**kali for android:让你的安卓设备跑起kali**

2013-09-27 14:59:06     [**我来说两句**](http://www.2cto.com/Article/201309/246638.html#comment_iframe)   来源：p0tt1.sniffer.pro

[收藏](javascript:;)    [[http://www.2cto.com/statics/images/dl.jpg](http://www.2cto.com/index.php?m=member&c=content&a=publish&modid=1&siteid=1)我要投稿](http://www.2cto.com/index.php?m=member&c=content&a=publish&modid=1&siteid=1)



**现在大家手上几乎都有安卓的设备了**

**如何让他霸气的跑起kali系统 作为渗透测试小钢炮呢？**

**分享下自己的经验~**

--------------------------猥琐的分割线---------------------

看看我们需要什么：

* 0x001 一个跑着安卓系统的设备，手机 平板 htpc 什么都行
* 但前提是 他已经获得了root权限（相信对大家来说不难，提权呗）系统是2.1以上的

0x002 又有至少5g的sdcard存储空间

0x003 有一个够快的无线网络 当然如果你有足够的耐心去等 当我没说

0x004 拥有一颗勇者之心 去应对从官网[下载](http://www.2cto.com/soft" \t "_blank)img文件这个漫长的过程（同0x003）

需要下载的软件

[linux deploy](https://play.google.com/store/apps/details?id=ru.meefik.linuxdeploy&hl=en) 这个是官方推荐的 不错的 而且傻瓜化了操作流程

vnc 连接器 这个你直接91手机助手搜索vnc 一大堆 用来使用GUI界面的kali

ssh连接器 这个360手机助手 搜索ssh 就行了 排行第一个的 用来使用命令行界面的 kali（推荐）

--------------------------猥琐的分割线---------------------

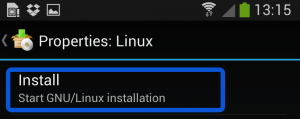
ok  正式开始~

把三个要安装的软件都装好 连上你的网络~

打开[linux deploy](https://play.google.com/store/apps/details?id=ru.meefik.linuxdeploy&hl=en" \o "\\" \t "_self)（就是那个小企鹅图标的） 按照下图配置好



然后呢 点击 install 按钮 如下图



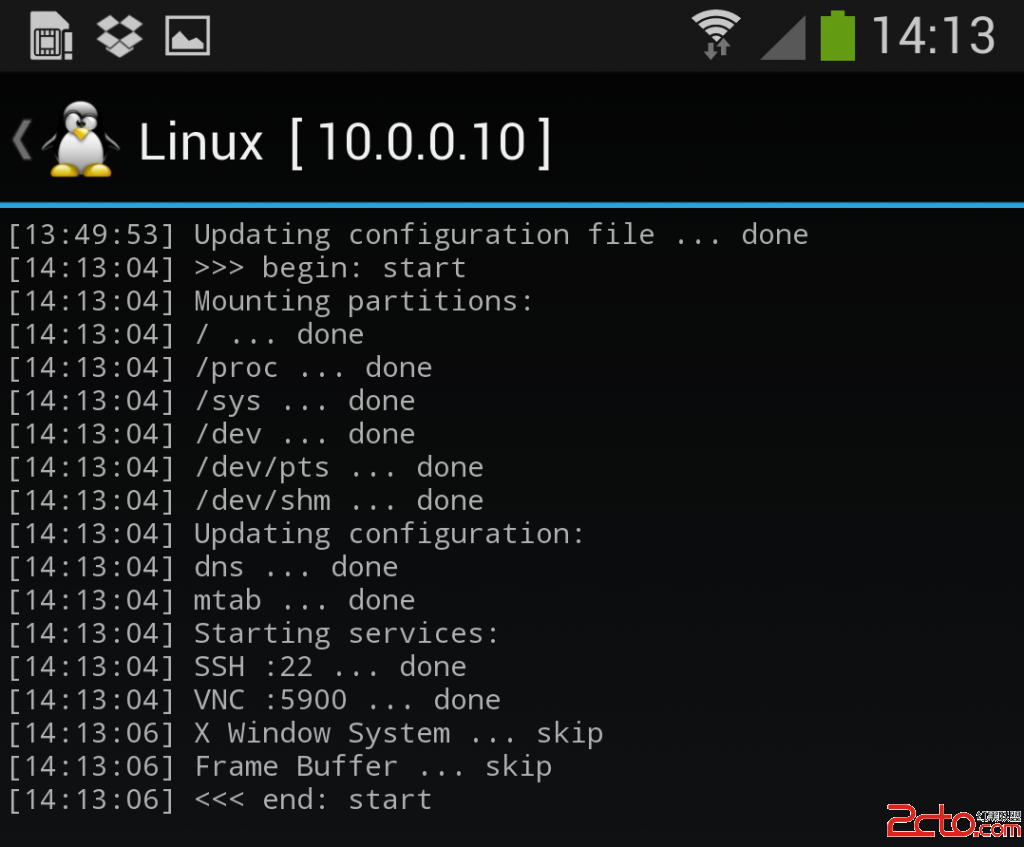
然后是漫长的等待 从kali的官网拖东西 速度27.8k~105k不等 反正我是这样  我挂了一下午 回来就完成了

记住等待~ 千万别让他断网 和 掉包 否则 重新 install~

等全部完成之后呢 我们点击右上角的start ！

记住 这里的 start 和 stop 就是挂载和卸载kali的镜像 就像虚拟光驱  跟安装 没关系 必须install完成后才有用

start以后呢 就会如下图



可以看到ssh 和 vnc 成功开启了！

现在我们可以用这两个连接器去连接了！下面告知下账号密码

vnc

ip:127.0.0.1 port:5900 pass:changeme

ssh

ip:127.0.0.1 port:22 user:android pass:changeme

这个时候你可以用vnc连接器链接下 看看我们可爱的kali界面 爽一下 漫长的等待值得了~

然后告诉你个不幸的消息 现在的kali只是个平台 没有pc上那么多功能 所以我们要接着安装

好在剩下的就太简单了

用ssh链接上 然后命令行输入命令

sudo su---------登陆root账户

apt-get install nmap---------我喜欢先安装我爱的nmap

apt-get install sqlmap-------然后是注入工具sqlmap

apt-get install met[asp](http://www.2cto.com/kf/web/asp/)loit---传说中的神器MSF用kali不就为了用它么？但是他比较大 安装时间有些长 所以我放在最后

apt-get update--------------这个不解释了吧~

apt-get upgrade-------------这个也不解释了吧~

apt-get remove iceweasel-l10n-zh-cn（安装中文版火狐）

好了，到这里 我平时爱用的就算装完了 剩下大家爱玩什么装什么吧~

操作和电脑的kali是一样的，如果你的设备是4核8核的 那我建议你

直接电脑ssh到你的安卓kali上 用它扫描和[渗透](http://vip.2cto.com/Article/61.html)把 为虾？

我不是理论大牛，我只能靠实践摸索 arm版的 至少现在这样安装的kali 扫描起来比windows下的namp sqlmap msf都快~

如果你的pc[系统](http://www.2cto.com/os/)就是kali 上面的话当我没说~

完成

折腾党伤不起

感谢和我一起折腾和把自己手机也折腾了的小伙伴

pois0n-装逼哥(三星S4)

Poe(三星S4)

还有苦逼的我(三星Note 10.1 & 三星notebook 1)

最后上几张图片 和我的小伙伴们欢乐一下~



