

前言

现在我们已经拥有了台可调用安卓硬件的完整的Kali Nethunter攻击机。那让我们开始干坏事吧！
(不是)

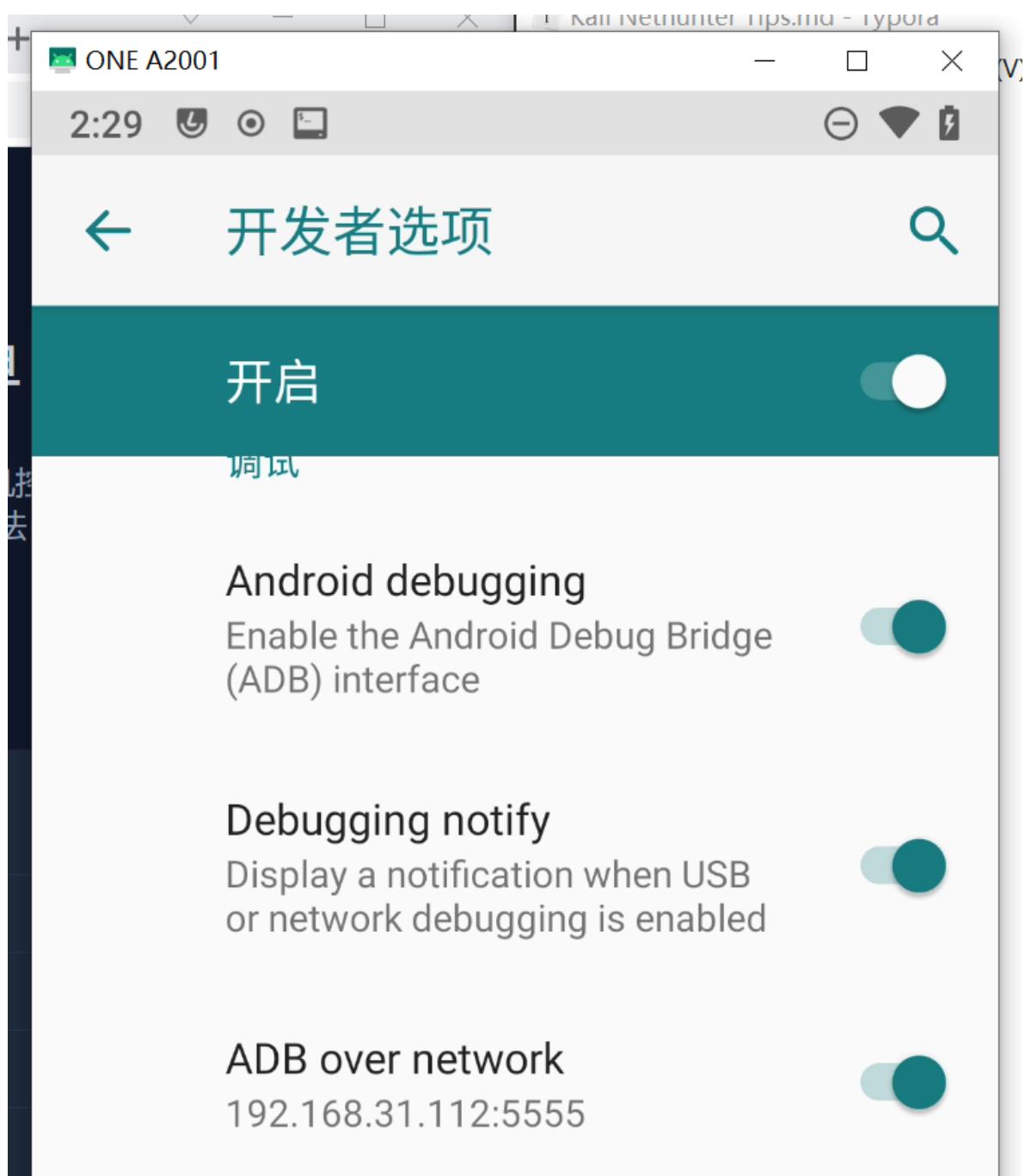
1.ADB模拟电脑终端

ADB指令大全详见：<https://quickref.cn/docs/adb.html>

补充资料：<https://cloud.tencent.com/developer/article/1621182>

与传统adb不同，以攻击为目的的adb桥接最好不要用到实体介质，故最好使用tcp连接adb的方式。

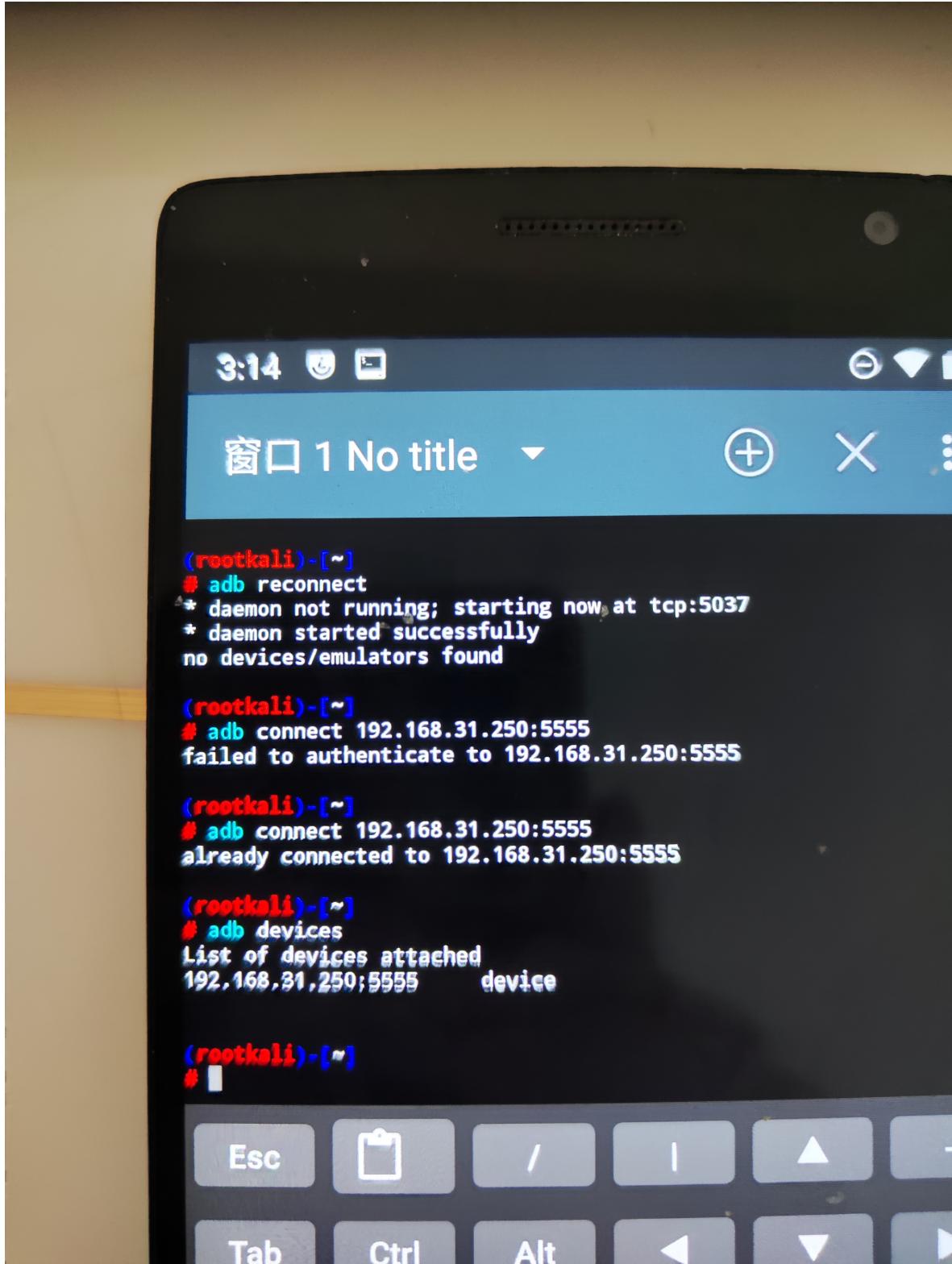
首先需要激活靶机adb调试中的tcp模式。对于旧版本的一加手机，在开发者选项中有开关可一键激活：



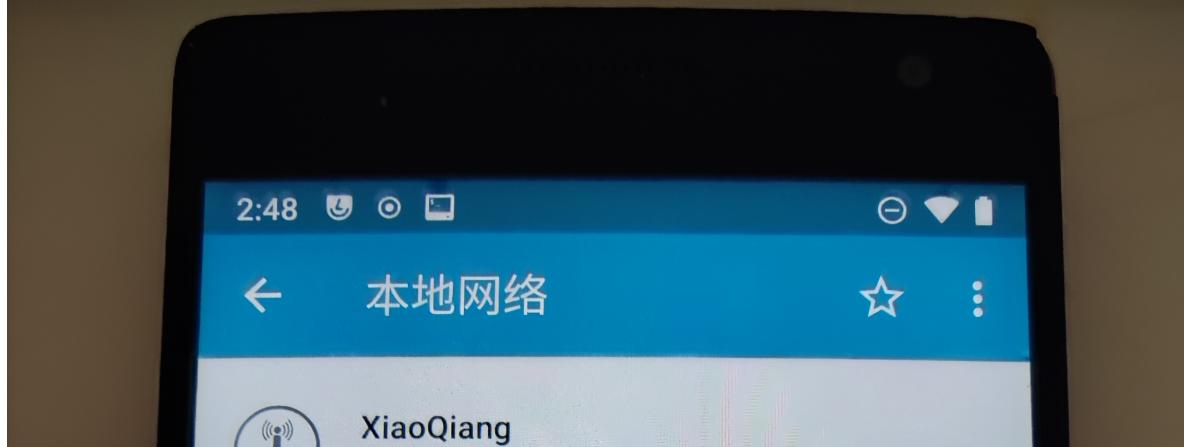
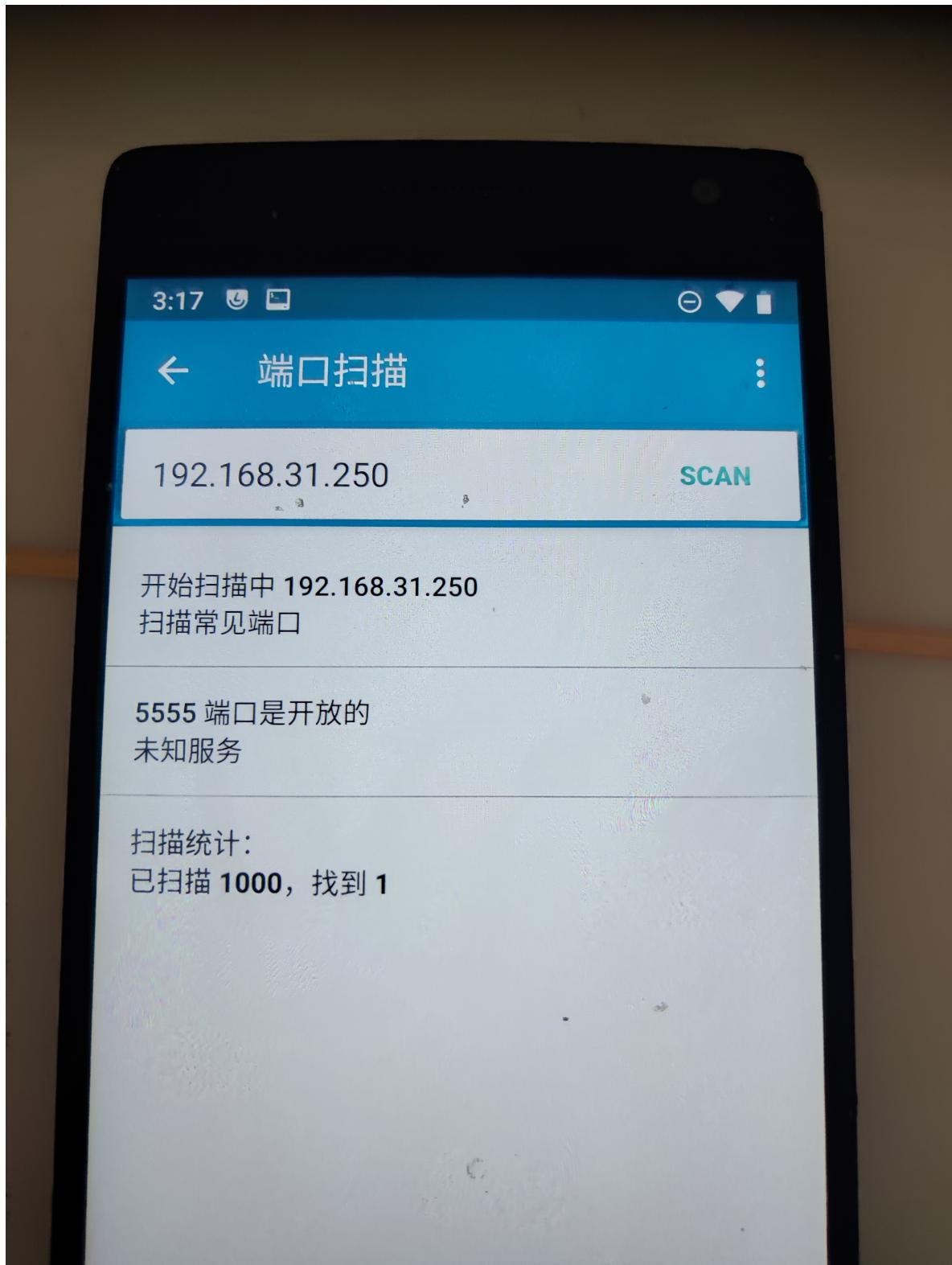
在ADB over network被激活之后，下方会有设备在局域网中的IP地址和adb服务端口号。默认为5555，即安卓默认监听端口。

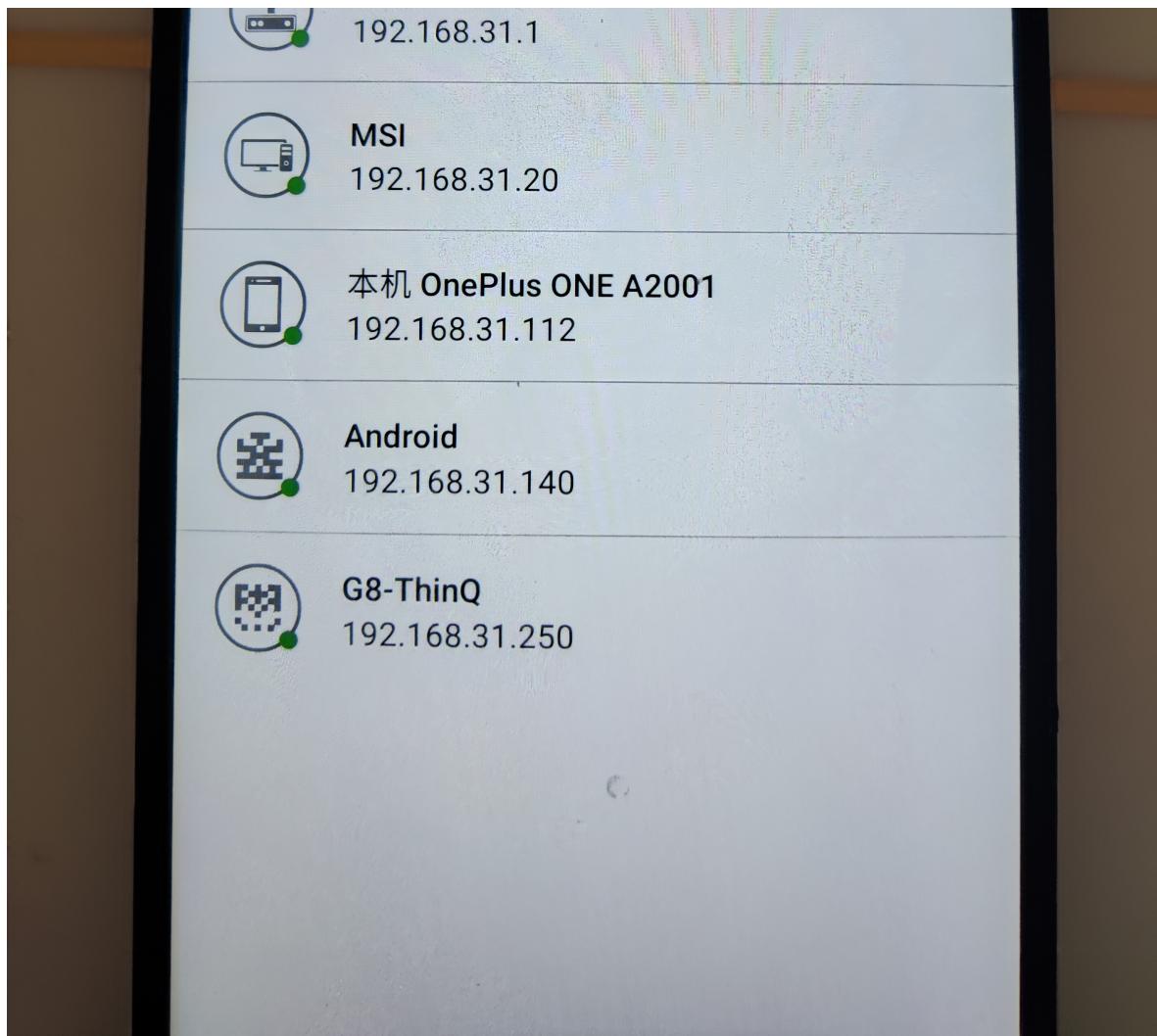
但绝大多数手机在低于安卓11的版本是没有开放的无线调试接口的，可以通过软件【ADB WIFI】实现（需要root权限）。

在kali终端中输入adb connect IP:端口号（一般默认为5555），第一次输入后会弹窗是否授予调试权限，点击确认后终端重复输入一次即可链接无限调试。adb devices指令若出现靶机ip地址则已经连接成功。



渗透时一般无法得知靶机的ip地址，可以通过软件【pingtools pro】进行ip地址扫描和端口扫描。





进入adb shell后即可提权对靶机系统进行操作：

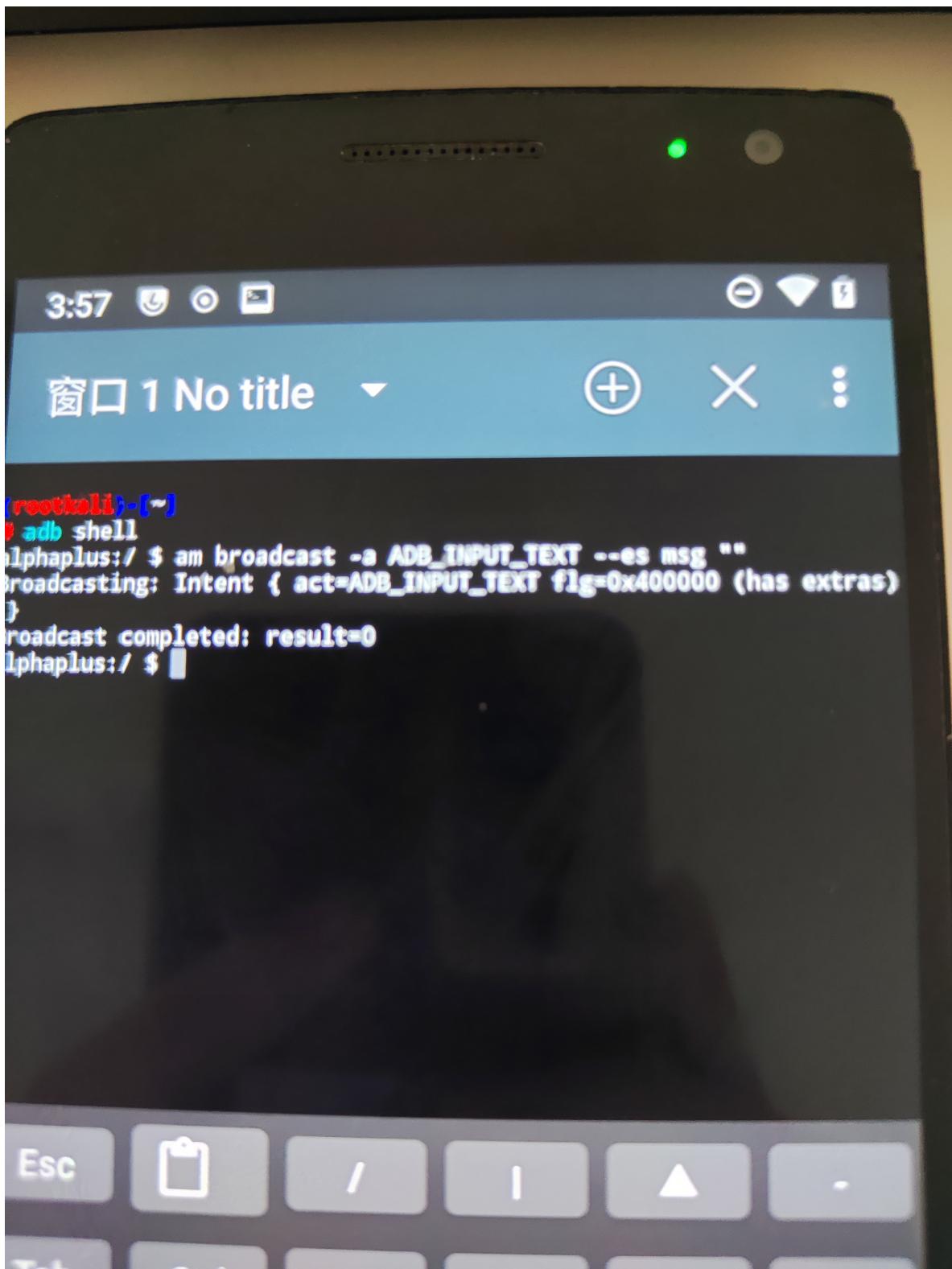
```
(rootkali)-[~]
# adb shell
alphaplus:/ $ ls
ls: ./veri: Permission denied
ls: ./cache: Permission denied
acct           init          postinstall
apex           init.environ.rc  proc
bin            init.mid.rc    product
bugreports     init.mid.service.rc sdcard
carrier         linkerconfig   second_stage_resources
config          lost+found    storage
d               metadata      sys
data            mnt          system
data_mirror     odm          system_ext
debug_ramdisk   odm_dlkm    vendor
dev             oem          vendor_dlkm
etc             persdata    vzw
1|alphaplus:/ $ pm list packages -f
package:/product/priv-app/ContentService/ContentService.apk=com.lge
.gallery.contentservice
package:/system/system_ext/priv-app/FontServer/FontServer.apk=com.h
y.system.fontserver
package:/system/system_ext/priv-app/LGStartupwizard/LGStartupwizard
```

ls: 显示根目录。

pm list packages -f 显示所有安装包包名及其绝对地址。

su:授予超级用户权限 (前提是已经获取root)

事实上adb shell可以用来做非常方便的自动化工作，不仅可以修改应用，文件；还可以模拟文本输入，点击，甚至是实体按键。



自动化文本输入。 (需要注意的是原生adb也有推送文本的功能，但不支持UTF-8，即中文输入)