

Kali Linux NetHunter

基础教程

(内部资料 v1.0)



大学霸

www.daxueba.net

前言

Kali Linux NetHunter 是一款基于 Android 设备构建的渗透测试平台。它包括一些特殊和独特的功能。NetHunter 支持无线 802.11 注入、一键 MANA AP 搭建、HID 键盘（类 Teensy 攻击）以及 BadUSB MITM 攻击测试等。

对于实施渗透测试的用户，如果到那都背上一台电脑或笔记本有点不太方便，而且还容易被人发现。但是，如果使用 NetHunter 的话，则只需要一部 Android 手机即可。目前，Android 手机相当普及，用户只需要将系统刷为 NetHunter 即可。在该系统中自带有大量的渗透测试工具，而且还默认安装了很多非常强大的第三方工具，如 cSploit、DriveDroid、Shodan 等。

为了满足用户的需要，笔者编写了《Kali Linux NetHunter 基础教程》教程。在该教程由浅至深的讲解 NetHunter 的使用，首先是环境的部署，然后是准备工作及配置，最后介绍了内置的和第三方渗透测试工具的使用方法。

1. 学习所需的系统和软件

- ☐ 一部已经 root 的 Android 手机
- ☐ 安装 Kali NetHunter 操作系统

2. 学习建议

大家学习之前，可以到百度网盘（xxxxxxxxxxxxxx）获取相关的资料和软件。如果大家在学习过程中遇到问题，也可以将问题发送到邮箱 xxxxxxxxxxxxxx。我们尽可能给大家解决。

目 录

第 1 章	搭建 Kali NetHunter 环境	1
1.1	NetHunter 概述	1
1.2	Kali NetHunter 支持的设备和 ROMs	1
1.3	刷机 Kali NetHunter	2
1.3.1	安装 Android SDK	2
1.3.2	下载相关资源	7
1.3.3	实施刷机	9
第 2 章	准备工作	17
2.1	apt-get 的使用	17
2.2	终端模拟器	18
2.3	启动/停止服务	19
2.4	查看监听的端口	20
2.5	接入外置无线网卡	21
2.5.1	OTG HUB 的功能	22
2.5.2	使用 OTG HUB	22
第 3 章	配置 Kali NetHunter	25
3.1	系统信息	25
3.2	NetHunter Chroot 管理	26
3.3	检查系统更新	28
3.4	服务管理	28
3.5	自定义命令	30
3.6	修改 MAC 地址	33
3.7	VNC 管理	35
第 4 章	实施渗透攻击	38
4.1	Nmap 扫描	38
4.2	HID 攻击	42
4.3	DuckHunter HID 攻击	44
4.4	BadUSB 中间人攻击	46
4.5	Wardriving 攻击	51
4.6	创建伪 AP	57
4.7	Wifite 工具	60
4.8	中间人攻击框架 (MITMF)	62
4.9	MSF 攻击载荷生成器	72
4.10	SearchSploit (搜索漏洞)	77
第 5 章	第三方软件	79
5.1	网络分析和渗透工具——cSploit	79

5.1.1	基本扫描	79
5.1.2	实施攻击	81
5.2	让 Android 设备变身启动盘——DriveDroid	84
5.2.1	配置 DriveDroid	84
5.2.2	创建 Linux 启动盘	89
5.2.3	创建 Windows 启动盘	92
5.3	无线路由器密钥破解器——Router Keygen	98
5.4	搜索引擎工具——Shodan	101
5.4.1	申请 Shodan 帐号	101
5.4.2	Shodan 专用过滤器	102
5.4.3	使用 Shodan 搜索默认密码	103
5.5	辅助工具——USB keyboard	106
5.5.1	配置黑客键盘	106
5.5.2	使用 USB keyboard	108
5.5.3	USB Keyboard 的 VNC 服务	110

第 1 章 搭建 Kali NetHunter 环境

NetHunter 是一个基于 Kali Linux 为 Nexus 设备构建的 Android 渗透测试平台，其中包括一些特殊和独特的功能。NetHunter 支持无线 802.11 注入，一键 MANA AP 搭建，HID 键盘（类 Teensy 攻击）以及 BadUSB MITM 攻击测试等。为了更好的使用 NetHunter 来实施渗透测试，本章将对 NetHunter 概念和环境搭建进行详细介绍。

1.1 NetHunter 概述

Kali NetHunter 是一款包含了稳健的渗透测试平台的叠加 ROM。叠加的内容里包含了一个定制的内核、一个 Kali Linux 的 Chroot 环境，和一个配套的可以用来更好的与各种安全工具与渗透攻击交互的 Android 软件。

除了 Kali Linux “填充”的渗透测试工具之外，NetHunter 还支持几种附加的种类，如 HID 攻击、BadUSB 攻击、Mana 攻击等。

1.2 Kali NetHunter 支持的设备和 ROMs

NetHunter 并不是支持在所有设备上都可以安装。所以，在刷入之前，首先要确定自己的手机支不支持。官方下载页面长时间没有更新，所以支持的型号是不全面的。想要了解自己的手机支不支持，最快捷的方法可以到 <http://forum.xda-developers.com/>（XDA 开发者论坛）网站搜索。在网站中搜索“nethunter+自己的机型”，如果找到就支持，并且可以在该页面找到 ROM 的下载地址。而且，内核所对应的 Android 版本号和基础 ROM 要一一对应。其中，NIGHTLY 内核的下载地址为 <https://idlekernel.com/nethunter/nightly/>。下面将以表格的形式列举出目前支持的机型，如表 1-1 所示。

表 1-1 NetHunter支持的设备和ROM

设备名	版本	注释
Nexus 4 (mako)	5.1.1 CM 13.0	
Nexus 5 (hammerhead)	5.1.1或6.0.1 CM 13.0	
Nexus 5x (bullhead)	6.0.1	
Nexus 6 (shamu)	5.1.1或6.0.1	
Nexus 6P (angler)	6.0.1	
Nexus 7 2012 (grouper)	5.1.1	
Nexus 7 2013 (flo)	5.1.1或6.0.1 CM 13.0	
Nexus 9 (flounder)	5.1.1或6.0.1	
Nexus 10 (manta)	5.1.1	
OnePlus One (oneplus1)	CM 12.1或13.0	Our preferred device

OnePlus Two (oneplus2)	CM 12.1或13.0	
OnePlus X (oneplusx)	CM 13.0	
LG G5(h830、h850)	6.0.1	
Galaxy Note 3 (hlte)	CM 12.1或13.0 TouchWiz 5.0	
Galaxy Note 7 (gracelte)	GraceUI 6.0.1	Best performing device Warning: Exynos models only!
Galaxy S5 (klte)	CM 12.1或13.0 TouchWiz 5.1或6.0	
Galaxy S7 (herolte)	TouchWiz 6.0.1	Warning: Exynos models only!
Galaxy S7 edge (hero2lte)	TouchWiz 6.0.1	Warning: Exynos models only!
SHIELD tablet (shieldtablet)	6.0.1	
SHIELD tablet K1	CM 13.0	

以上列举了支持的所有设备和 ROMs，在该教程中将选择 OenPlus One 设备来刷入 Kali NetHunter。

1.3 刷机 Kali NetHunter

通过前面的介绍，用户对 NetHunter 应该有了清晰的认识。接下来，就可以开始着手将设备重新刷机为 Kali NetHunter。在刷 Kali NetHunter 之前，也需要做一些准备工作，如安装 Android SDK、下载相关的包等。本节将介绍整个刷机的过程。

1.3.1 安装 Android SDK

SDK (software development kit) 软件开发工具包。被软件开发工程师用于为特定的软件包、软件框架、硬件平台、操作系统等见了应用软件的开发工具的集合。在后面刷机时将需要使用 fastboot 工具，而且包括在 SDK 中。但是，fastboot 默认没有安装在系统中，需要用户手动安装。所以，这里将通过安装 Android SDK 的方式来安装 fastboot，而且会自动安装对应的驱动。下面将介绍安装 SDK 的方法。

【实例 1-1】安装 Android SDK。具体操作步骤如下所示：

(1) 下载 Android SDK。其下载地址是 <https://developer.android.com/studio/index.html#downloads>。在浏览器中打开该地址，将显示如图 1.1 所示的界面。

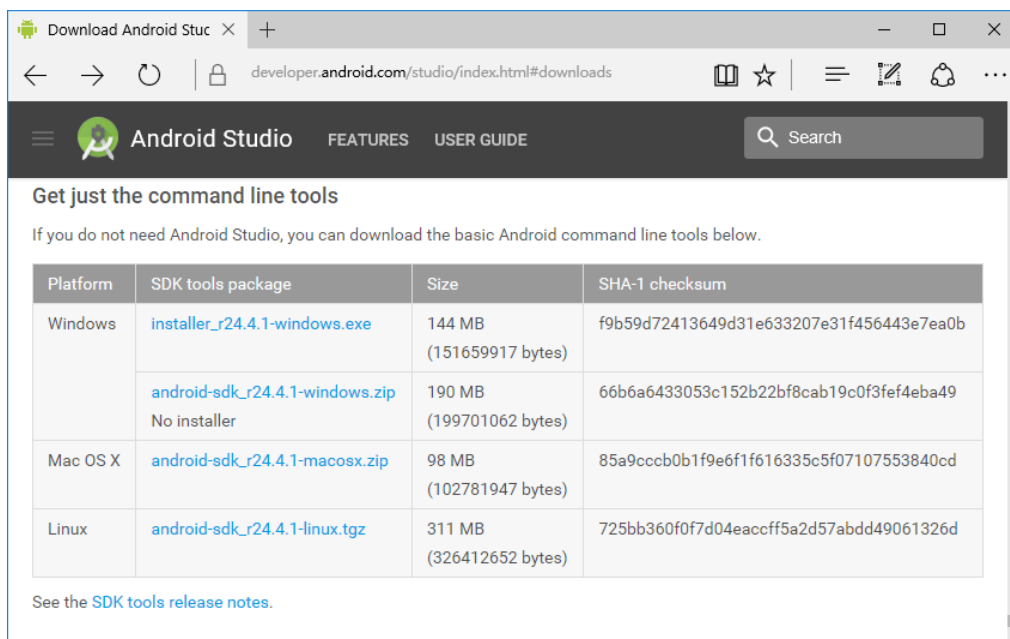


图 1.1 下载 Android SDK

(2) 在该界面可以看到，Android 的所有相关产品。本教程中只需要 Android SDK，而不需要其它开发工具，如 Eclipse。所以，这里选择 Get just the command line tools 下面的软件包。从该界面可以看到，这里提供有 Windows、Mac OS X 和 Linux 三种平台的软件包，而且可以看到 Windows 平台中提供的.zip 包无需安装就可以直接使用。所以，本例中将选择下载 Windows 平台的.zip 包。单击软件包名后，将显示如图 1.2 所示的界面。

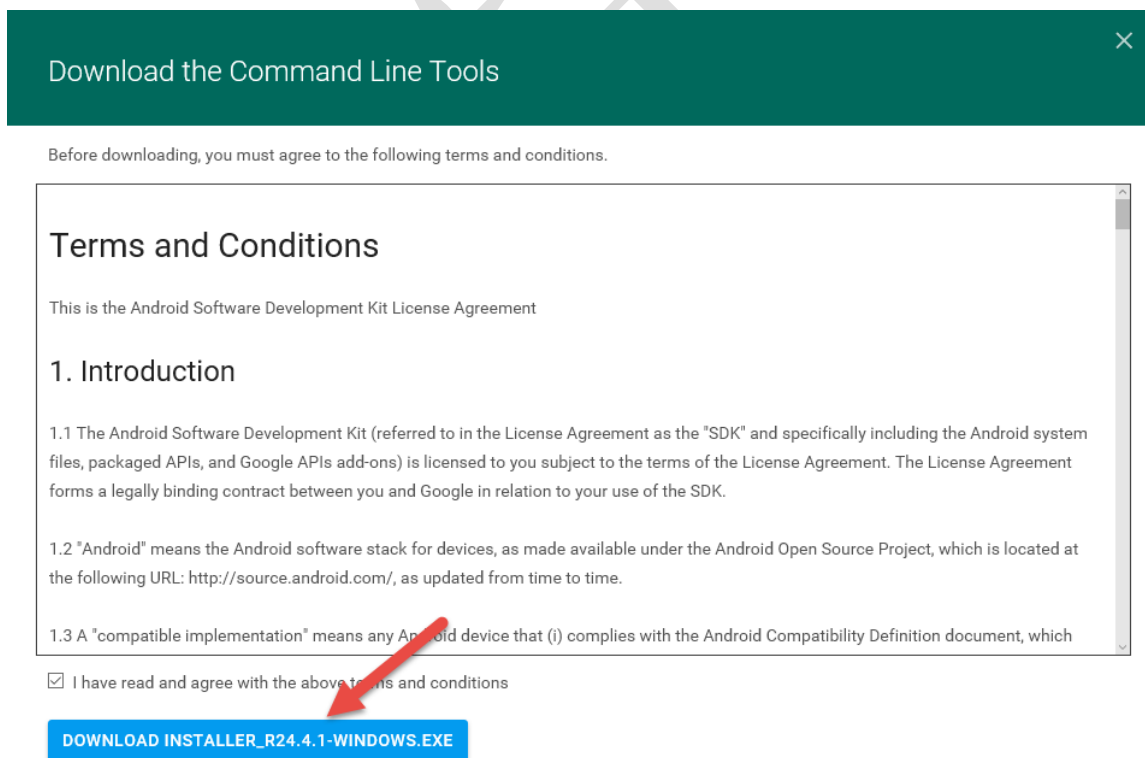


图 1.2 下载命令行工具

提示：用户也可以通过右键单击，复制包的下载地址。然后，使用迅雷进行下载。

(3) 该界面显示了下载软件包的一些条件。此时，勾选 I have read and agree with the above terms and conditions 前面的复选框。然后，单击 **DOWNLOAD ANDROID-SDK_R24.4.1-WINDOWS.ZIP**。下载完成后，文件名为 `android-sdk_r24.4.1-windows.zip`。接下来，使用 WinRAR 解压该软件包。这里将该软件包解压到桌面，解压完成后在桌面上将会创建一个名为 `android-sdk-windows` 的文件夹。打开该文件夹后，将显示如图 1.3 所示的界面。

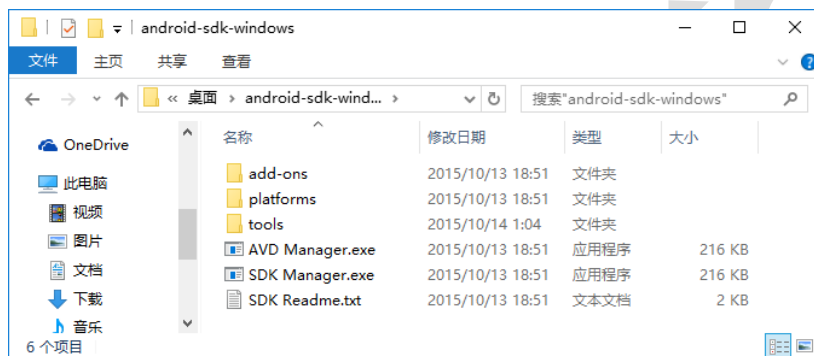


图 1.3 解压后的文件

(4) 从该界面可以看到有两个.exe 的可执行文件。其中，AVD Manager.exe 是 Android 虚拟设备管理器；SDK Manager.exe 是软件开发工具管理器。因为前面仅下载的是 SDK，所以接下来还需要安装四个组件。如下所示：

❑ Tools>Android SDK Tools, Android SDK platform-tools。

❑ Extras>Android Support Repository, Google USB Driver。

此时，运行 SDK Manager.exe 可执行文件，启动 SDK 管理器。成功启动后，显示界面如图 1.4 所示。

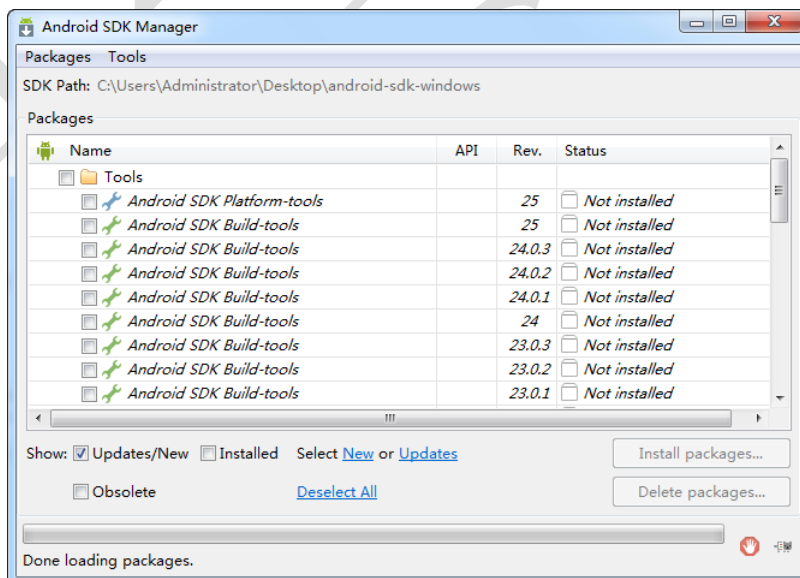


图 1.4 SDK 管理器

(5) 以上就是 Android SDK 管理器界面。在该界面可以更新、下载、安装及卸载 Android SDK 管理的攻击。接下来，在该界面选择需要安装的四组件，如图 1.5 所示。

(6) 从该界面右下角可以看到，将要安装 4 个包。此时，单击右下角的 Install 4 packages...按钮，将显示如图 1.6 所示的界面。

(7) 该界面显示了选择将要安装的包和一些许可协议。此时，单击 Accept License 单选按钮，并单击 Install 按钮将开始安装选择的包，如图 1.7 所示。

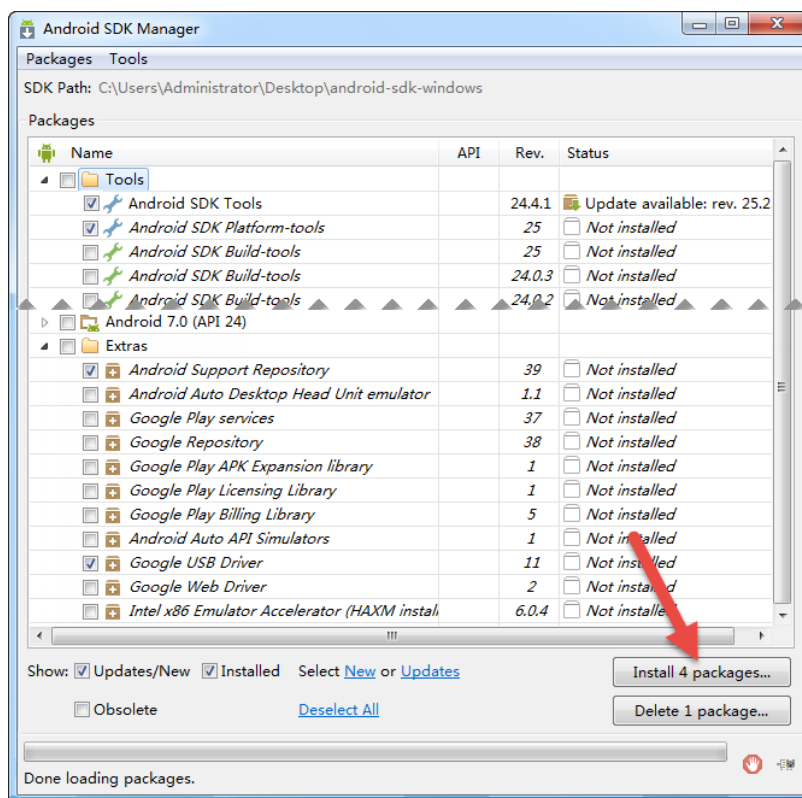


图 1.5 选择安装的组件

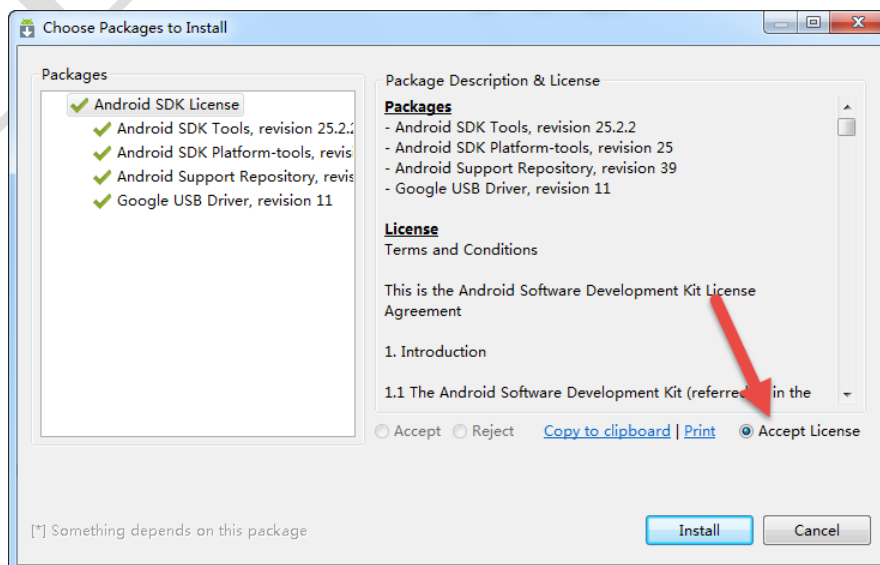


图 1.6 准备安装的包

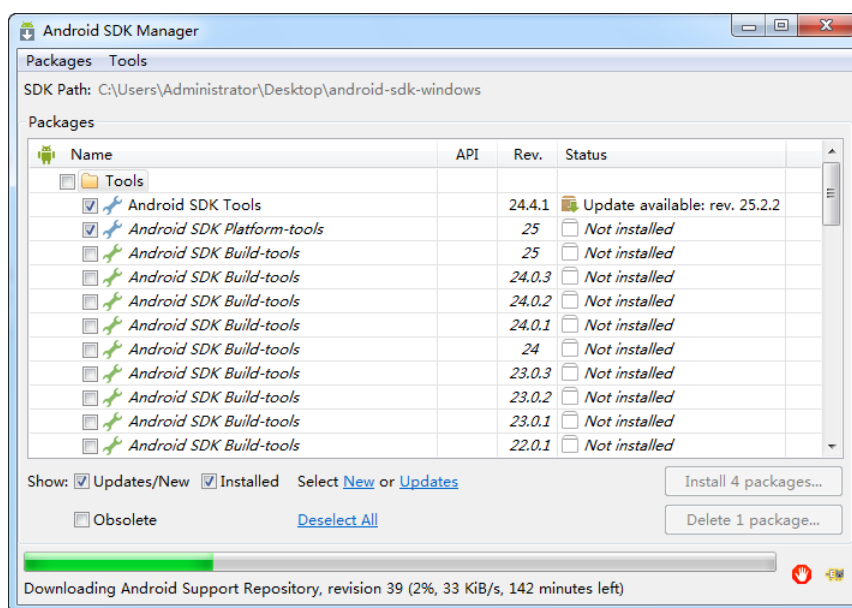


图 1.7 正在安装软件包

注意：如果以上安装包非常慢时，可能会影响用户的其它操作。所以，这里将介绍一种方法来加快它的速度。在 Android SDK Manager 的菜单栏中依次选择 Tools|Options...命令，如图 1.8 所示。单击 Options...命令后，将显示如图 1.9 所示的界面。

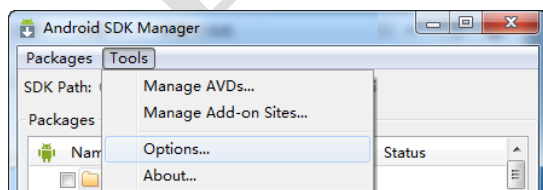


图 1.8 菜单栏

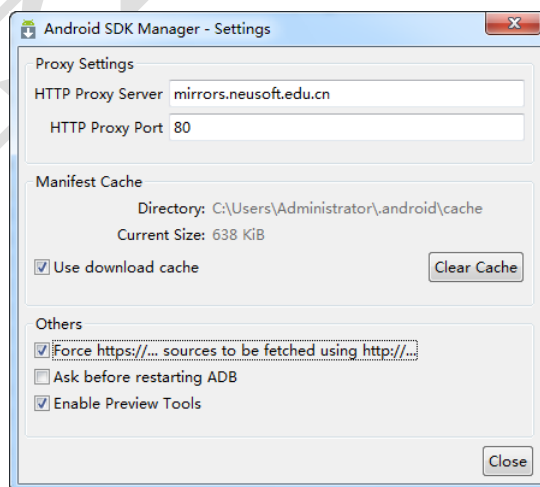


图 1.9 设置代理

在该界面设置一个代理服务器，具体配置如下所示：

- ☐ HTTP Proxy Server: 输入代理服务器的地址 mirrors.neusoft.edu.cn;
- ☐ HTTP Proxy Port: 设置代理端口号为 80;
- ☐ 勾选 Force https://...sources to be fetched using http://...前面的复选框;

(8) 安装完成后，进入 android-sdk-windows 目录中，将看到有一个名称为 platform-tools 的新文件夹，如图 1.10 所示。

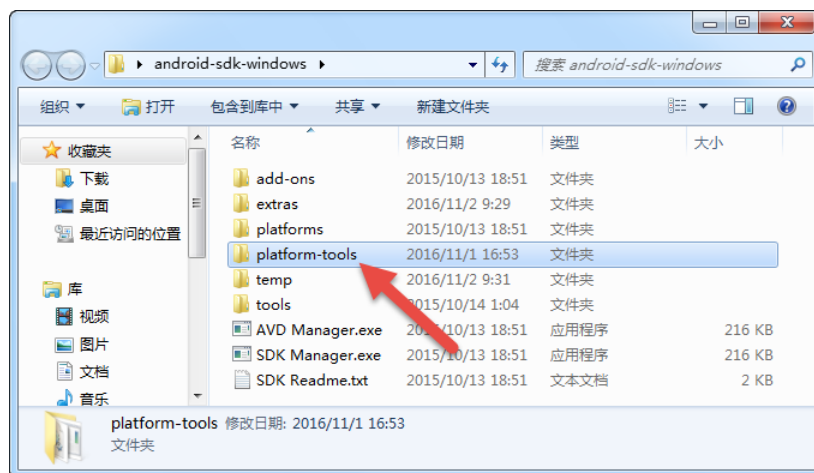


图 1.10 新创建的文件夹

(9) 为了确定 SDK 是否确实正常的工作了，这里使用 `adb` 命令检查下。打开 Windows 的命令提示符窗口，输入以下命令：

```
cd Desktop\android-sdk-windows\platform-tools
adb version
```

执行以上命令后，显示效果如图 1.11 所示。

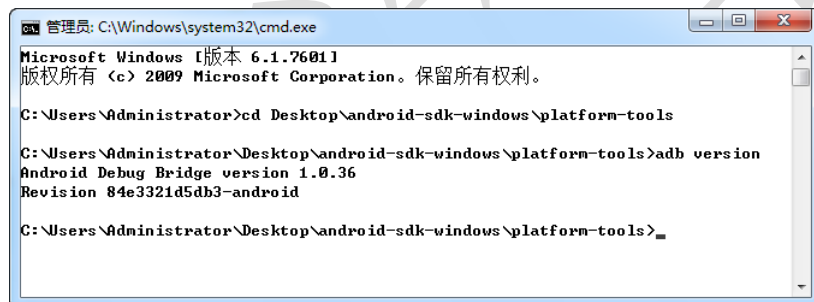


图 1.11 运行效果

(10) 从输出的信息中，可以看到成功显示了 ADB 的版本为 1.0.36。由此可以说明，SDK 工具正常运行了。

1.3.2 下载相关资源

当用户将刷机工具准备完后，则需要下载 ROM 包。ROM 是 ROM image（只读内存镜像）的简称，常用于手机定制系统。一般手机刷机的过程，就是将只读内存镜像（ROM image）写入只读内存（ROM）的过程。常见的 ROM image 有 img、zip 等格式。img 通常用 fastboot 程序通过数据线刷入（线刷），后者通常用 recovery 模式从 SD 刷入（卡刷），故 img 镜像也被称为线刷包，zip 镜像也称为卡刷包。如果将手机刷机为 Kali netHunter，则需要提前将需要的包下载好。所以，这里将介绍需要用到的 ROM 包。

- ❑ TWRP——第三方 Recovery: twrp-3.0.2-0-bacon.img。其中，下载地址为 <https://dl.twrp.me/bacon/>。
- ❑ SuperSU——root 软件：BETA-SuperSU-v2.60-20151205163135.zip。其中，下载地址为 <https://download.chainfire.eu/745/SuperSU/BETA-SuperSU-v2.60-20151205163135.zip>。
- ❑ CM 13.0 —— Kali NetHunter 基于的第三方 Android 操作系统：cm-13.0-20161031-NIGHTLY-bacon-recovery.img。其中，下载地址为

<https://download.cyanogenmod.org/?device=bacon&type=>。

- ❑ Kali NetHunter Kernel — — Kali NetHunter 内核：
kernel-nethunter-oneplus1-marshmallow-3.15.2-20160922-0014.zip。其中，下载地址为
<https://build.nethunter.com/nightly>（注意：该网站经常更新，选个合适的版本下载即可）。
- ❑ Kali NetHunter — — Kali Nethunter ROM 包：
nethunter-generic-armhf-kalifs-full-rolling-3.15.2-20160922-0014.zip。其中，下载地址为
<https://build.nethunter.com/nightly>（注意：该网站经常更新，选个合适的版本下载即可）。

当以上所有资源下载完成后，将这些包都拷贝到 Desktop/android-sdk-windows/platform-tools 文件夹下面。这里为了方便记忆，将 Recovery 包重命名为 recovery.img，SuperSu 重命名为 root.zip。当需要某个包时，用户可以使用“adb push 软件包 目标”命令将需要到包上传到手机的根目录中（/sdcard）。例如，上传 CM 13.0 ROM 包到手机的/sdcard 目录中。打开 Windows 系统的命令行提示符窗口，然后执行如下命令：

```
cd Desktop\android-sdk-windows\platform-tools
adb push cm-13.0-20160928-NIGHTLY-bacon.zip /sdcard
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
[100%] /sdcard/cm-13.0-20160928-NIGHTLY-bacon.zip
```

从输出的信息中，可以看到成功上传了 CM 包。接下来，用户用同样的方式，将其它包也上传到手机的根目录。如下所示：

```
adb push root.zip /sdcard #上传 Root 包
adb push kernel-nethunter-oneplus1-marshmallow-3.15.2-20160922-0014.zip /sdcard #上传 Nethunter 内核
adb push nethunter-generic-armhf-kalifs-full-rolling-3.15.2-20160922-0014.zip /sdcard #上传 Nethunter
```

将以上 ROM 上传成功后，即可开始刷机了。

以上提到获取 Kali NetHunter 包的第三方网站会经常更新，所以使用最新版可以马上体验到新的功能。但是，就太稳定。Kali 官网也提供有稳定版，只是已经很久没更新了，所以没有新版本中的功能多。为了方便用户的使用，这里也介绍下 Kali NetHunter 官网的下载地址。如下所示：

<https://www.offensive-security.com/kali-linux-nethunter-download/>

在浏览器中成功访问以上地址后，将显示如图 1.12 所示的界面。

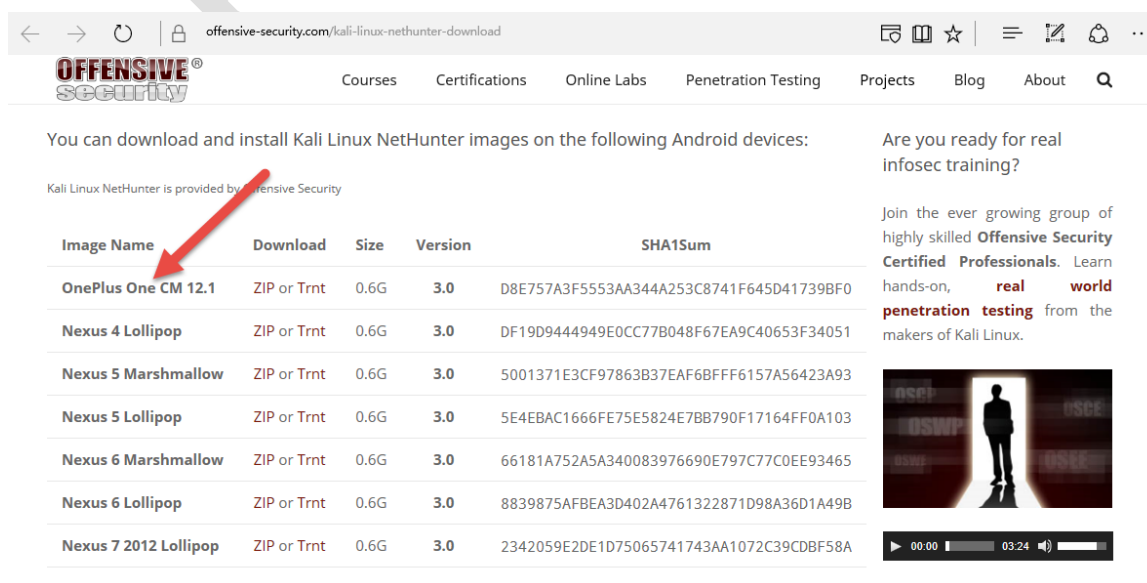


图 1.12 Kali NetHunter 的官方下载地址

从该界面可以看到提供了所有支持设备的 ROM 包，版本为 3.0。本教程使用的设备是 OnePlus One，所有选择下载 OnePlus One 对应的 ROM 包。而且，可以看到，该设备支持的 CM 系统为 12.1。所以，如果要安装 Kali NetHunter 的稳定版，则需要安装 CM 12.1 系统。下载成功后，这两个软件包名分别为 nethunter-oneplus1-lollipop-3.0.zip 和 cm-12.1-20151117-SNAPSHOT-YOG7DAO1K6-bacon.zip。

1.3.3 实施刷机

当用户将前面的工作都准备完成后，即可开始刷机。其中，整个刷机过程分为三个步骤，分别是解锁 Bootloader、刷入第三方 Recovery 和实施刷机。为了使用户能体验到所有的功能，本教程将使用最新版来搭建 Kali NetHunter 环境。下面将详细的介绍整个刷机过程。

1. 解锁 Bootloader

在嵌入式操作系统中，Bootloader 是在操作系统内核运行之前运行。可以初始化硬件设备、建立内存空间映射图，从而将系统的软硬件环境带到一个合适状态，以便最终调用操作系统内核准备好正确的环境。在嵌入式系统中，通常并没有像 BIOS 那样的固件程序，因此整个系统的加载启动任务就完全由 Bootloader 来完成。

由此可以看出，Bootloader 很重要。如果 Bootloader 不能正常加载，手机就是砖头一个，无法正常启动和使用。这也就是这里为什么要解锁 Bootloader 才能刷入第三方 ROM。如果不破解 Bootloader，就无法初始化手机硬件，手机也就无法使用。下面将介绍解锁 Bootloader 的方法。

【实例 1-2】解锁 Bootloader。具体操作步骤如下所示：

（1）进入 fastboot 模式。首先将手机关机。然后，按下“音量上键+电源键”即可进入 fastboot 模式。成功进入 fastboot 模式后，手机上将会显示“fastboot”文字。

（2）将手机插入到 PC 机中，然后打开 Windows 的命令提示符窗口，并输入以下命令：

```
cd Desktop\android-sdk-windows\platform-tools
fastboot devices
1d568ee2      fastboot
```

从输出的结果中，可以看到显示出了当前连接的设备。

（3）此时，解锁 Bootloader。执行命令如下所示：

```
fastboot oem unlock
...
OKAY [ 0.016s]
finished. total time: 0.016s
```



从输出的信息中，可以看到提示 OKAY，则表示解锁成功。

（4）重启手机。执行命令如下所示：

```
fastboot reboot
rebooting...
finished. total time: 0.016s
```

从输出的信息中，可以看到手机正在重启。当手机成功重启后，将进入到系统中。接下来，还需要调整手机的一些设置。

（5）开启手机的 USB 调试。在手机中依次选择“设置”|“关于手机”|“连续按 7 次版本号”，将启用开发者选项。然后，返回到设置界面，选择“开发者选项”命令，将打开如图 1.13 所示的界面。

（6）在该界面选择 Android 调试选项，单击右侧的  按钮启用 USB 调试。单击  按钮后，将弹出一个提示对话框，如图 1.14 所示。

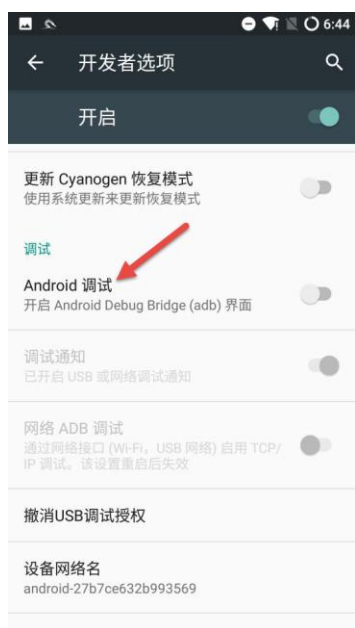


图 1.13 开发者选项

是否允许USB调试?

USB调试仅适用于开发工作。该功能可用于在您的计算机和设备之间复制数据、在您的设备上安装应用而不发送通知以及读取日志数据。

取消 确定

图 1.14 是否允许 USB 调试

(7) 该对话框中显示了 USB 调试的功能，是否确定要开启 USB 调试。这里单击“确定”按钮，开启 USB 调试后，显示界面如图 1.15 所示。

(8) 禁用 Cyanogen 恢复模式。在手机中依次选择“设置”|“开发者选项”命令，禁用“更新 Cyanogen 恢复模式”选项，如图 1.6 所示。

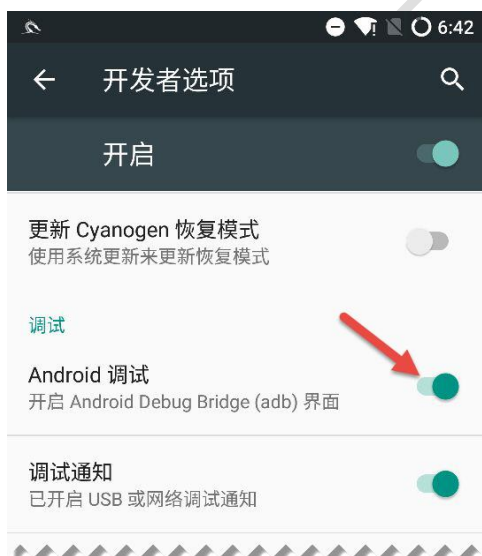


图 1.15 禁用更新 Cyanogen 恢复模式



图 1.16 启用 USB 调试

2. 刷入第三方 Recovery（即 TWRP）

TWRP（TeamWin Recovery Project）是一款 XDA 大神开发的一款全触屏操作的第三方 Recovery。支持滑动确认等好玩实用的功能。TWRP 和 CWM 一样，但是 TWRP 更强大。它最大的特点就是全触控操作，而且操作便捷。例如，用 CWM 双清或者三清甚至是四清，是一件很麻烦的事情。因为需要用户一个一个点，非常不方便，这时 TWRP 方便的地方就体现出来了。TWRP 可以勾选多个选项，一次性完成工作，不需要一个个清。所以，下面将介绍刷入 TWRP 的方法。

【实例 1-3】刷入第三方 Recovery（TWRP）。具体操作步骤如下所示：

（1）同样将手机关机，然后使用“音量上键+电源键”进入 fastboot 模式。

（2）将 Recovery 文件烧写到手机中。在前面已经将下载的 Recovery 文件重命名为 recovery.img。并且复制到 Desktop/android-sdk-windows/platform-tools 目录中。所以，这里可以开始烧该文件了。打开 Windows 下的命令提示符窗口，执行以下命令：

```
cd Desktop/android-sdk-windows/platform-tools
fastboot flash recovery recovery.img
```

当烧写完成后，手动的按下电源直到手机关机，然后拔下手机。接下来，长按“音量下键+电源键”，即可进入新刷入的 Recovery（TWRP）模式。

3. 开始刷机







现在用户的手机中有一个解锁 Bootloader 和一个 Recovery。接下来，即可进行刷机。具体操作步骤如下所示：

（1）长按“音量下键+电源键”，进入 Recovery 模式。成功进入 Recovery 模式后，将显示如图 1.17 所示的界面。

（2）从该界面可以看到有八个选项可以进行操作。其中，每个选项的作用如下所示：

- ☐ Install: 用来刷入 ROM 包。
- ☐ Wipe: 进行双清、三清、四清操作的。简单的说，就是清理手机中的数据。
- ☐ Backup: 用来备份数据。
- ☐ Restore: 用来恢复数据。
- ☐ Mouter: 用来挂载某系统文件。
- ☐ Settings: 设置 TWRP 操作。
- ☐ Advanced: 高级选项。
- ☐ Reboot: 重新启动系统。

TWRP 默认使用的语言是英文，为了使用户更好的使用该工具，可以修改用户为中文。在主界面单击 Settings 按钮，将显示设置选项界面，如图 1.18 所示。

（3）从该界面可以看到有五个设置选项卡，分别是 （通用设置）、（时间设置）、（亮度设置）、（振动设置）和 （语言设置）。该界面选择了 （语言设置）选项卡，从该界面可以看到默认使用的语言是 English。此时，选择 Chinese（Simplified）选项，然后单击 Set Language 按钮使修改生效。设置完成后，返回到主界面，将显示如图 1.19 所示的界面。

（4）从该界面可以看到 TWRP 的语言已成功设置为中文。接下来，进行四清操作。在该界面单击“清除”按钮，将显示如图 1.20 所示的界面。

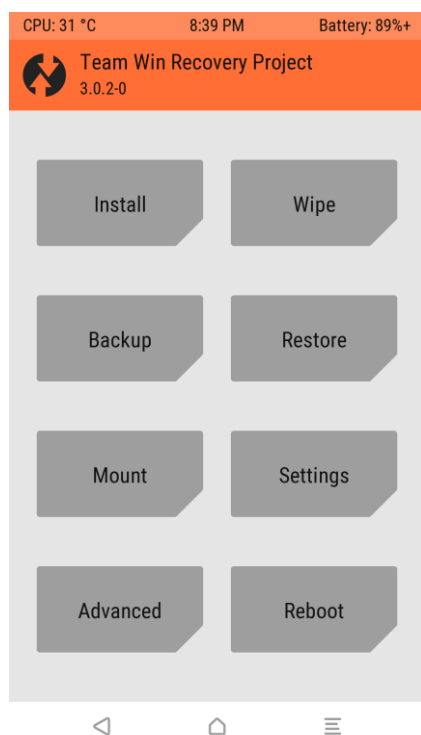


图 1.17 Recovery 模式

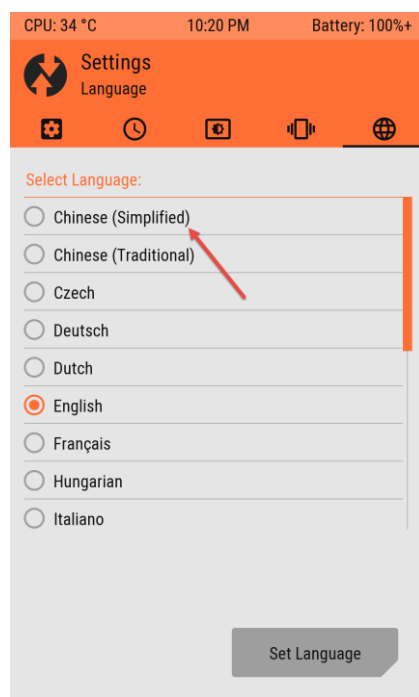


图 1.18 设置界面



图 1.19 成功设置为中文



图 1.20 清除 (Wipe) 界面

(5) 从该界面可以看到有两个选项，分别是“高级清除菜单”和“格式化 Data 分区”。其中，“高级清除菜单”是用来选择进行清理操作的；“格式化 Data 分区”是用来格式化数据的。这里可以进行格式化数据，也可以不进行格式化。如果手机中有重要文件的话，切记不要单击“格式化 Data 分区”

按钮。因为，它会将手机的内存卡一起格式化掉。这里单击“高级清除菜单”按钮，将显示如图 1.21 所示的界面。

（6）在该界面选择要清除的分区。这里进行四清操作。在选择清除分区之前，这里分别先介绍下二清、三清和四清的区别。如下所示：

- ❑ 四清：最完整的清除，将会把系统、缓存、用户数据等全部清除。其中，四清选项为 Dalvik / ART Cache、System、Data 和 Cache。
- ❑ 三清：比四清少了个格式化系统。如果用户不确定下载的 ROM 包是否真的可用时，建议选择三清。万一下载的 ROM 无法刷入，不至于开不了机。当然如果用户的手机里有一个绝对可以刷入的包做保底的话，忽略三清用四清或者两清。其中，三清选项为 Dalvik / ART Cache、Data 和 Cache。
- ❑ 二清：又称双清。这里的双清适用于同个 ROM 直接的升级，刷内核或者补丁包。例如，从 C-RoM V6.2 升级到 V6.3 时，用双清可以清理缓存，但是又不至于把用户数据和应用程序给 Wipe 了。这样比不双清直接刷要干净一点。其中，双清选项为 Dalvik / ART Cache 和 Cache。当然在这一步也可以把 System 给选上，更干净。

这里进行四清操作，所以具体勾选如图 1.22 所示。



图 1.21 选择 Wipe 操作



图 1.22 进行四清操作

（7）当勾选好后，滑动底下“滑动确认清除”滑块将开始对选择的分区进行清除。清除完成后，将显示如图 1.23 所示的界面。

（8）从该界面可以看到，提示清除成功。接下来，依次刷入下载的 ROM 包。首先要确定所有包都已经拷贝在手机中，如果没有的话，使用 `adb push` 命令将文件上传到手机上。返回到 Recovery 的主界面，点击 `INSTALL` 按钮，将显示如图 1.24 所示的界面。



图 1.23 四清操作成功

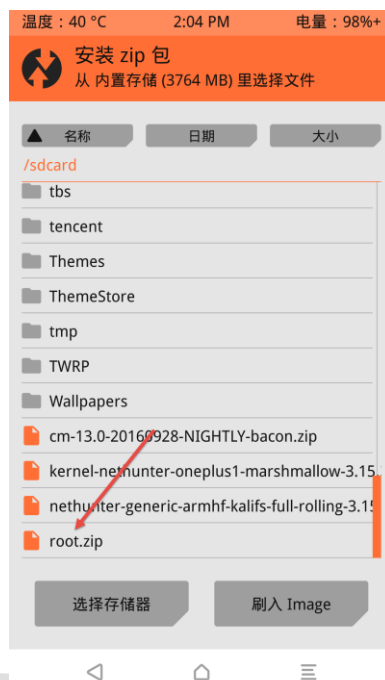


图 1.24 选择刷入的 ROM 包

(9) 该界面显示了根目录 (/sdcard) 下的所有文件。从该界面可以看到，需要刷入的 ROM 包都已经保存在该目录中。例如，先刷入 SuperSu 包。在该界面选择 root.zip 包，将显示如图 1.25 所示的信息。

(10) 该界面显示了将要刷入的 ROM 包信息。此时，滑动底下的“滑动确认刷入”滑块将开始刷机。刷入成功后，将显示如图 1.26 所示的界面。



图 1.25 ROM 包信息

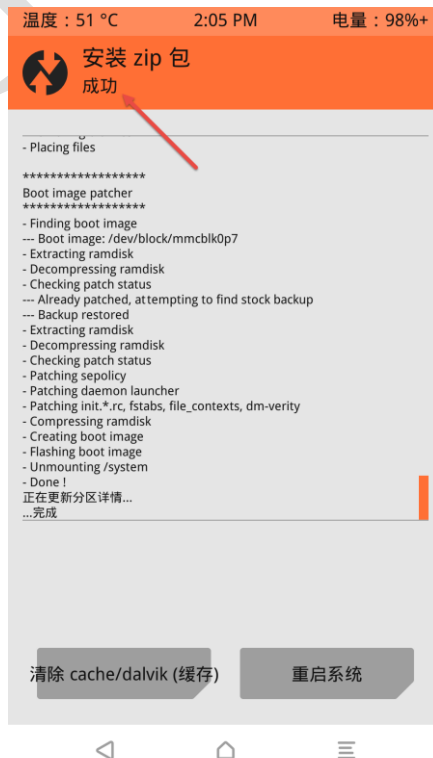


图 1.26 ROM 包刷入成功

（11）从该界面可以看到，提示 ROM 包刷入成功。接下来，返回到主界面，单击“安装”按钮，刷入 CM 系统包。刷入成功后，不要着急开机。首先，单击“清除 cache/dalvik（缓存）”按钮，然后再重新启动系统。单击“清除 cache/dalvik（缓存）”按钮后，将显示如图 1.27 所示的界面。

（12）该界面提示是否确定要清除 Cache 和 Dalvik。此时，滑动底下的“滑动确认清除”滑块，将开始清除缓存。完成后，将显示如图 1.28 所示的界面。



图 1.27 是否确认清除缓存



图 1.28 清除缓存成功

从该界面可以看到清除缓存成功。接下来，单击“重启系统”按钮。

（13）重新启动手机后，则需要一些基本设置，如语言、网络、时间等。设置非常简单，根据提示一步步设置完成后，即可进入 CM13.0 系统。然后，设置 CM13.0 系统允许 USB 调试模式，并关机再次进入 Recovery 模式。

（14）接下来，再次长按“音量下键+电源键”，重新进入 TWRP Recovery 模式。点击 INSTALL，刷入 Kali NetHunter 内核，即 kernel-nethunter-oneplus1-marshmallow-3.15.2-20160922-0014.zip 包。注意，在刷入前不要执行任何清除操作。

（15）返回 Recovery 的主界面，再次点击 INSTALL 按钮，刷入 Kali NetHunter，即 nethunter-generic-armhf-kalifs-full-rolling-3.15.2-20160922-0014.zip 包。注意，同样在刷入前不要执行任何清除操作。

（16）将以上两个 ROM 包都刷入系统后，则整个刷机过程就操作完成了。也就是说，已经成功刷入了 NetHunter。成功刷入 NetHunter 后，同样先执行默认清除（Wipe）操作，再重启系统。成功启动后，将进入 Kali NetHunter 系统，显示界面如图 1.29 所示。

（17）从该界面可以看到，成功进入了 Kali NetHunter 系统。此时，单击 Home 键，即可看到安装的所有程序，如图 1.30 所示。



图 1.29 Kali NetHunter 系统界面



图 1.30 所有程序

(18) 从该界面可以看到 NetHunter 程序，在该程序中有自带的渗透测试工具，如图 1.31 所示。而且 Kali 中还自带了一些第三方软件，如 cSploit、NetHunter VNC、Router Keygen、Shodan 等。

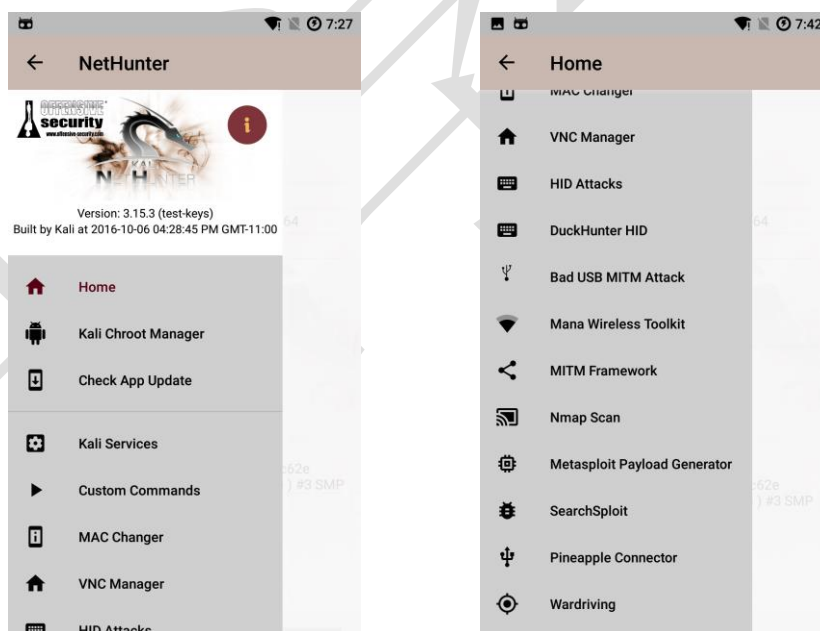


图 1.31 NetHunter 的列表

(19) 从该界面的列表中，可以看到 NetHunter 中的所有配置项和自带的渗透工具。如 HID Attacks、Bad USB MITM Attack、Mana Wireless Toolkit 等。这些所有的配置，在后面章节将会详细介绍。

提示：刷官方的版本和以上的方法类似，只是将 CM 13.0 改为 CM 12.1。重新启动系统后，直接刷入官方的 Kali NetHunter 包即可，无需刷入 Kali NetHunter 内核包。