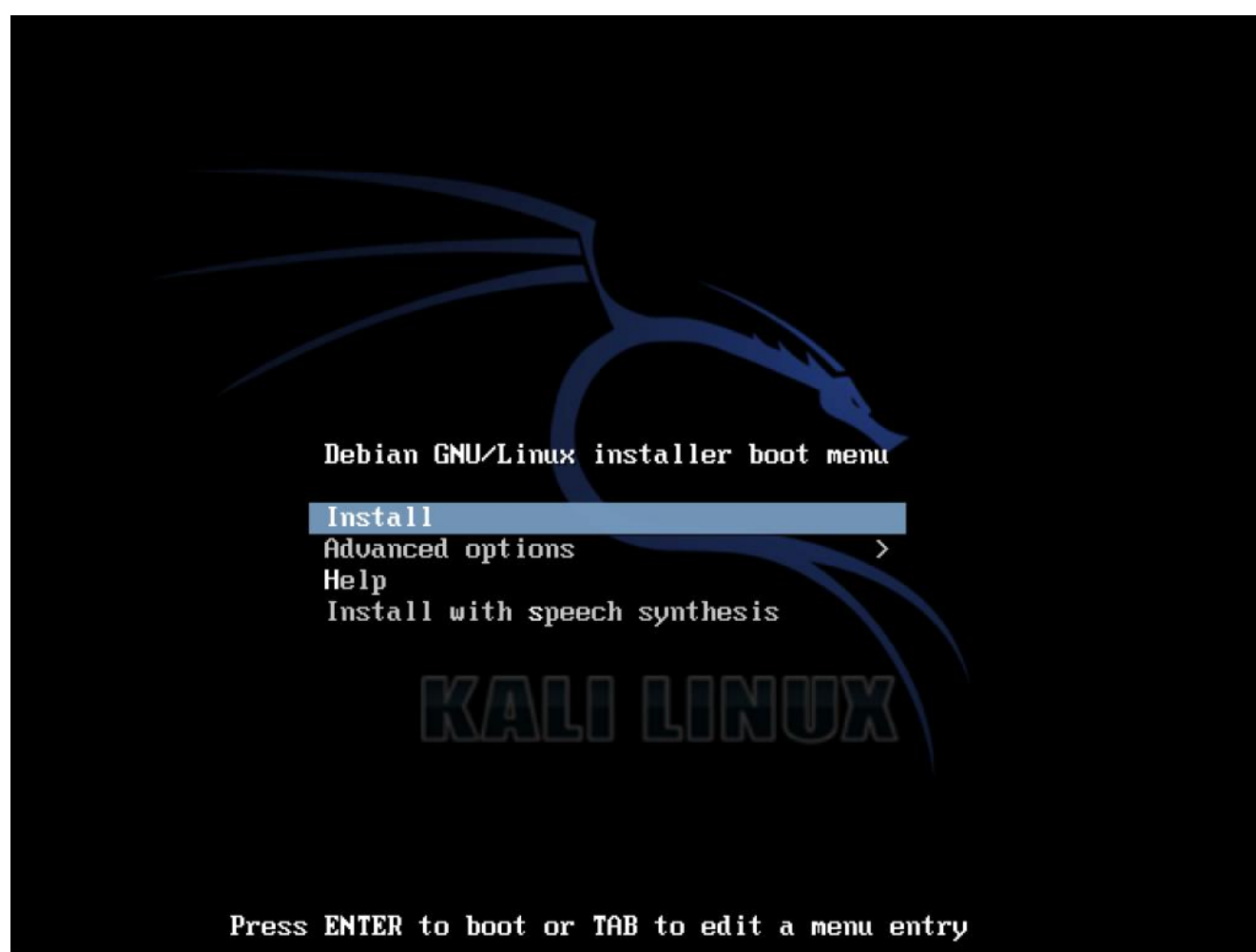
- 安装 Kali Linux 最少 8G 硬盘可用空间.
- i386 和 amd64 架构, 最低 512MB 内存.
- CD-DVD 光驱/支持 USB 引导

准备安装

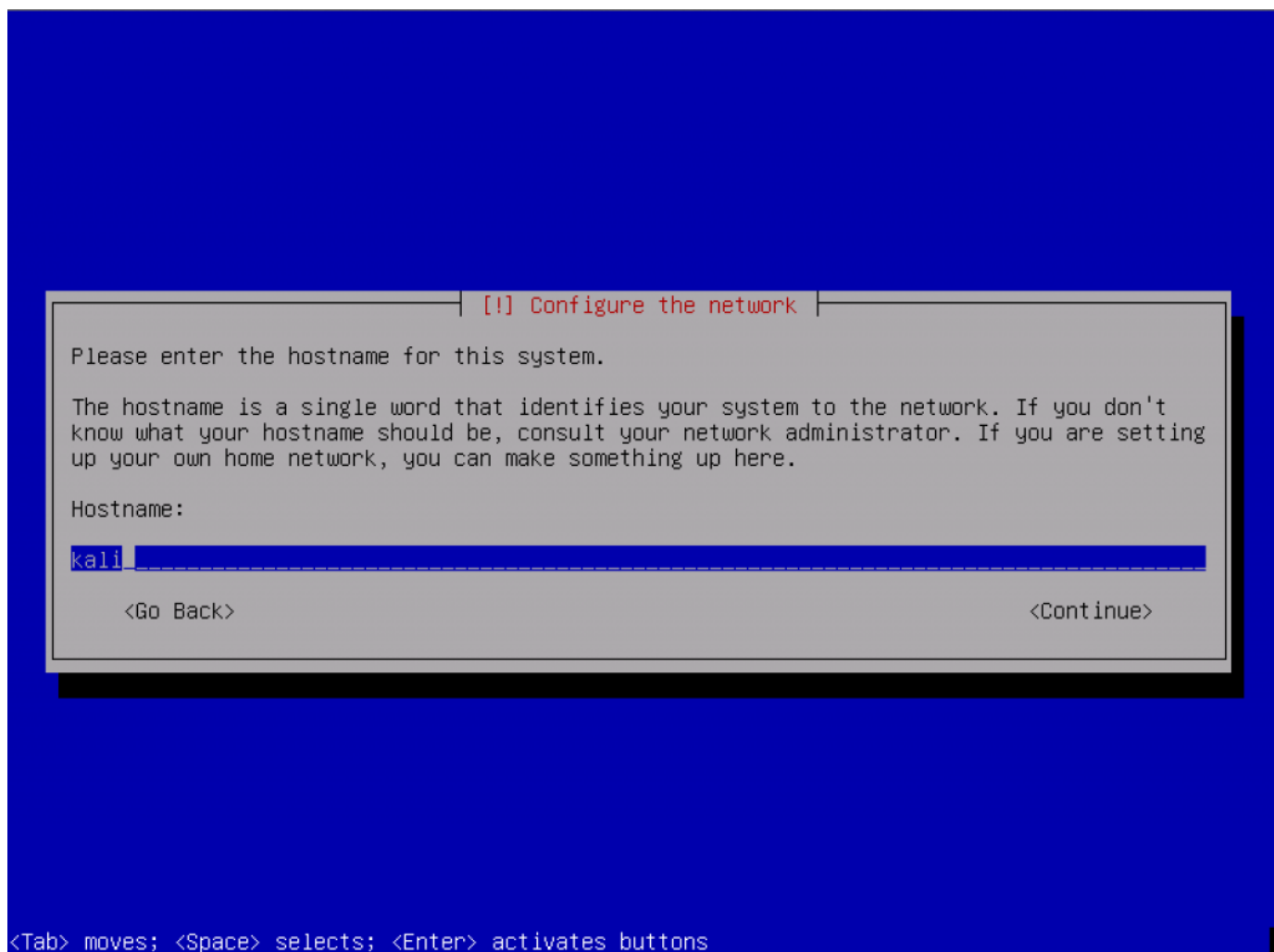
1. [下载 Kali mini ISO](#).
2. 把 Kali Linux 刻录到 DVD 盘或[制作 Kali Linux 镜像 U 盘](#).
3. 确认你电脑的 BIOS 设置了从 CD/USB 引导.

Kali Linux 安装步骤

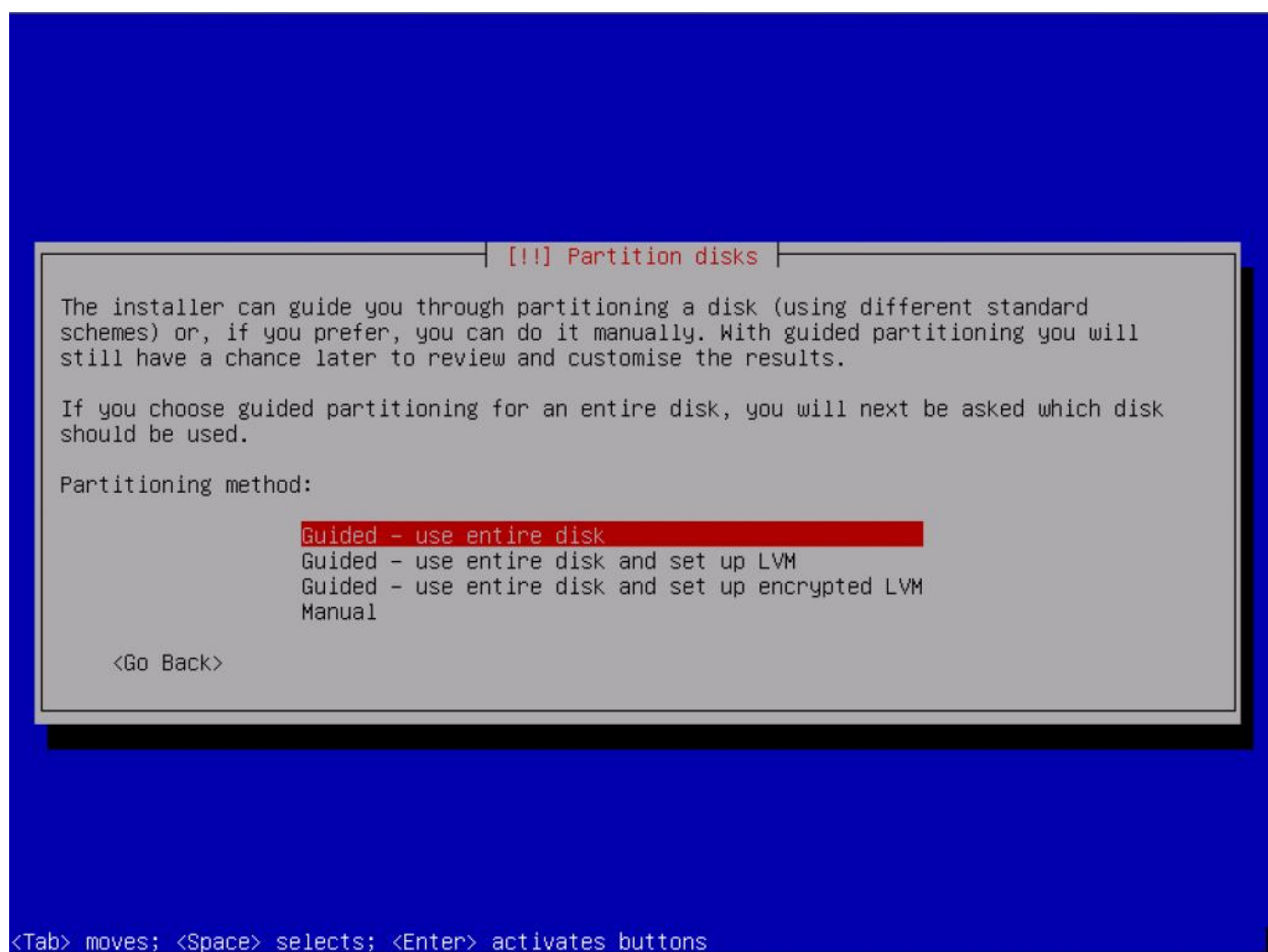
当你第一次启动迷你 ISO，你会用一个小的引导菜单，其中提供了各种选项。在这篇文章中，我们将简单地做一个基本的安装。



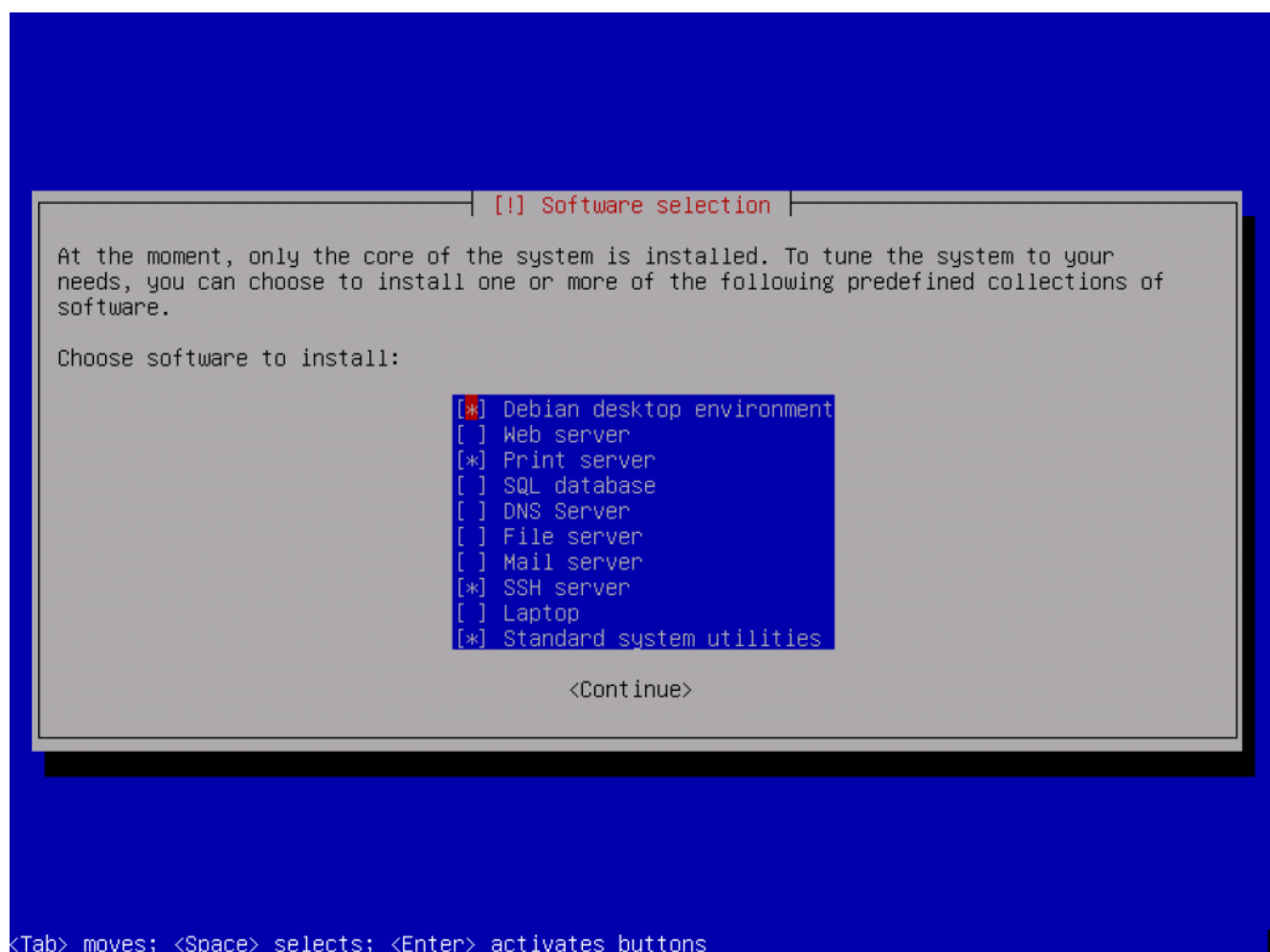
接下来，你会被提示输入不同的东西，如您的语言和键盘类型、主机名。



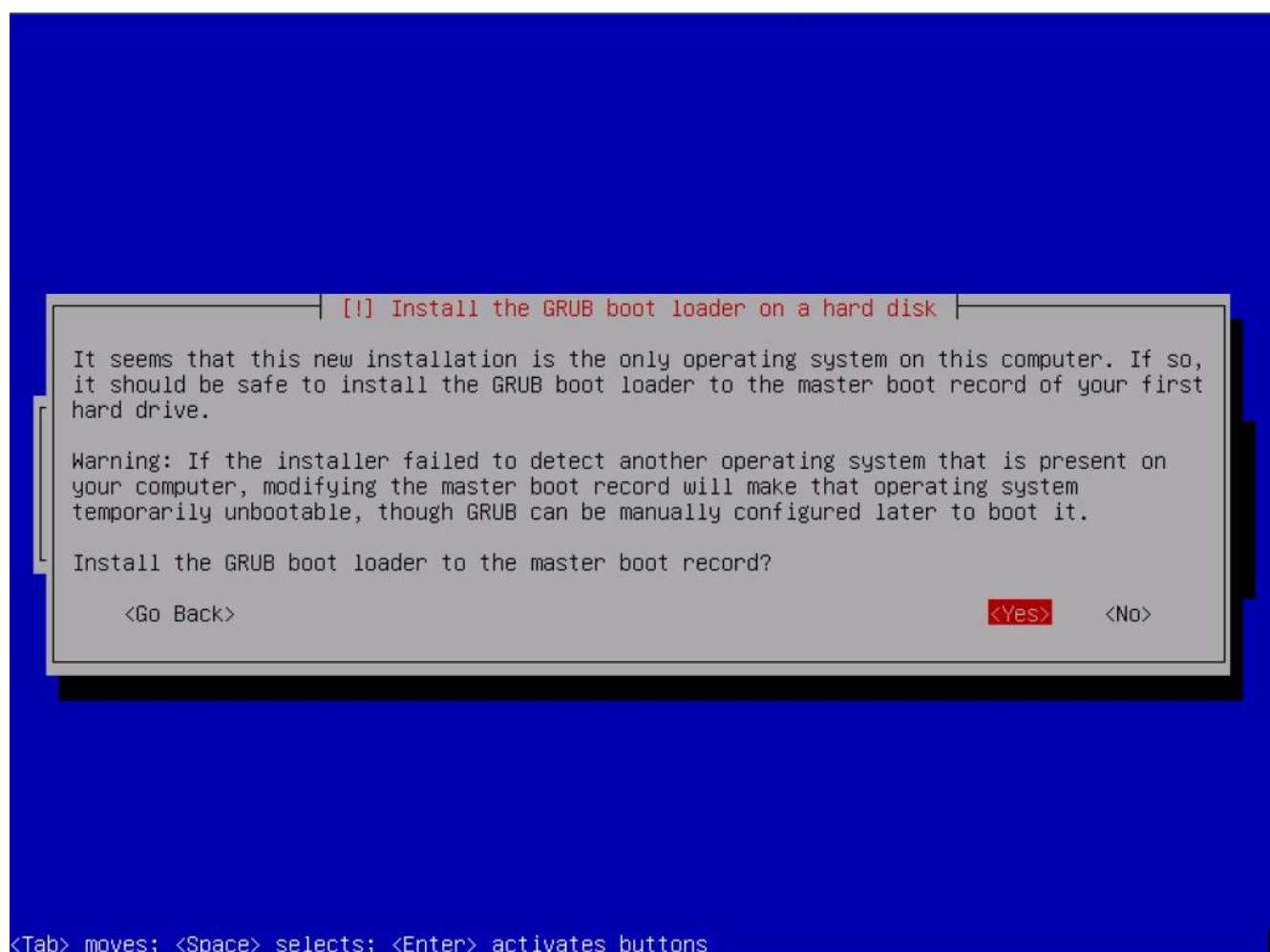
接下来选择时区, 然后会出现分区选项, 为了快速起见, 本文我们选 ‘Guided - use entire disk’ 这个选项, 一直按照提示做, 直到创建新的分区格局.



为了减少网络流量, 默认只选择了一小部分的软件包. 如果你要添加另外的服务或功能, 可以在这个界面做选择.



至此, 安装程序会在系统上下载并安装它所需的软件包. 这步花的时间与你的网速有关. 最后, 会提示你安装 GRUB 以完成整个安装过程.



安装完成

六、Kali Linux PXE 网络安装

配置 PXE 服务

在网络上引导和安装卡利（PXE）可用于安装一台没有光驱和 USB 端口的笔记本电脑，首先我们需要安装 dnsmasq 来提供 DHCP/ TFTP 服务器，然后编辑 dnsmasq.conf 文件。

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

在 *dnsmasq.conf* 中启用 DHCP、TFTP 和 PXE booting，如下，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/
service dnsmasq restart    重启让 dnsmasq 服务生效
```

下载 Kali PXE Netboot 镜像

现在，我们需要创建一个目录来保存卡利 Netboot 镜像

```
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
```

配置目标从网络启动

一切配置完毕之后，你现在就可以启动你的目标系统，将其配置为从网络启动，它应该从您的 PXE 服务器得到一个 IP 地址，并开始启动卡利。

七、PXE 预启动执行环境

预启动执行环境（Preboot eXecution Environment, PXE，也被称为预执行环境）是让计算机通过[网卡](#)独立地使用数据设备(如硬盘)或者安装操作系统。

PXE 当初是作为 [Intel](#) 的[有线管理](#)体系的一部分, [Intel](#) 和 [Systemsoft](#) 于 1999 年 9 月 20 日公布其规格(版本 2.1)^[1]。通过使用像[网际协议](#)(IP)、[用户数据报协议](#)(UDP)、[动态主机设定协定](#)(DHCP)、[小型文件传输协议](#)(TFTP)等几种[网络协议](#)和[全局唯一标识符](#)(GUID)、[通用网络驱动接口](#)(UNDI)、[通用唯一识别码](#)(UUID)的概念并通过对客户机(通过 PXE 自检的电脑)[固件](#)扩展预设的 [API](#) 来实现目的。

*PXE 客户机(client)*这个术语是指机器在 PXE 启动过程中的角色。一个 *PXE 客户机(client)*可以是一台服务器、桌面级电脑、笔记本电脑或者其他装有 PXE 启动代码的机器。

客户机的固件为接受到可用的 PXE 启动服务器, 要在网络中尝试找出 PXE 重定向服务(DHCP 代理)。在分析返回的包后, 固件会向合适的启动服务器询问[网络自检程序](#)(NBP)的路径, 并且通过 [TFTP](#) 协议下载到电脑的内存中, 有可能会去校验它, 最后执行它。当只有全部的 PXE 客户机(client)只使用一个 NBP 时, 全部的 PXE 客户机可能会被指定是用 [BOOTP](#) 协议, 从而不需要 DHCP 代理, 但是仍然需要 TFTP 启动服务。

PXE 被设计成适合各种计算机体系。2.1 版的描述中确定了 6 种系统规格, 包括 [IA-64](#) 和 [DEC Alpha](#)。可是只有 [IA-32](#) 的完全表述。Intel 在 IA-64 的 [扩展固件接口](#)中包括了 PXE, 落实了标准。

PXE 协议大致上结合了 DHCP 和 TFTP, 虽然都有在两者上面有改进。DHCP 用于查找合适的启动服务器, TFTP 用于下载初始引导程序和附加文件。

为了开始一个 PXE 自检会话, PXE 固件广播一个带有明确的 PXE 选项 DHCPDISCOVER 包(*扩展 DHCPDISCOVER*)到 67/UDP 端口(DHCP 服务器端口)。PXE 选项是 PXE 固件有 PXE 能力的鉴定, 但是会一般的 DHCP 服务忽略。当固件受到从这样的服务受到 DHCP OFFER 包时, 它会通过要求其提供配置信息来自我配置。

当 PXE 重定向服务 (DHCP 代理) 收到一个 *扩展 DHCPDISCOVER* 包时, 它会通过发送一个带有明确的 PXE 选项 DHCPDISCOVER 包到 PXE 客户机的 68/UDP 端口 (DHCP 客户机端口) 来回答。一个 *扩展 DHCPDISCOVER* 包主要包含:

- 一个 PXE 发现控制领域, 以决定是使用[多播](#), [广播\(网路\)](#)或[单播](#)来联系 PXE 启动服务器。
- 一个列出可用的 PXE 启动服务器类型的地址表。
- 一个代表每个一个 PXE 启动服务器类型的条目单。
- 一个带有提示用户按下哪一个键来看到启动菜单的 PXE 启动菜单/
- 一个超过多长时间就启动第一启动菜单的超时数值。

一个 DHCP 代理服务可能在相同的主机上运行一个标准的 DHCP 服务器。尽管两个服务不可以共享 67/UDP 端口, DHCP 代理服务在 4011/UDP 端口上运行, 要求从客户端来的 DHCPDISCOVER 包变成 DHCPREQUEST 包。标准 DHCP 服务在其发送的 DHCP OFFER 包中加入特殊的 PXE 选项组合, 这样 PXE 客户端知道可以在同一个主机的 4011/UDP 端口找到一个 DHCP 代理服务。

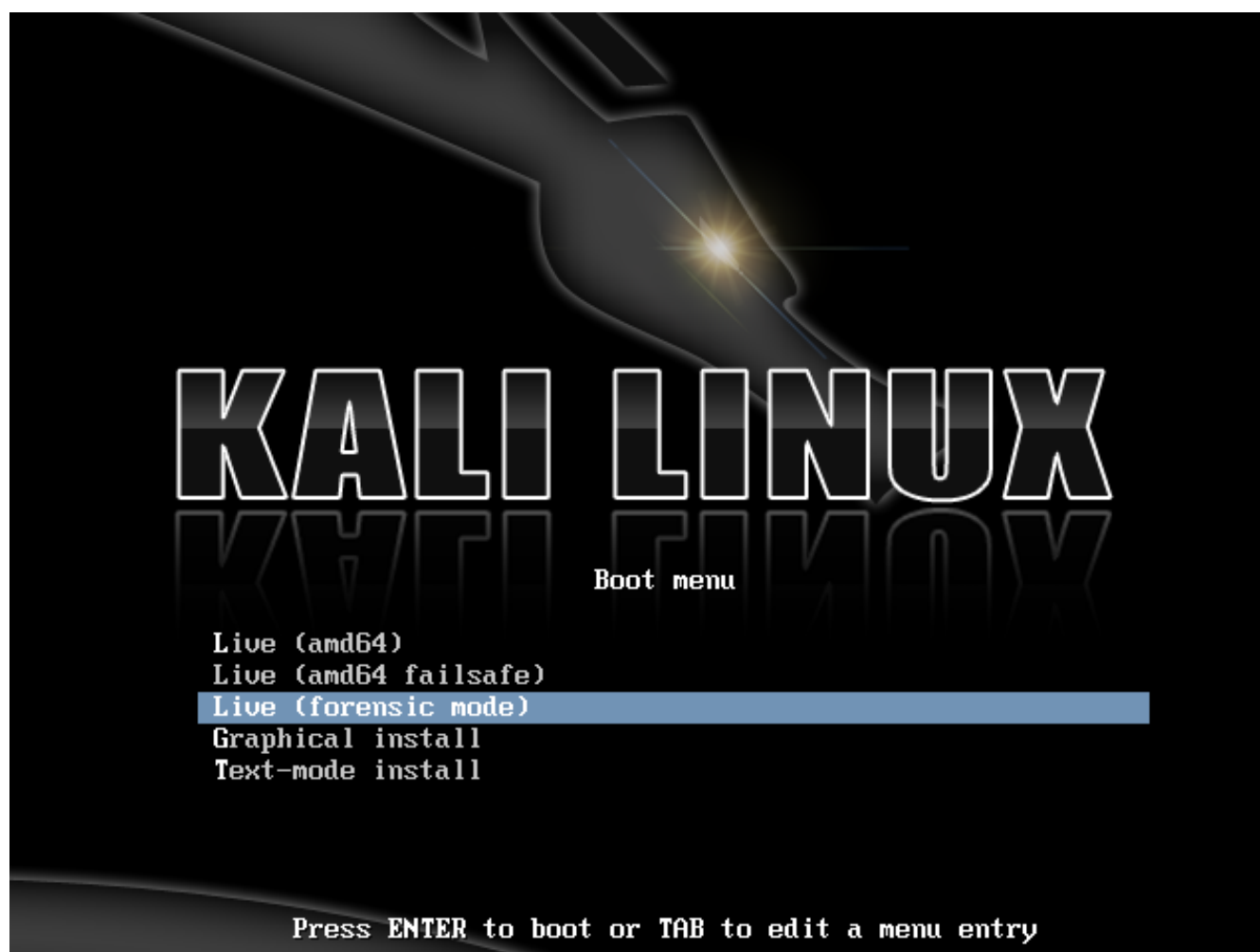
和一个正在启动系统的启动服务联系必须有一个 [IP 地址](#) (可能来自 DHCP 服务)。

通过[多播](#)或[单播](#)一个带有特殊的 PXE 选项的 *DHCPREQUEST* 包(扩展 *DHCPREQUEST*包)到 4011/UDP 端口, 或者[广播\(网路\)](#)这种包到 67/UDP 端口。这种包包含有 PXE 启动服务类型和 PXE 启动层, 一个守护进程允许运行多个启动服务类型。 一个扩展 *DHCPREQUEST*包可能是一个 *DHCPINFORM*包。

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-0.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、 封装最新的 Kali ISO

Kali Linux 允许你用 Debian 的 live-build 脚本封装最新的 Kali ISO. 封装镜像最简单的办法就是在 Kali Linux 环境下做如下操作。

你需要先安装 live-build 和 cdebootstrap 这两个包：

```
apt-get install git live-build cdebootstrap
```

下一步克隆 Kali cdimage 的 Git 源：

```
git clone git://git.kali.org/live-build-config.git
```

现在切换到 cdimage.kali.org 目录下的 live 目录里，然后封装 ISO。

```
cd live-build-config
```

```
lb clean --purge
lb config
lb build
```

live-build 脚本可以完整的定制 Kali Linux 镜像.更多关于 Kali live-build 脚本的信息,请看下一节。

五、 建立你自己的卡利 ISO

使用 Debian 最新版本的 live-build 脚本可以很方便的制作一个你自己的 ISO 文件。封装定制的 Kali ISO 很简单,很有趣,很有意义. 你可以用 Debian 的 live-build 脚本对 Kali ISO 进行全面的配置. 这些脚本以一系列配置文件的方式对镜像进行全面的自动定制, 让任何人都可以轻易地就能打造一个 Live 系统镜像. 官方发布的 Kali ISO 也采用了这些脚本.

最理想的是在预装 Kali 的环境里定制你的 Kali ISO. 如果不是这样, 请务必使用最新版本的 live-build 脚本 (3.x 分支的脚本可用于 Debian wheezy). 首先我们要用以下命令搭建好定制 Kali ISO 的环境:

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

封装 Kali ISO 的配置(可选)

config 目录里包含了定制 ISO 的各种重要的自定义选项, 这些选项在 Debian 的 [live build 3.x](#) 页面有文档说明. 然而如果你没有耐心, 请特别注意以下的配置文件:

config/package-lists/kali.list.chroot - 包含要安装在 Kali ISO 里的软件包的列表. 你可以指定移除已经安装的软件包. 也可以切换你的 Kali ISO 的桌面环境 (KDE, Gnome, XFCE, LXDE 等).

hooks/ - hooks 目录允许我们在不同阶段调用脚本封装定制 Kali Live ISO. 更多关于 hooks 的信息, 参考 [live build 手册](#). 举个例子, Kali 是这样添加取证模式的引导菜单的:

```
$ 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
```

在封装 ISO 之前, 可以指定需要的架构, 选择 amd64 或者 i386. 还要注意” lb build” 需要 root 权限. 如果你不指定架构, live build 将根据你现在使用的架构来封装 ISO.

如果你想在 32 位系统封装 64 位的 ISO, 务必打开多架构支持:

```
dpkg --add-architecture amd64
apt-get update
```

配置 live-build 封装 64 位或者 32 位 ISO:

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

```
lb build
```

最后一个命令需要一些时间, 因为它下载所有需要的软件包然后封装 ISO. 如果你打算经常定制 ISO, 你可以把 kali 的软件包缓存在本地便于今后的封装. 最简单的就是安装 **apt-cacher-ng**, 然后在每次打包时配置 `http_proxy` 环境变量.

```
apt-get install apt-cacher-ng
/etc/init.d/apt-cacher-ng start
export http_proxy=http://localhost:3142/
.... # setup and configure your live build
lb build
```

六、更改卡利桌面环境

不是所有的 Kali Linux 用户都希望使用 Gnome 作为默认的桌面环境,所以我们简化了更换桌面管理器所需的工作.要封装一个定制过桌面环境的专属 Kali ISO 镜像,从[封装定制的 Kali Live ISO](#)这篇文档开始吧.在封装你的 ISO 之前,先编辑 **config/package-lists/kali.list.chroot** 的最后部分,加入你选择的桌面环境的相关信息到这些注释的后面:

```
# 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
```

七、 解决无线驱动程序问题

如果你不确定你在找什么,那么 Linux 的无线驱动问题的疑难排解将会是个挫折.本文将以一般指引的方式来帮助你更好的找到解决无线问题所需要的信息.

1. 没有网卡

- 愚蠢的问题:它是无线网卡吗?(我们见过很多次了)
- 无线网卡插好了吗?
- **lsusb** 或者 **lspci** 能看到它吗(手机除外)?可能需要更新 pci ids 和 usb ids
- **dmesg** 里有关于加载驱动或加载失败的信息吗
- 是 Kali 的虚拟机吗?如果是,除非你的是 USB 网卡,否则不可用 (VMWare/VirtualBox/QEMU 会虚拟每个 PCI 硬件).USB 网卡连到虚拟机了吗?
- 如果 **dmesg** 里没有信息并且不是虚拟机,那么你可能需要试试最新的 *Compat-wireless*(有时需要固件)->检查 linux 无线驱动

2. 有网卡但不能做任何事

- 看错误信息
- 如果没有错误信息,就执行 **dmesg|tail**,可能会告诉你怎么回事
- 可能缺少固件
- 检查 **rkill** 和硬件开关还有 BIOS 选项

3. 没有监听模式

- STA 驱动(Ralink, Broadcom)还有其他厂商生产提供的驱动都不支持监听模式
- **ndiswrapper** 不支持监听模式.永远不会.
- **Airodump-ng**/**Wireshark** 不显示任何信息:检查 **rkill** 和硬件开关还有 BIOS 选项

4. 注入

- 用 **aireplay-ng -9** 测试(用 **airmon-ng** 确定网卡处于监听模式)
- **Airmon-ng** 不显示芯片信息:这不是大问题,只是不能获取网卡的信息,不会影响网卡的功能.
- 处于监听模式但不能注入:检查 **rkill** 和硬件开关还有 BIOS 选项
- 网络管理器有时和 **Aircrack** 工具包有冲突.运行 **airmon-ng check kill** 来杀掉这些进程.

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的 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 Galaxy Note 10.1 安装 Kali ARM



The Samsung Galaxy Note 10.1 is a 10.1-inch tablet computer designed, developed, and marketed by Samsung. The tablet incorporates a 1.4 GHz quad-core Exynos processor and 2 GB of RAM. The touch screen works surprisingly well with Kali as well as the wireless card, however Bluetooth and audio are not yet functional on this image.

If all you want to do is to install Kali on your Galaxy Note 10.1, follow these instructions:

1. You' ll need **at least 7 GB free** on your internal SD card for our image.
2. Root your Samsung Galaxy Note 10.1 if you have not already done so.
3. Download the **Kali Linux Galaxy Note 10.1** image from our [downloads](#) area.
4. Rename the downloaded Kali image to **linux.img** and copy it to the root directory of your internal SD card.
5. Download a recovery.img file from [OpenSGN](#) and copy it to the root directory of your internal SD card.
6. Get root on your Galaxy Note 10.1, change to the root directory of the internal SD storage, and backup your recovery partition:

```
dd if=/dev/block/mmcblk0p6 of=recovery.img_orig
```

7. **dd** the downloaded recovery.img image to the recovery partition:

Alert! This process will overwrite your recovery partition. Please make sure you know what you are doing. You may brick your device if you fumble this.

```
dd if=recovery.img of=/dev/block/mmcblk0p6
```

8. Reboot your Galaxy Note 10.1 into recovery mode. You can do this by **turning it off**, then press and hold both the **power button** and the **volume up** button. Once you see the “Samsung Galaxy Note 10.1” text appear, **release the power button but keep pressing the volume up button**. This should boot you into Kali and auto-login into Gnome.
9. Open the onscreen keyboard by going to : **Applications -> Universal Access -> Florence Virtual Keyboard**.
10. Wireless works but seems to skip the scanning of networks without some massaging. **If the Gnome Network Manager shows no wireless networks**, simply add your wireless network as a “hidden” one and you should get connected as usual.
11. You can modify, debug, and explore our image easily from within your Galaxy Note, using a wonderful Android App called [Linux Deploy](#).

三、 在 ODROID 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](#)。

四、 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:  priority=10 tries=5 successful=1
      40960     32768    2 Label:  "KERN-B"
                        Type:  ChromeOS kernel
                        UUID:  37CE46C9-0A7A-4994-80FC-9C0FFCB4FDC1
                        Attr:  priority=5 tries=5 successful=1
      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](#)。

五、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。

六、在 MK/SS808 上安装 Kali ARM



SS808 ARM Devices (rk3306)

SainSmart SS808 是一种基于 **rockchip** 芯片的 ARM 设备. 它搭载了一个双核 1.6GHz 的 A9 处理, 还有 1G 内存, 能很好的运行 Kali.

如果你想安装 Kali 到你的 SS808, 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 SS808 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, 使用的是 SS808 镜像. **如果有变, 自行更改.**
4. 把 [MK808-Finless-1-6-Custom-ROM](#) 下载到 Windows 系统的电脑并解压这个 zip 文件.

5. 阅读 MK808 Finless ROM 工具的 README, 然后安装需要的 Windows 驱动.
6. 运行 Finless ROM 刷机工具, 确认下面有提示 “Found RKAndroid Loader Rock USB”. 然后在列表中取消 kernel.img 和 recovery.img 选项, 然后开始刷机.
7. 然后下一步用 kail 的 kernel.img 和 recovery.img 覆盖 Finless ROM 目录下的 kernel.img 和 recovery.img.
8. 在 Finless ROM 工具里, 确认只选了 “kernel.img” 和 “recovery.img”, 然后再刷一次.
9. 把 microSD 卡插入到 SS808 然后启动.

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-SS808.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, 插入 SD 卡到 SS808 再启动. 你将可以用 (root/toor) 登录, 然后用 **startx** 启动图形界面. 就这样, 完成了!

05. Kali Linux 开发

一、定制 Raspberry Pi 镜像

本文针对开发者描述何如创建一个定制的 Raspberry Pi ARM 版 Kali Linux 镜像的方法. 如果你只是想安装 Kali 镜像, 请查阅我们的文章 [“安装 Kali Linux ARM 版到 Raspberry Pi”](#).

01. 创建 Kali rootfs

创建一个 armel 架构的如 Kali 文档中所述的 [Kali rootfs](#). 最后生成的 rootfs 将位于 `~/arm-stuff/rootfs/kali-armel` 目录.

02. 创建镜像文件

然后, 我们创建用于存放我们 Raspberry Pi rootfs 和 boot 镜像的物理镜像文件.

```
apt-get install kpartx xz-utils sharutils
cd ~
mkdir -p arm-stuff
cd arm-stuff/
mkdir -p images
cd images
dd if=/dev/zero of=kali-custom-rpi.img bs=1MB count=5000
```

03. 分区并挂载镜像文件

```
parted kali-custom-rpi.img --script -- mklabel msdos
parted kali-custom-rpi.img --script -- mkpart primary fat32 0 64
parted kali-custom-rpi.img --script -- mkpart primary ext4 64 -1
loopdevice=`losetup -f --show kali-custom-rpi.img`
device=`kpartx -va $loopdevice| sed -E 's/.*(loop[0-9])p.*/1/g' | head -1`
device="/dev/mapper/${device}"
bootp=${device}p1
rootp=${device}p2

mkfs.vfat $bootp
mkfs.ext4 $rootp
mkdir -p root
mkdir -p boot
mount $rootp root
mount $bootp boot
```

04. 复制和修改 Kali rootfs

```
rsync -HPavz /root/arm-stuff/rootfs/kali-armel/ root
echo nameserver 8.8.8.8 > root/etc/resolv.conf
```

05. 编译 Raspberry Pi 内核和模块

如果你不是以 ARM 硬件作为开发环境, 需要搭建 [ARM 交叉编译环境](#) 来编译 ARM 内核和模块. 完成后, 执行如下命令.

```
cd ~/arm-stuff
mkdir -p kernel
cd kernel
git clone https://github.com/raspberrypi/tools.git
git clone https://github.com/raspberrypi/linux.git raspberrypi
cd raspberrypi
```



```
export ARCH=arm
export CROSS_COMPILE=~/.arm-stuff/kernel/toolchains/arm-eabi-linaro-4.6.2/bin/arm-eabi-
make bcmrpi_cutdown_defconfig
# configure your kernel !
make menuconfig
make -j$(cat /proc/cpuinfo|grep processor|wc -l)
make modules_install INSTALL_MOD_PATH=~/.arm-stuff/images/root
cd ../tools/mkimage/
python imagetool-uncompressed.py ../../raspberrypi/arch/arm/boot/Image
cd ~/.arm-stuff/images
git clone git://github.com/raspberrypi/firmware.git rpi-firmware
cp -rf rpi-firmware/boot/* boot/
rm -rf rpi-firmware

cp ~/.arm-stuff/kernel/tools/mkimage/kernel.img boot/
echo "dwc_otg.lpm_enable=0 console=ttyAMA0,115200 kgdboc=ttyAMA0,115200 console=tty1
root=/dev/mmcblk0p2 rootfstype=ext4 rootwait" > boot/cmdline.txt
umount $rootp
umount $bootp
kpartx -dv $loopdevice
losetup -d $loopdevice
```

使用 **dd** 工具克隆这个文件到你的 SD 卡. 在本例中, 我们假设存储设备在 `/dev/sdb`. 请按需修改.

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

dd 操作完成后, 卸载并弹出 SD 卡. 然后启动进入到 Kali Linux

二、定制 Chromebook 镜像

针对开发者, 如下的文档描述我们创建个性化的 **Kali Linux Samsung chromebook ARM 镜像** 的方法. 如果你想安装预发的 Kali image, 查阅我们的文档 [在三星 Chromebook 安装 Kali](#).

本文档中, 我们创建一个镜像(包含两种引导分区) – 一种分区包含了强制从 SD 卡引导的内核, 另一种包含了强制从 USB 引导的内核. 根据你的 USB 存储媒介的类型, 确保你在用 **dd** 把镜像克隆到 USB 设备后(本指南最后的命令), 用更高的优先级标志相关的引导分区.

01. 创建 Kali rootfs

开始创建我们文档中描述的 [Kali rootfs](#) 使用 armhf 架构. 到文档的最后, 在 `~/arm-stuff/rootfs/kali-armhf` 目录里应该有一个里面包含很多文件的 rootfs 目录.

02. 创建镜像文件

下一步, 我们创建用于存放我们 Chromebook rootfs 和引导镜像的物理镜像文件.

```
apt-get install kpartx xz-utils gdisk uboot-mkimage u-boot-tools vboot-kernel-utils vboot-utils
cgpt
cd ~
mkdir -p arm-stuff
cd arm-stuff/
mkdir -p images
cd images
dd if=/dev/zero of=kali-custom-chrome.img bs=1MB count=5000
```

03. 分区和挂载镜像文件

```
parted kali-custom-chrome.img --script -- mklabel msdos
parted kali-custom-chrome.img --script -- mktable gpt
gdisk kali-custom-chrome.img << EOF
x
l
8192
m
n
1

+16M
7f00
n
2

+16M
7f00
n
3
```

```
w
y
EOF
loopdevice=`losetup -f --show kali-custom-chrome.img`
device=`kpartx -va $loopdevice| sed -E 's/.*(loop[0-9])p.*/1/g' | head -1`
device="/dev/mapper/${device}"
bootp1=${device}p1
bootp2=${device}p2
rootp=${device}p3

mkfs.ext4 $rootp
mkdir -p root
mount $rootp root
```

04. 复制和修改 Kali rootfs

用 **rsync** 递归复制先前挂载的 Kali rootfs 镜像.

```
cd ~/arm-stuff/images/
rsync -HPavz ~/arm-stuff/rootfs/kali-armhf/ root

echo nameserver 8.8.8.8 > root/etc/resolv.conf

mkdir -p root/etc/X11/xorg.conf.d/
cat << EOF > root/etc/X11/xorg.conf.d/50-touchpad.conf
Section "InputClass"
    Identifier "touchpad"
    MatchIsTouchpad "on"
    Option "FingerHigh" "5"
    Option "FingerLow" "5"
EndSection
EOF
```

05. 编译三星 Chromium 内核和模块

如果你不是使用 ARM 硬件作为开发环境, 为了编译 ARM 内核和模块你应该先建立 [ARM 交叉编译环境](#). 完成后, 用如下命令继续.

获取 Chromium 内核源代码并放到我们的开发树结构中:

```
cd ~/arm-stuff
```

```

mkdir -p kernel
cd kernel
git clone http://git.chromium.org/chromiumos/third_party/kernel.git -b chromeos-3.4 chromeos
cd chromeos
cat << EOF > kernel.its
/dts-v1/;

/ {
    description = "Chrome OS kernel image with one or more FDT blobs";
    #address-cells = <1>;
    images {
        kernel@1 {
            description = "kernel";
            data = /incbin(("arch/arm/boot/zImage"));
            type = "kernel_noload";
            arch = "arm";
            os = "linux";
            compression = "none";
            load = <0>;
            entry = <0>;
        };
        fdt@1 {
            description = "exynos5250-snow.dtb";
            data = /incbin(("arch/arm/boot/exynos5250-snow.dtb"));
            type = "flat_dt";
            arch = "arm";
            compression = "none";
            hash@1 {
                algo = "sha1";
            };
        };
    };
    configurations {
        default = "conf@1";
        conf@1 {
            kernel = "kernel@1";
            fdt = "fdt@1";
        };
    };
};
EOF

```

为内核打补丁, 我们以打无线注入补丁为例.

```
mkdir -p ../patches
```

```
wget http://patches.aircrack-ng.org/mac80211.compat08082009.wl_frag+ack_v1.patch
-O ../patches/mac80211.patch
wget http://patches.aircrack-ng.org/channel-negative-one-maxim.patch
-O ../patches/negative.patch
patch -p1 < ../patches/negative.patch
patch -p1 < ../patches/mac80211.patch
```

配置, 然后像下面一样交叉编译 Chromium 内核.

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

./chromeos/scripts/prepareconfig chromeos-exynos5
# Disable LSM
sed -i 's/CONFIG_SECURITY_CHROMIUMOS=y/# CONFIG_SECURITY_CHROMIUMOS is
not set/g' .config
# If cross compiling, do this once:
sed -i 's/if defined(__linux__)/if defined(__linux__) ||defined(__KERNEL__) /g'
include/drm/drm.h

make menuconfig
make -j$(cat /proc/cpuinfo|grep processor|wc -l)
make dtbs
cp ./scripts/dtc/dtc /usr/bin/
mkimage -f kernel.its kernel.itb
make modules_install INSTALL_MOD_PATH=~/.arm-stuff/images/root/

# copy over firmware. Ideally use the original firmware (/lib/firmware) from the Chromebook.
git clone git://git.kernel.org/pub/scm/linux/kernel/git/dwmw2/linux-firmware.git
cp -rf linux-firmware/* ~/.arm-stuff/images/root/lib/firmware/
rm -rf linux-firmware
echo "console=tty1 debug verbose root=/dev/mmcblk1p3 rootwait rw rootfstype=ext4" >
/tmp/config-sd
echo "console=tty1 debug verbose root=/dev/sda3 rootwait rw rootfstype=ext4" > /tmp/config-usb

vbutil_kernel --pack /tmp/newkern-sd --keyblock /usr/share/vboot/devkeys/kernel.keyblock
--version 1 --signprivate /usr/share/vboot/devkeys/kernel_data_key.vbprivk
--config=/tmp/config-sd --vmlinuz kernel.itb --arch arm
vbutil_kernel --pack /tmp/newkern-usb --keyblock /usr/share/vboot/devkeys/kernel.keyblock
--version 1 --signprivate /usr/share/vboot/devkeys/kernel_data_key.vbprivk
--config=/tmp/config-usb --vmlinuz kernel.itb --arch arm
```

06. 准备引导分区

```
dd if=/tmp/newkern-sd of=$bootp1 # first boot partition for SD
dd if=/tmp/newkern-usb of=$bootp2 # second boot partition for USB

umount $rootp

kpartx -dv $loopdevice
losetup -d $loopdevice
```

07. 用 dd 克隆镜像然后标记 USB 为可引导

```
dd if=kali-custom-chrome.img of=/dev/sdb bs=512k
```

```
cgpt repair /dev/sdb
```

这里,你要给分区 1 还是分区 2 标记更高的优先权.数字大则有更高的优先权.如下的例子将把第一个分区(用-i 参数)的优先权设置成 10,因为我们要从 SD 卡引导.

```
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: priority=10 tries=5 successful=1
40960	32768	2	Label: "KERN-B" Type: ChromeOS kernel UUID: 37CE46C9-0A7A-4994-80FC-9C0FFCB4FDC1 Attr: priority=5 tries=5 successful=1
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:~#
```

这个操作完成后, 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.

三、定制 ODROID X2 U2 镜像

The following document describes our own method of creating a **custom Kali Linux ODROID image** and is targeted at developers. If you would like to install a pre-made Kali ODROID image, check our [Install Kali on ODROID](#) article.

01. Create a Kali rootfs

Start by building a [Kali rootfs](#) as described in our Kali documentation using an **armhf** architecture. By the end of this process, you should have a populated rootfs directory in `~/arm-stuff/rootfs/kali-armhf`.

02. Create the Image File

Next, we create the physical image file which will hold our ODROID rootfs and boot images.

```
apt-get install kpartx xz-utils
cd ~
mkdir -p arm-stuff
cd arm-stuff/
mkdir -p images
cd images
dd if=/dev/zero of=kali-custom-odroid.img bs=1MB count=5000
```

03. Partition and Mount the Image File

```
parted kali-custom-odroid.img --script -- mklabel msdos
parted kali-custom-odroid.img --script -- mkpart primary fat32 4096s 266239s
parted kali-custom-odroid.img --script -- mkpart primary ext4 266240s 100%
```

```
loopdevice=`losetup -f --show kali-custom-odroid.img`
device=`kpartx -va $loopdevice | sed -E 's/.*(loop[0-9])p.*/\1/g' | head -1`
device="/dev/mapper/${device}"
```

```
bootp=${device}p1
rootp=${device}p2
mkfs.vfat $bootp
mkfs.ext4 -L kaliroot $rootp
mkdir -p boot root
mount $bootp boot
mount $rootp root
```

04. Copy and Modify the Kali rootfs

Copy over the Kali rootfs you bootstrapped earlier using **rsync** to the mounted image.

```
cd ~/arm-stuff/images/
rsync -HPavz ~/arm-stuff/rootfs/kali-armhf/ root
echo nameserver 8.8.8.8 > root/etc/resolv.conf
```

Edit the `~/arm-stuff/images/root/etc/inittab` file and locate the “Example how to put a getty on a serial line”.

```
nano root/etc/inittab
```

Add the following line to the end of that section.

```
T1:12345:respawn:/sbin/agetty 115200 ttySAC1 vt100
```

If you want the serial console to autologin as root, use the following line instead:

```
T1:12345:respawn:/bin/login -f root ttySAC1 </dev/ttySAC1 >/dev/ttySAC1 2>&1
```

Now, make sure there is a `ttySAC1` entry in the `~/arm-stuff/images/root/etc/udev/links.conf` file.

```
nano root/etc/udev/links.conf
```

If an entry for `ttySAC1` doesn't already exist, add it to the file so it looks as follows:

```
M null          c  1 3
M console       c  5 1
M ttySAC1       c  5 1
```

Add `ttySAC` entries in the `~/arm-stuff/images/root/etc/udev/links.conf` file.


```
cat << EOF >> root/etc/securetty
ttySAC0
ttySAC1
ttySAC2
EOF
```

Place a basic xorg.conf file in the rootfs.

```
cat << EOF > root/etc/X11/xorg.conf
# X.Org X server configuration file for xfree86-video-mali
```

```
Section "Device"
    Identifier "Mali-Fbdev"
#   Driver   "mali"
    Option   "fbdev"           "/dev/fb6"
    Option   "DRI2"            "true"
    Option   "DRI2_PAGE_FLIP"  "true"
    Option   "DRI2_WAIT_VSYNC" "true"
    Option   "UMP_CACHED"      "true"
    Option   "UMP_LOCK"        "false"
EndSection
```

```
Section "Screen"
    Identifier "Mali-Screen"
    Device     "Mali-Fbdev"
    DefaultDepth 16
EndSection
```

```
Section "DRI"
    Mode 0666
EndSection
EOF
```

Link **init** in the root, rootfs directory:

```
cd ~/arm-stuff/images/root
ln -s /sbin/init init
```

05. Compile the ODROID Kernel and Modules

If you're not using ARM hardware as the development environment, you will need to set up an [ARM cross-compilation environment](#) to build an ARM kernel and modules. Once that's done, proceed with the following instructions.

We next need to fetch the ODROID kernel sources and place them in our development tree structure:

```
cd ~/arm-stuff
mkdir -p kernel
cd kernel
git clone --depth 1 https://github.com/hardkernel/linux.git -b odroid-3.0.y odroid
cd odroid
```

Configure, then cross-compile the ODROID kernel.

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

```
# for ODROID-X2
make odroidx2_ubuntu_defconfig
# for ODROID-U2
make odroidu2_ubuntu_defconfig
# configure your kernel !
make menuconfig
make -j $(cat /proc/cpuinfo|grep processor|wc -l)
make modules_install INSTALL_MOD_PATH=~/.arm-stuff/images/root/
```

Chroot into the rootfs and create an [initrd](#). Make sure to use the correct kernel version/extraversion for the `mkinitramfs` command. In our case, it was "3.0.63" .

```
LANG=C chroot ~/.arm-stuff/images/root/
apt-get install initramfs-tools uboot-mkimage
cd /
# Change the example "3.0.65" to your current odroid kernel revision
mkinitramfs -c gzip -o ./initramfs 3.0.65
mkimage -A arm -O linux -T ramdisk -C none -a 0 -e 0 -n initramfs -d ./initramfs ./uInitrd
rm initramfs
exit
```

06. Prepare the Boot Partition

Copy the kernel and generated initrd file to the mounted boot partition as shown below.

```
mv ~/.arm-stuff/images/root/uInitrd ~/.arm-stuff/images/boot/
cp arch/arm/boot/zImage ~/.arm-stuff/images/boot/
```

Dump a **boot.txt** file, which contains required boot parameters for the ODROID in the boot partition.

```
cat << EOF > ~/arm-stuff/images/boot/boot.txt
setenv initrd_high "0xffffffff"
setenv fdt_high "0xffffffff"
setenv bootcmd "fatload mmc 0:1 0x40008000 zImage; fatload mmc 0:1 0x42000000 uInitrd;
bootm 0x40008000 0x42000000"
setenv bootargs "console=tty1 console=ttySAC1,115200n8 root=LABEL=kaliroot rootwait ro
mem=2047M"
boot
EOF
```

Generate a **boot.scr** file, which is required to boot the ODROID.

```
mkimage -A arm -T script -C none -n "Boot.scr for odroid-x" -d ~/arm-stuff/images/boot/boot.txt
~/arm-stuff/images/boot/boot.scr
```

Unmount the root and boot partitions, then umount the loop device.

```
cd ~/arm-stuff/images/
umount $bootp
umount $rootp
kpartx -dv $loopdevice
```

```
wget http://www.mdrjr.net/odroid/mirror/BSPs/Alpha4/unpacked/boot.tar.gz
tar xzpf boot.tar.gz
cd boot
sh sd_fusing.sh $loopdevice
cd ..
losetup -d $loopdevice
```

Now, image the file onto your USB storage device. Our device is **/dev/sdb**. Change this as needed.

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

Once this operation is complete, connect your UART serial cable to the ODROID and boot it up with the microSD/SD card plugged in. Through the serial console, you will be able to log in to Kali (root / toor) and startx.

If everything works and you want the ODROID to start on boot, make sure to use the “autologin” line in the inittab given above and add the following to your bash_profile:

```
# If you don't have a .bash_profile, copy it from /etc/skel/.profile first
cat << EOF >> ~/.bash_profile
if [ -z "$DISPLAY" ] && [ $(tty) = /dev/ttySAC1 ]; then
    startx
fi
EOF
```

08. Install Mali Graphic Drivers (Optional)

These steps are experimental and not fully tested yet. They should be preformed inside the Kali rootfs.

```
#
http://malideveloper.arm.com/develop-for-mali/drivers/open-source-mali-gpus-linux-exadri2-and-
x11-display-drivers/
apt-get install build-essential autoconf automake make libtool xorg xorg-dev xutils-dev
libdrm-dev
wget
http://malideveloper.arm.com/downloads/drivers/DX910/r3p2-01rel0/DX910-SW-99003-r3p2-01r
el0.tgz
wget
http://malideveloper.arm.com/downloads/drivers/DX910/r3p2-01rel0/DX910-SW-99006-r3p2-01r
el0.tgz
wget --no-check-certificate https://dl.dropbox.com/u/65312725/mali_opengl_hf_lib.tgz

tar -xzf mali_opengl_hf_lib.tgz
cp mali_opengl_hf_lib/* /usr/lib/

tar -xzf DX910-SW-99003-r3p2-01rel0.tgz
tar -xzf DX910-SW-99006-r3p2-01rel0.tgz
cd DX910-SW-99003-r3p2-01rel0/x11/xf86-video-mali-0.0.1/
./autogen.sh
chmod +x configure

CFLAGS="-O3 -Wall -W -Wextra -I/usr/include/libdrm
-IDX910-SW-99006-r3p2-01rel0/driver/src/ump/include" LDFLAGS="-L/usr/lib -IMali -IUMP
-lpthread" ./configure --prefix=/usr --x-includes=/usr/include --x-libraries=/usr/lib
cp -rf ../../DX910-SW-99006-r3p2-01rel0/driver/src/ump/include/ump src/
mkdir -p umplock
cd umplock
wget
http://service.i-onik.de/a10_source_1.5/lichee/linux-3.0/modules/mali/DX910-SW-99002-r3p0-04
rel0/driver/src/devicedrv/umplock/umplock_ioctl.h
cd ..
```

```
make
make install
```

四、 定制 MK/SS808 Kali 镜像

The following document describes our own method of creating a **custom Kali Linux MK/SS808 ARM image** and is targeted at developers. If you would like to install a pre-made Kali image, check out our [Install Kali on MK/SS808](#) article.

01. Create a Kali rootfs

Build yourself a [Kali rootfs](#) as described in our Kali documentation, using an **armhf** architecture. By the end of this process, you should have a populated rootfs directory in `~/arm-stuff/rootfs/kali-armhf`.

02. Create the Image File

Next, we create the physical image file which will hold our MK/SS808 rootfs and boot images.

```
apt-get install kpartx xz-utils sharutils
cd ~
mkdir -p arm-stuff
cd arm-stuff/
mkdir -p images
cd images
dd if=/dev/zero of=kali-custom-ss808.img bs=1MB count=5000
```

03. Partition and Mount the Image File

```
parted kali-custom-ss808.img --script -- mklabel msdos
parted kali-custom-ss808.img --script -- mkpart primary ext4 1 -1
loopdevice=`losetup -f --show kali-custom-ss808.img`
device=`kpartx -va $loopdevice| sed -E 's/.*(loop[0-9])p.*/\1/g'| head -1`
device="/dev/mapper/${device}"
rootp=${device}p1
```

```
mkfs.ext4 $rootp
mkdir -p root
mount $rootp root
```

04. Copy and Modify the Kali rootfs

```
rsync -HPavz /root/arm-stuff/rootfs/kali-armhf-xfce4/ root
echo nameserver 8.8.8.8 > root/etc/resolv.conf
```

05. Compile the rk3066 Kernel and Modules

If you're not using ARM hardware as the development environment, you will need to set up an [ARM cross-compilation environment](#) to build an ARM kernel and modules. Once that's done, proceed with the following steps.

```
apt-get install xz-utils
cd ~/arm-stuff
mkdir -p kernel
cd kernel

git clone git://github.com/aloksinha2001/picuntu-3.0.8-alok.git rk3066-kernel
cd rk3066-kernel
sed -i "/vpu_service/d" arch/arm/plat-rk/Makefile
export ARCH=arm
export CROSS_COMPILE=~/.arm-stuff/kernel/toolchains/arm-eabi-linaro-4.6.2/bin/arm-eabi-

# A basic configuration for the UG802 and MK802 III
# make rk30_hotdog_ti_defconfig
# A basic configuration for the MK808
make rk30_hotdog_defconfig

# configure your kernel !
make menuconfig

#          Configure          the          kernel          as          per
http://www.armvtech.com/armvtechforum/viewtopic.php?f=66&t=835
mkdir ../initramfs/
wget http://208.88.127.99/initramfs.cpio -O ../initramfs/initramfs.cpio

mkdir -p ../patches
wget          http://patches.aircrack-ng.org/mac80211.compat08082009.wl_frag+ack_v1.patch
-O ../patches/mac80211.patch
wget          http://patches.aircrack-ng.org/channel-negative-one-maxim.patch-
-O ../patches/negative.patch
```

```
patch -p1 < ../patches/mac80211.patch
patch -p1 < ../patches/negative.patch

./make_kernel_ruikemei.sh
make modules -j$(cat /proc/cpuinfo|grep processor|wc -l)
make modules_install INSTALL_MOD_PATH=~/.arm-stuff/images/root
git clone git://git.kernel.org/pub/scm/linux/kernel/git/dwmw2/linux-firmware.git firmware-git
mkdir -p ~/.arm-stuff/images/root/lib/firmware
cp -rf firmware-git/* ~/.arm-stuff/images/root/lib/firmware/
rm -rf firmware-git
umount $rootp
kpartx -dv $loopdevice
losetup -d $loopdevice
```

07. dd the Image to a USB device

Use the **dd** utility to image this file to your SD card. In our example, we assume the storage device is located at `/dev/sdb`. **Change this as needed.**

```
dd if=kali-custom-ss808.img of=/dev/sdb bs=512k
```

Once the dd operation is complete, unmount and eject the SD card and boot your MK/SS808 into Kali Linux

五、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。

六、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。

七、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 策略

一、Kali Linux 工具策略

我们知道很多的工具或脚本都能做同样的工作. 有的比较好用, 有的是喜好问题. 为此, 保持渗透测试软件源的更新和可用是一项极具挑战性的任务. Kali 开发组使用如下检验标准来判断一个工具是否被包含在我们的发行版.

- 在渗透测试环境下该工具是否 可用/实用?
- 该工具的功能是否与别的工具重复?
- 该工具是否允许自由地重新分发?
- 该工具的依赖关系如何?能否在”独立”环境下运行?

根据这些问题的答案和其它的因素, 才决定该工具是否要标记包含在 Kali.

多数 Kali 开发组成员都从事渗透测试工作, 结合我们的经验, 同时从其它方面考虑, 从而为 Kali 发行版选择最有价值, 最好的工具. 以 DOS, DDOS 为目的或无名的工具很少用于合法用途, 因此默认不会被安装在 Kali Linux.

请求添加新工具

我们的大门永远向新的和更好的工具敞开, 但是每个工具都必须是有用的. 请在提交工具上放一些心思和精力, 不要只给开发者发一行消息. 可以通过我们的 [Kali Linux 漏洞追踪系统](#)提交新的工具请求..

二、Kali Linux Root 用户策略

大部分发行版鼓励它们的用户使用一般用户权限来操作. 这是个明智的安全忠告, 它使得用户和 OS 之间有一个额外的保护层. 特别是对于需要权限分离的多用户系统.

Kali Linux 本质上是一个安全和审计平台, 许多工具都需要用 root 权限运行. 通常, 使用 Kali

Linux 时,不可能是多用户环境,因此默认用户是”root”.此外不建议 Linux 新手使用 Kali Linux,因为他们在使用超级用户时更容易制造毁灭性的错误.

三、Kali Linux 开源软件策略

Kali Linux 的主要包含了数以千计的自由软件包.作为 Debian 的衍生版,Kali 所有的自由软件都遵循 Debian 的自由软件准则.

与上述不同的是,Kali Linux 的非自由软件部分包含了一系列由 Offensive Security 重新分发的非开源工具,这些工具已经经过开发商的默认许可或特别许可.在把每个 Kali 专有的非开源软件包导入到你的 Kali 衍生版之前,你应该先详查这个软件包的授权(从 Debian 导入的非开源软件包除外).

更重要的是,所有 Kali 的专有开发或软件整合都已经投入到 GNU GPL 下.

如果你想获得更多关于指定软件授权的信息,可以查阅源码包中的 `debian/copyright` 或从 `/usr/share/doc/package/copyright` 查阅已经安装的包的授权信息.

四、Kali Linux 安全更新策略

Kali Linux 和 Debian 的源有紧密的联系,因此安全更新会像 Debian 发行版一样频繁,更新的都是 debian 维护的包(大部分).其它包则由 Kali 团队尽力的维护.

五、Kali Linux 网络服务策略

Kali Linux 处理网络服务这点上与大部分别的发行版不同.最主要的是 Kali 默认不启用任何外部监听的服务,目的是在渗透测试时保持最低程度的探测.

Kali 默认安装了很多服务,例如 Apache 和 SSH.但在需要时你要手动运行他们.

07. 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 IRC 频道

Kali Linux has an official IRC channel located on the [Freenode](#) network. The official IRC channel is `#kali-linux` Please take a few moments to review the rules and guidelines below before joining the channel

IRC Rules and Guidelines

We try to remain as informal as possible but there are some rules that we'd appreciate if you would follow! Broadly, if you're friendly, tolerant, and reasonable, you'll probably get a long way without any specific knowledge of the rules - but for the avoidance of doubt, here they are.

How to Treat Other Users

In order to make the channel a pleasant place for all of our users, we expect all to remain as friendly and tolerant as possible. We request that you refrain from profanity and that you show respect to channel members and visitors. If you find that you're becoming frustrated with the channel or other users, we encourage you to take a moment to do something

else. Try to ensure you don't make people feel like you're just taking advantage of them - help others out while you're waiting for a reply to your questions, and say thanks!

How to Argue

As mentioned above, we'd appreciate it if you'd strive to be friendly and tolerant. We also encourage debates and in-depth discussions about topical subjects. If you choose to participate in one, we expect you to remain as reasonable as possible and employ the skills of logic and critical thinking. These skills will serve you well in discussion, enable you to communicate more efficiently, and spot when others are being less than forthcoming with the truth!

Staying on Topic

We maintain no strict policy regarding off-topic chat in the channel however, the discussion of Kali Linux projects is the primary focus of the channel, so you may be asked to take discussions elsewhere, particularly if there are venues on freenode better suited to them (such as ##politics), if there are other conversations going on, or if they're repetitive or otherwise seen by the channel staff as being detrimental to the good atmosphere of the channel.

Certain things are seen as being specifically off-topic. These topics include:

Support or encouragement of illegal activity - it should go without saying, but we don't exist to help you break the law or do things you shouldn't be doing. Such queries are off-topic for the channel, for freenode as a whole, and may well get you removed from the channel and/or network. Please don't ask. Laws vary from country to country and channel OPs may determine whether a specific discussion is appropriate for the channel or not. Warez/Cracks/Pirated Software - these too are offtopic for the channel and network so please don't ask.

Political/Religious Matters

Many people have very strong political/religious beliefs and we respect that. We also recognize that these are volatile topics, which have nothing to do with Kali Linux and are best discussed elsewhere.

Asking for Help

If you're asking for help, first off, thanks! - questions and the resulting discussion of the answer(s) in a collaborative environment are what make IRC great and by helping to add to the atmosphere, you benefit all of us. We often find that we learn a lot even from questions we already think we know the answers to - about people, alternative approaches, and cool new resources and tools. However, if you are intending to ask a question, we'd appreciate it if you'd follow a couple useful guidelines to help you, and us, make the best use of our time: Do your research first - it's very frustrating when people ask a question that can virtually be answered by punching the keywords into a Google search! We also have forums and a wiki that contain answers to many questions we see daily so it's to everyone's benefit if these assets are used before asking in IRC.

Give Us the Whole Picture

If you're asked for more information, please provide it accurately. The correct answer will depend on it. Looking at this from another angle: the more we learn about your problem, the more this independently benefits us too - a large part of the development of new releases is derived from helping others with issues discovered with specific setups; even if you're asking us questions, you can help teach us something too! If you find the answer somewhere else, tell us - it isn't compulsory, but if you don't get an answer to your question in the channel but you find it elsewhere, consider letting us know! That way, we can help out the next person with a similar question. It also lets people know that you already have an answer you're happy with, or that if anyone's researching the question for you, they can stop. Wait for the answer - not everyone in the channel is online all the time - you may find you get an answer a few minutes, or even hours, later. Feel free to stick around and chat, or even answer other people's questions - you'll find it helps pass the time and makes others likely to help you! Help us build a community of friendly security professionals and enthusiasts.

Spam, Flooding, and Various Other Forms of Disruptive Behaviour

Spam, flooding, disrespect or verbal attacks against other users, misleading links, intentionally wrong answers, and other forms of disruptive behaviour not otherwise specified are unwelcome. Disruptive behaviour includes but is not restricted to the operation of unauthorised bots, public logging of the channel, and scripts such as those that publicly announce what track your MP3 player is playing or your away status. If you have more than 5 lines of text to paste, use [pastebin](#) for your data and then paste the URL into channel.

Dealing With the Channel Staff

From time to time, you may be asked to take conversations elsewhere, treat others reasonably, steer a conversation in a particular direction, or a variety of other things in order to preserve the ambiance and usefulness of the channel. If you're the target of such a request, please be as reasonable as you can and if you wish to take issue with it, do so in a private message with the channel staffer in question, rather than making noise in channel.

Discipline

Repeated breaking of the rules will cause channel staffers to mute (+q), ban (+b), kick, or otherwise remove you from the channel. This will particularly apply if you're seen to be willfully ignoring the rules after we've drawn your attention to them. Many forms of disruptive behaviour, such as flooding or trolling, may result in discipline without a warning. We try and avoid the use of force wherever possible and we'd appreciate it if you'd help us in pursuing this goal! If you're a bystander while a staffer is forced to use his or her powers for channel management, we'd appreciate your understanding and consideration in awaiting the end of the incident, and your assistance in keeping the situation as favorable as possible by not complaining, commentating, or gloating. This serves to make antisocial behavior such as flooding less attractive (the smaller the reaction, the less the return on the malfeasance), and so benefits you as well as us!

三、Kali Linux 社区论坛

Kali Linux has official community-driven forums located at forums.kali.org. We welcome everyone to the Kali Linux community and we have outlined a few simple rules below. Please take a few moments to review them before joining the forums.

论坛规则

- By registering with our forums you agree to be bound by the following rules.
- We do not condone any illegal activity at all.
- Any advice/information offered in the forums is to be used for the legal informational/professional/educational purposes for which it is intended.

- New registrants posts will be moderated first, causing a slight delay in the post appearing – DO NOT report problems with your post not appearing instantly during your first 3 days of membership.
- Use sensible descriptive titles for your posts – not titles such as “Please Help!!” or “Need Assistance” or “what Am I Doing Wrong?” etc
- Do not cross-post – 1 post in the relevant area is enough!
- Search for related previous postings before creating a new thread. If you create a new thread asking something that has already been asked, don’t be surprised if the thread gets deleted without notice.
- Do not post about breaking into networks that do not belong to you and for which you have no permissions.
- Any religious, political, or pornographic references will not be tolerated.
- Posts like – “Oooh! look!! I’ve cracked my neighbours wireless AP” or “How do I hack a network!?” are not needed here, thanks.
- Please don’t bother with spam messages – they will be removed/moved/edited/deleted and you will be banned.
- Members signatures may NOT contain URL links, in any form.
- We will not tolerate abusive, sexist, racist, or any other derogatory remarks, or members acting like self-appointed moderators. The forum staff are here to help you. Please use their services. If ANY member has an issue with the content of ANY post within the forums, use the “REPORT THIS POST” button – This is the red triangle icon when using the default forum theme, or the asterisk icon when using the Blackfire Razor forum theme, found in the top right corner of each post.
- Breaking the forum rules may incur infractions ranging from loss of posting privileges to a temporary or permanent ban.
- These rules are subject to alteration and/or addition. It is your responsibility to be aware of any changes.

四、Kali Linux 官方镜像

官方源的使用

Kali Linux 提供了 3 类软件源, 这些源在世界各地都有镜像:

- [http.kali.org](http://kali.org) (镜像列表): 主要安装包软件源;
- security.kali.org (镜像列表): 安全包软件源;
- cdimage.kali.org (镜像列表): ISO 镜像源.

当你使用以上的 3 个域名做源时, 会自动连接到离你最近的与官方同步的镜像. 如果你要手动选择一个镜像, 请点击上面域名旁的 *镜像列表*, 选一个合适你的.

Kali Linux 镜像的架设

要架设一个 Kali Linux 的官方镜像源, 你需要一台运行 rsync 和 ssh, 大硬盘, 大带宽的服务器.

截至 2013-03-14, 主要安装包软件源大约 160G, ISO 镜像源大约 10G. 但应该考虑到这些数字在不停的增长.

我们希望你通过 HTTP, FTP 或 RSYNC 之一来同步镜像文件, 所以必须安装相应的服务.

软件包档案的同步推送

当官方源有更新时会用基于 SSH 的触发器 ping 镜像. 一般每天 4 次.

如果你还没有专用于镜像的帐号, 先创建一个. (本例子中我们专用于镜像的专用用户是 "archvsync"):

```
$ sudo adduser --disabled-password archvsync
Adding user 'archvsync' ...
[...]
Is the information correct? [Y/n]
```

创建用于存放镜像的目录, 然后修改目录属主为刚才创建的专用用户:

```
$ sudo mkdir /srv/mirrors/kali{,-security,-images}
$ sudo chown archvsync:archvsync /srv/mirrors/kali{,-security,-images}
```

下一步配置 rsync 后台程序 (按需启用后台运行) 导出这些目录:

```
$ sudo sed -i -e "s/ENABLED=false/ENABLED=true/" /etc/default/rsync
$ sudo vim /etc/rsyncd.conf
$ cat /etc/rsyncd.conf
uid = nobody
gid = nogroup
max connections = 25
socket options = SO_KEEPALIVE

[kali]
path = /srv/mirrors/kali
comment = The Kali Archive
read only = true
```

```
[kali-security]
path = /srv/mirrors/kali-security
comment = The Kali security archive
read only = true
```

```
[kali-images]
path = /srv/mirrors/kali-images
comment = The Kali ISO images
read only = true
```

```
$ sudo service rsync start
```

```
Starting rsync daemon: rsync.
```

这个文档不包括 WEB 服务器和 FTP 服务器的配置. 理论上你应该导出镜像到 <http://yourmirror.net/kali> , <http://yourmirror.net/kali-security> 和 <http://yourmirror.net/kali-images> (FTP 也一样).

现在是有趣的部分: 专用用户处理 SSH 触发器配置和镜像站点的搭建. 首先应该用专用用户解压 [ftpsync.tar.gz](http://archive.kali.org/ftpsync.tar.gz):

```
$ sudo su - archvsync
$ wget http://archive.kali.org/ftpsync.tar.gz
$ tar xzf ftpsync.tar.gz
```

现在我们要创建两个配置文件. 在模板的基础上至少要修改 *MIRRORNAME*, *TO*, *RSYNC_PATH*, 和 *RSYNC_HOST* 这几个参数.:

```
$ cp etc/ftpsync.conf.template etc/ftpsync-kali.conf
$ cp etc/ftpsync.conf.template etc/ftpsync-kali-security.conf
$ vim etc/ftpsync-kali.conf
$ grep -E '^[^#]' etc/ftpsync-kali.conf
MIRRORNAME=`hostname -f`
TO="/srv/mirrors/kali/"
RSYNC_PATH="kali"
RSYNC_HOST=archive.kali.org
$ vim etc/ftpsync-kali-security.conf
$ grep -E '^[^#]' etc/ftpsync-kali-security.conf
MIRRORNAME=`hostname -f`
TO="/srv/mirrors/kali-security/"
RSYNC_PATH="kali-security"
RSYNC_HOST=archive.kali.org
```

最后一步建立. `ssh/authorized_keys` 以便 `archive.kali.org` 能触发你的镜像.:

```
$ mkdir -p .ssh
$ wget -O - -q http://archive.kali.org/pushmirror.pub >>.ssh/authorized_keys
```

如果你的 `ftpsync.tar.gz` 不是解压到 `home` 目录, 那么你要修正 `ssh/authorized_keys` 中的 `~/bin/ftpsync` 为相应的路径.

现在发一封包含你的镜像URL的 email 到 devel@kali.org, 以便把你的镜像加入镜像列表. 请明确的指出当镜像出现问题(或要进行更改/协商镜像的配置)时我们该联系谁.

与其等待 `archive.kali.org` 的第一次推送, 不如先用离你近的源进行 `rsync` 初始化同步, 选择上面镜像列表里的任意一个镜像. 假设你选了 `archive-4.kali.org`, 那么你应该以专用用户权限运行如下命令:

```
$ rsync -qaH archive-4.kali.org::kali /srv/mirrors/kali/ &
$ rsync -qaH archive-4.kali.org::kali-security /srv/mirrors/kali-security/ &
$ rsync -qaH archive-4.kali.org::kali-images /srv/mirrors/kali-images/ &
```

手工同步 ISO 镜像

ISO 镜像源不使用推送同步模式, 所以你要建立一个每日运行的 `rsync` 计划任务. 我们提供了一个可直接用的脚本 `bin/mirror-kali-images`, 你只要配置 `etc/mirror-kali-images.conf`, 再以专用用户权限把它添加到 `crontab`.

```
$ sudo su - archvsync
$ cp etc/mirror-kali-image.conf.sample etc/mirror-kali-images.conf
$ vim etc/mirror-kali-images.conf
$ grep -E '^[^#]' etc/mirror-kali-images.conf
TO=/srv/mirrors/kali-images/
$ crontab -e
$ crontab -l
# m h dom mon dow    command
39 3 * * * ~/bin/mirror-kali-images
```

请设置一个精确的时间, 以防 `archive.kali.org` 由于同一时间过多的同步而超负荷..

五、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
- docs.kali.org
- forums.Kali.org
- bugs.kali.org
- 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。

社交媒体

- [twitter](#)
- [facebook](#)
- 千人 QQ 群号：89927936
- 公众号名称：kali Linux
- 微信号：kali-Linux



微信二维码

我们在有重要信息的时候才发推。发布信息和博客文章都会被推送到我们的 twitter。账户是[@KaliLinux](#)。中国地区会通过微信公众平台同时发布最新资讯。

六、提交 Kali 的技术问题

这里指导一个报告者如何提交一份最好的问题报告,以便问题能尽快的被修复. 问题报告者的目的是让 Kali Linux 的开发者问题重现然后发现问题. 如果 Kali 开发者发现了问题,他们会收集更多的信息直到找到问题的根本. 否则,他们会要求提供更多的信息直到他们出现提交者遇到的问题. 请记住,我们的开发团队使用英文,所以最好用**英文**提交.

Kali Linux 诞生于对社区的回报. 社区促使我们的项目得以更好的保持持续发展. 在你写评论时请记住,为你提供支持的开发者都是无私奉献的志愿者.

想要解决问题,请明确以下的要点:

- 你是因为想要解决问题才提交的问题,所以请提供全面的信息.
- 弄清楚你提交的是事实还是假设.
- 保持问题报告的客观性,只陈述经过适当研究后的事实.
- 不要引用 Wikipeda 和其它非主要资源的结果作为报告.
- 一个 BUG,不要以不同的报告,不同的人,不同的硬件多次提交.
- 不要把多个问题堆在一起报告,如果可以请分别提交.
- 不要发类似“Me too!”或“+1”这样的评论.
- 不要抱怨修复一个漏洞为何那么久.

Kali Linux 问题追踪系统在 <http://bugs.kali.org>. 这篇文档指导你如何创建帐号,如何创建系统资料,和如何提交一份详细的报告.

创建 Kali Linux 问题追踪系统帐户

如果你还没有创建帐户,应该先完成这一步. 创建用户后你才可以提交问题报告或对已存在的问题进行评论.

在问题追踪系统页面,点击 ‘Signup for new account’ 开始创建.

KALI LINUX BUG TRACKER

Anonymous | [Login](#) | [Signup for a new account](#) 2013-03-20 05:25 EDT

[Main](#) | [My View](#) | [View Issues](#) | [Change Log](#) | [Roadmap](#) | [Repositories](#)

Unassigned [^] (1 - 10 / 47)

0000147	syslinux.cfg contains a few mistakes [All Projects] General Bug - 2013-03-19 21:38
0000146	The debian openssl has a --no-sslv2 patch [All Projects] Kali Package Bug - 2013-03-19 15:42
0000143	Automated HTTP Enumeration Tool [All Projects] New Tool Requests - 2013-03-19 14:40
0000142	Unhide Forensic Tool, Find hidden processes and ports [All Projects] New Tool Requests - 2013-03-19 14:39
0000140	Inguma [All Projects] New Tool Requests - 2013-03-19 14:37
0000139	Junkie [All Projects] New Tool Requests - 2013-03-19 14:36
0000138	sqlmap [All Projects] Tool Upgrade - 2013-03-19 14:08
0000135	android-sdk issue [All Projects] General Bug - 2013-03-19 13:01
0000130	Need to upgrade python-usb from 0.8 to 1.0 for libusb software

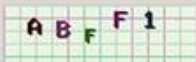
Resolved [^] (1 - 5 / 5)

0000122	msfpro console fails to launch [All Projects] General Bug - 20
0000076	b43 wireless driver firmware r [All Projects] Kali Package Bug
0000102	The Social-Engineer Toolkit (SE [All Projects] Tool Upgrade - 20
0000100	Social Engineering Tool cannot [All Projects] General Bug - 20
0000063	No Keyboard or Mouse after M [All Projects] General Bug - 20

输入用户名和 email, 然后输入验证码. 点击 signup 按钮.

KALI LINUX BUG TRACKER

Signup

Username:	<input type="text" value="NewBugSubmitter"/>
E-mail:	<input type="text" value="nbs@email.com"/>
Enter the code as it is shown in the box on the right.:	<div><input type="text" value="ABFF1"/></div>

On completion of this form and verification of your answers, you will be sent a confirmation e-mail to the e-mail address you specified. Using the confirmation e-mail, you will be able to activate your account. If you fail to activate your account within seven days, it will be purged. You must specify a valid e-mail address in order to receive the account confirmation e-mail.

Signup

[[Login](#)] [[Lost your password?](#)]

如果成功了, 下一步会提示你帐户已经注册好. 要激活帐户请回复官方的 email 确认邮件. 点击” Proceed” 继续到漏洞追踪系统登录页面.



在 Kali Linux 问题追踪系统创建一份资料

不是必须的,但是作为你的帐户的一部分,建议创建一份独特的资料.你可以为每个系统创建自定义的资料,或者从默认资料里选择.这些资料用于报告时定义你的平台,操作系统和版本信息.

创建或编辑自定义资料,从主页选择 My Account 然后选择 Profiles.为你的系统添加具体的信息和描述,完成时点击” Add Profile” 按钮.

The image shows two web forms. The top form is titled 'Add Profile' and has links for '[My Account]', '[Preferences]', '[Manage Columns]', and '[Profiles]'. It contains four input fields: 'Platform' (Intel x64), 'Operating System' (Kali), 'OS Version' (1.0.1), and 'Additional Description' (Linux kali 3.7-trunk-amd64 #1 SMP Debian 3.7.2-0+kali6 x86_64 GNU/Linux, -This system is a VMWare guest system, -VMWare Fusion Professional Version 5.0.3 (1040386), -2 processor cores (2.6GHz Intel Core i7), -4096MB RAM). A red asterisk indicates required fields. An 'Add Profile' button is at the bottom right. The bottom form is titled 'Edit or Delete Profiles' and has three radio buttons: 'Edit Profile' (selected), 'Make Default', and 'Delete Profile'. It has a 'Select Profile' dropdown menu and a 'Submit' button.

资料添加好后, 在你创建一个新的问题报告时会出现” Select Profile” 下拉菜单. 可以根据你的需要创建不同的配置文件, 只要你在提交问题报告时选择正确的配置文件.

在开始报告之前, 在网站搜索和你的问题相关的关键字. 如果存在已经被报告的问题(与硬件无关), 请不要重复提交或者添加没有必要的注释, 例如” Me too!” 或者” +1”. 你可以点击 ID 链接来查看问题的状态.

如果你认为问题和硬件有关, 即使类似的硬件也报告过, 也请以你的具信息提交一份新的报告. 你的硬件与别硬件不一定完全相同. 不要以为同样的桌面或者笔记本型号就不可能遇到不一样的问题.

创建报告

开始你的报告, 登入你的帐户然后点击登录页面上的” Report Issue”. 你需要填尽可能多的信息. 必要时请查看本文前面提出的那几点要求.

报告中必须包含以下字段:

- Category(分类)
- Summary(摘要)
- Description(描述)

其它字段不是必须的, 但我们请特别多注意下面每个选项:

- Reproducibility(重现性)
- Select Profile(选择资料)
- Steps to Reproduce(重现步骤)
- Additional Information(附加信息)
- Upload File (error logs, screenshot)-上传文件(错误日志,屏幕截图)

选择适当的分类

目前 Kali 的问题被分为 4 类. 报告问题之前请先确定它的类别:

- General Bug(一般问题)
- Kali Package Bug(Kali 软件包问题)
- New Tool Requests(请求添加新工具)
- Tool Upgrade(工具升级)

不要提出问题追踪系统不支持的请求. Kali Linux 提供许多可选的支持, 包括 <http://docs.kali.org> , <https://forums.kali.org> 和 freenode 上的 IRC 聊天室(#kali-linux).

提供一个描述性的摘要

摘要字段本质上是一个问题报告的”名字”, Kali 开发者和其它访问者会第一个看它. 提供一个简短但具描述性的摘要可以描述问题或者明确要求.

Good: Chromium Package installed from Repo will not run as root user(优: 从源安装的 Chromium 软件包不能用 root 运行)

Bad: Chromium doesn' t work(劣: chromium 不能运行)

摘要不应该包括所有东西, 除非必须要包含它才能传达你提交报告的原因.

使用 dpkg 为问题报告找到软件包和软件版本

你可以用 dpkg 参数组合找到安装过哪个软件包. 在你的报告中列入这些命令的输出结果很重要. 输出结果也可以以文本文件格式上传. (在本文后面讨论).

- search
- list
- status

例子的输出:

```

root@kali:~# which chromium
/usr/bin/chromium
root@kali:~# type chromium
chromium is /usr/bin/chromium
root@kali:~# dpkg --search /usr/bin/chromium
chromium: /usr/bin/chromium
root@kali:~# dpkg --list chromium
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name          Version      Architecture Description
+++-+-----+-----+-----+-----+
ii  chromium        24.0.1312.68 amd64      Google open source chromium web
root@kali:~# dpkg --status chromium
Package: chromium
Status: install ok installed
Priority: optional
Section: web
Installed-Size: 98439
Maintainer: Debian Chromium Maintainers <pkg-chromium-maint@lists.aliases.debian.org>
Architecture: amd64
Source: chromium-browser
Version: 24.0.1312.68-1
...Output Truncated...

```

建立描述方案

现在是提交经过你深思熟虑的报告的时候了. 尽可能多的提供细节和结果.

请务必在适当的地方包含如下内容:

- 任何错误信息的准确并完整的文本(屏幕截图或日志文件)
- 你具体输入了什么或者做过什么产生的问题
- 如果可以,提供一个修复建议或者补丁
- 软件包的版本和与依赖包有关系的任何信息
- 内核版本,C 共享库,或者别看起来合适的资料
- `uname -a`
- `dpkg -s libc6 | grep ^Version`
- 适当的时候,软件版本(例如 `python -V`)
- 你的硬件信息

- 如果你要报告硬件驱动问题,请列出你所有的硬件信息
- 在你系统上安装源里的 `lshw` 报告完整的硬件信息
- 添加其它相关的资料
- 别为报告”太长”而担心,只要是相关信息,有比没有更好.

例子

```
Package: Chromium
Architecture: amd64
Maintainer: Debian Chromium Maintainers
Source: chromium-browser
Version: 24.0.1312.68-1
I installed the chromium web browser from the Kali Linux repos, using the command
‘apt-get install chromium’. I launched the program from the Kali menu by selecting
Applications/Internet/Chromium Web Browser. Chromium did not launch as expected,
instead it provided an error pop-up window.
The error message stated, “Chromium cannot be run as root. Please start Chromium
as a normal user. To run as root, you must specify an alternate -user-data-dir for
storage of profile information”.
I clicked the Close button to close the pop up window.
uname -a output: Linux kali 3.7-trunk-amd64 #1 SMP Debian 3.7.2+kali6 x86_64
GNU/Linux
C Library Version: 2.13-38
```

再现性的重要

Kali Linux 问题追踪系统允许你提交被报告的问题出现频率. 如果你提交一个要求添加新工具或工具更新的请求, 简单的在下拉菜单选择 N/A. 如果提交问题, 请提供相应的回答.

继续回到上面的例子, Chromium 设计成无法用 root 启动, 你可以从下拉菜单选择 “总是” .

你提供了一个准确的反馈, 这很重要, 如果 Kali 开发者试图重现该问题, 他们需要知道该问题的发生的频率. 如果出问题的频率是偶尔, 但你却标着总是, 开发者可能会因为测试时没遇到问题而草率地关闭这个报告.

选择适当的资料

如上所述, 为每一个报告的问题使用一个自定义的资料是最好的. 如果没有创建自定义资料, 从下拉菜单中选择相应的资料. 在本指南发布时, 下列选项是可用的.

- armel Kali 1.0
- armhf Kali 1.0
- x64 Kali 1.0
- x86 Kali 1.0

提供重现该问题的步骤

与描述部分相比这部分虽然看起来可能是多余的, 但这部分只包含重现该问题采取的步骤. 一些步骤可能只起辅助作用, 但它们很重要务必尽力写. 可能缺少的就是那个重现问题必需的步骤.

例子:

1. Opened a terminal window by selecting Applications/Accessories/Terminal
2. Typed 'apt-get install chromium' in the terminal and hit enter to run the command
3. Attempted to run Chromium web browser by selecting Applications/Internet/Chromium Web Browser

提供更多信息

在这部分你可以提供与问题相关的更多的信息. 如果你有修复问题的方法, 请在这部分提供它. 同样的, 坚持事实和正确的写步骤很重要, 以便开发者能重现.

例子:

There is a simple fix that is well documented on several forums. I tried it and it fixed the issue for me.

- Using a text editor open /etc/chromium/default
- Add `--user-data-dir` flag
- i.e. `CHROMIUM_FLAGS="--user-data-dir"`

Can this be patched within the repo version of Chromium so adding this flag is not required for future releases?

上传相关文件

有时提供不是很容易提供的信息给开发组很重要. 报告的这部分允许你添加屏幕截图或者日志文件. 注意文件的大小限制.

你可以点击” Choose File” 按钮来添加一个文件. 它会打开系统的文件管理器然后上传你选择的文件. 选好文件之后点击” 打开” 按钮返回你的报告, 然后点击” Upload File” 按钮.

提交报告

至此, 你已经准备好提交报告了. 剩下的就是点击” Submit Report” 按钮. 你的报告会被提交然后分配到一个 tracking ID (追踪 ID). 报告会在你的” My View” 页面下的” Reported by Me” 看见. 你可以跟踪问题的解决.

摘要

问题报告的目的是帮助开发者用他们的双眼看到错误. 你可以通过提供详细的说明让他们和你一起亲自看到错误.

详细描述一切, 陈述采取了什么步骤, 看到了什么, 除了你期盼的结果外你做了什么.

尝试通过研究找到问题或解决办法. 如果你可以为你的系统提供一个解决问题的方案, 就可以给开发者提供同等级的问题报告. 让开发者知道你到底做过什么很重要, 以便让他们成功地重复过程. 这不该成为你解决异常问题的绊脚石.

准确, 清晰, 简明扼要地写报告, 以确保开发者不会误解你的意思.

开发者不会忽悠你, 准备好额外的信息以便他们问起.

请对你的请求有耐心, 开发者像你一样也想修复问题. 我们热爱我们的工作并以继续让 Kali 成为有史以来最尖端的渗透测试发行版为骄傲.

七、Kali Linux 招聘信息

蓝盾信息安全技术股份有限公司 kali 技术小组

简历邮箱: akast@ngsst.com （简历中写上你的相关技术案例）

工作地点: 广州

招聘类型: 全职员工、实习生（不少于三个月）。

学历要求: 原则上要求本科学历，但技术好的朋友可以不用考虑学历问题。

我们这里有丰富的学习资源和个人技术展示平台，加入我们会让你快速的进步，团队内部每周末都有各种类型的渗透比赛。

1. Debian 系 Linux 安全工程师

要求英语良好。

- 1、源代码编译和 deb 解包打包。
- 2、apt 更新服务器架设、维护。
- 3、负责 kali 系统里各类安全工具的汉化、全功能测试、编写测试报告，以及新工具收集。有渗透测试、无线安全经验者优先。

2. 渗透测试工程师

- 1、熟悉常见的 PHP/ASP/.NET/Java 等 WEB 脚本语言；
- 2、熟练使用主流渗透测试和扫描工具，如 IBM AppScan/HP Inspect/Nessus/Awvs 等；
- 3、具备独立 WEB 渗透能力，熟练掌握 SQL 注入/XSS/CSRF/文件上传/文件包含/命令执行等漏洞利用方法；
- 4、熟练掌握 Apache/IIS 等 WEB 服务器和 Mysql/Oracle/SQLserver 等数据库服务器的安全配置策略；
- 5、熟悉 Windows 和 Linux 等主流操作系统安全配置，了解内核安全机制；
- 6、渗透思路清晰，对社会工程学攻击方法有一定研究并能有效利用；
- 7、有内网渗透经验，熟悉 AD 运作原理、认证协议、管理方式，熟练域环境下的渗透；
- 8、需要有不少于 3 个不同类型的成功渗透案例。

3. 脚本漏洞挖掘工程师

- 1、熟悉常见的 PHP/ASP/.NET/Java 等 WEB 脚本语言，并至少熟练其中的一种；
- 2、擅长代码审计，能独立挖掘 WEB 应用安全漏洞，需要有不少于 3 个成功的漏洞挖掘案例。
- 3、熟练使用 Shell、Perl、Python、ruby 其中的一种脚本语言编写相应的工具。

4. 逆向工程师

- 1、热爱底层工作，对逆向工程有强烈兴趣；
 - 2、熟悉 x86/x64 系列汇编语言、C/C++语言，能熟练读懂汇编代码；具备编程能力；
 - 3、了解 Windows PE 结构；
 - 4、熟练使用 IDA、OD、WINDBG 等调试工具；
 - 5、学习能力强，富有团队精神，有责任感与进取心。
- 能独立编写漏洞利用程序 shellcode、exploit 者优先。

5. 各类安全培训讲师

蓝盾培训学院招聘各类信息安全技术培训讲师，目前需要以下 7 个方向的讲师：

- 1、渗透测试
- 2、电脑取证
- 3、逆向工程
- 4、无线安全
- 5、硬件安全
- 6、漏洞挖掘
- 7、物联网安全

PS: 如果你有在 WooYun 平台提交过安全问题请在简历里写上你的 WooYun 相关信息，企业可能会优先考虑

如 <http://www.wooyun.org/whitehats/>某某某

<http://www.wooyun.org/teams/NEURON>