

# Android模拟器root

## 实验概述

root是玩安卓手机用户非常熟悉的名词，对于很多安卓用户来说新机到手第一件事就是root也是再平常不过的了。即便是root之后手机的安全问题、保修问题需要担心，大家也依然热衷于root，这是为什么呢？为什么用户会有安卓手机一定要root的意识呢？本实验将介绍root的作用和危害以及如何对android模拟器进行root。

## 实验目的

1. 了解命令行启动模拟器的方法
2. 掌握模拟器获取root权限的流程
3. 熟练android模拟器终端基本命令
4. 了解root的作用是什么

## 实验原理

一般情况下，手机厂家和运营商在手机出厂时都会限制root权限，一方面是考虑到用户的使用水平有限，另外一方面是想通过root权限限制用户，让用户使用预装的应用程序。那么用户想要删除系统预装的各种应用程序，获取root权限就是第一步。手机预装软件拖慢手机运行速度，后台运行，洩漏资料，占用流量，消耗电量，甚至栽种木马，威胁安全，每一个恶意行为都是在挑战着用户的承受极限，强烈刺激用户获取root权限来删除它们。

没有root权限，会发现很多事情都干不成，比如说使用防火墙和过滤、备份工具，以及下载更高级应用。安卓系统每一次升级都会伴随着新的功能和体验，玩家们想要即时体验新系统，那就得刷机，而刷机的前提是需要获取root权限。

谷歌的 android系统管理员用户就叫做root，该帐户拥有整个系统至高无上的权利，它可以访问和修改你手机几乎所有的文件，只有root才具备最高级别的管理权限。我们root手机的过程也就是获得手机最高使用权限的过程。同时为了防止不良软件也取得root用户的权限，当我们在root的过程中，还会给系统装一个程序，用来作为运行提示，由用户来决定，是否给予最高权限。这个程序的名字叫做Superuser.apk。当某些程序执行su指令想取得系统最高权限的时候，Superuser就会自动启动，拦截该动作并作出询问，当用户认为该程序可以安全使用的时候，那么我们就选择允许，否则，可以禁止该程序继续取得最高权限。Root的过程其实就是把su文件放到/system/bin/，Superuser.apk放到system/app下面，还需要设置/system/bin/su可以让任意用户可运行，有set uid和set gid的权限。即要在android机器上运行命令：adb shell chmod 4755 /system/bin/su。而通常，厂商是不会允许我们随便这么去做的，我们就需要利用操作系统的各种漏洞，来完成这个过程，也就是一个root的过程。

## 实验环境

虚拟机：kali linux

Apk: Superuser.apk（路径：/root/tools/superuser）

工具：su（路径：/root/tools/superuser）

## 实验步骤


1、使用命令“android list avd”查看存在的模拟器，如图 1



```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~# android list avd
Available Android Virtual Devices:
  Name: 2.3
  Device: Nexus 4 (Google)
  Path: /root/.android/avd/2.3.avd
  Target: Android 2.3.3 (API level 10)
  Tag/ABI: default/x86
  Skin: 768x1280
  -----
  Name: 4
  Device: Nexus 4 (Google)
  Path: /root/.android/avd/4.avd
  Target: Android 4.0 (API level 14)
  Tag/ABI: default/armv7a
  Skin: 768x1280
root@kali:~#
```

图 1查看模拟器

2、使用命令“emulator -avd 4”启动Android4.0模拟器，如图 2



```
root@kali:~# emulator -avd 4
emulator: WARNING: Classic qemu does not support SMP. The hw.cpu.ncore option fr
om your config file is ignored.
emulator: Listening for console connections on port: 5554
emulator: Serial number of this emulator (for ADB): emulator-5554
emulator: emulator window was out of view and was recentered

emulator: WARNING: UpdateCheck: Failure: Error
emulator: WARNING: UpdateCheck: Failure: Error
emulator: WARNING: UpdateCheck: failed to get the latest version, skipping check
(current version '25.2.2-3098464')
```

图 2启动模拟器

3、模拟器成功开启，如图 3



图 3模拟器界面

4、在模拟器中打开超级终端APP，使用su命令查看手机是否root，如下图返回来的结果是手机没有root，如图 4

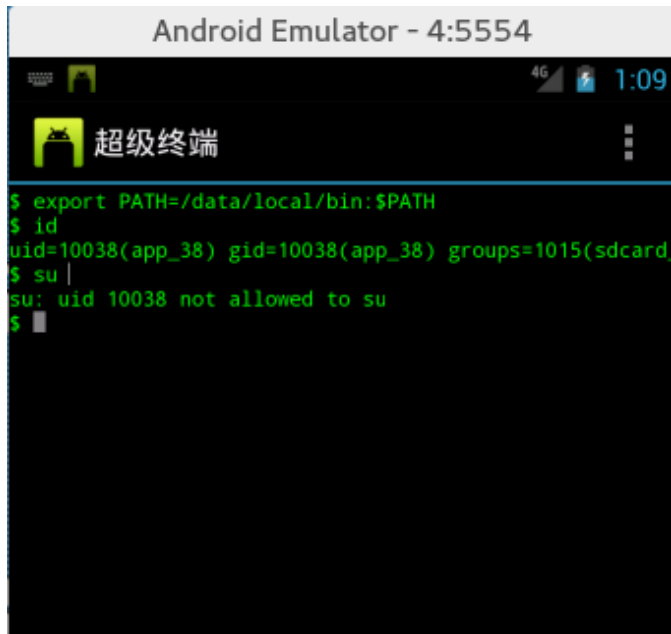


图 4 su失败

## 5、进入Android系统命令行，查看挂载

使用命令：“adb shell”->“mount”如图 5

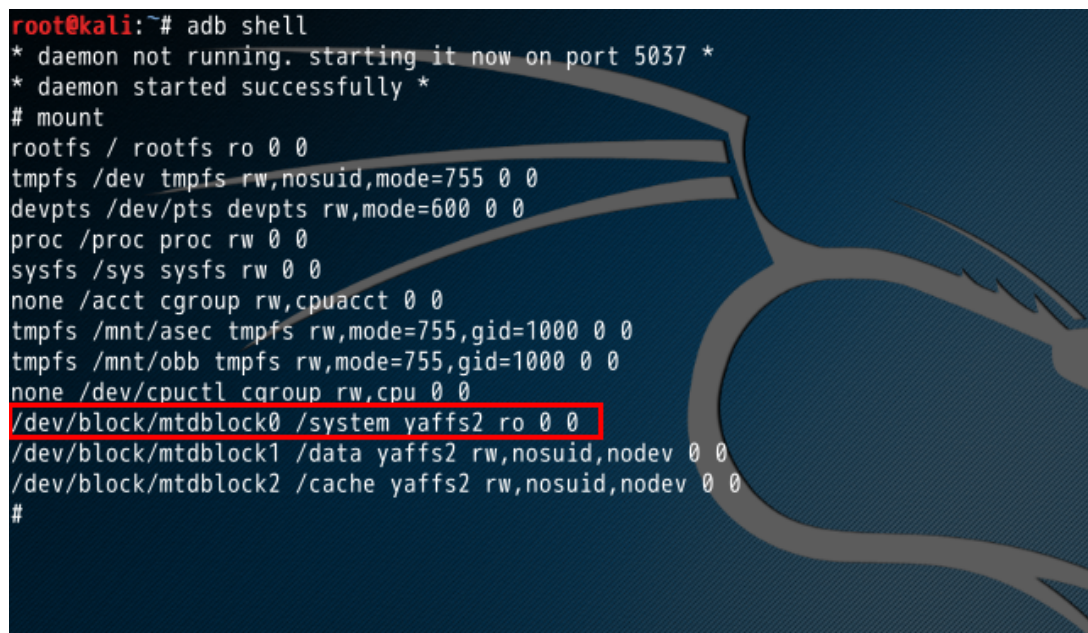
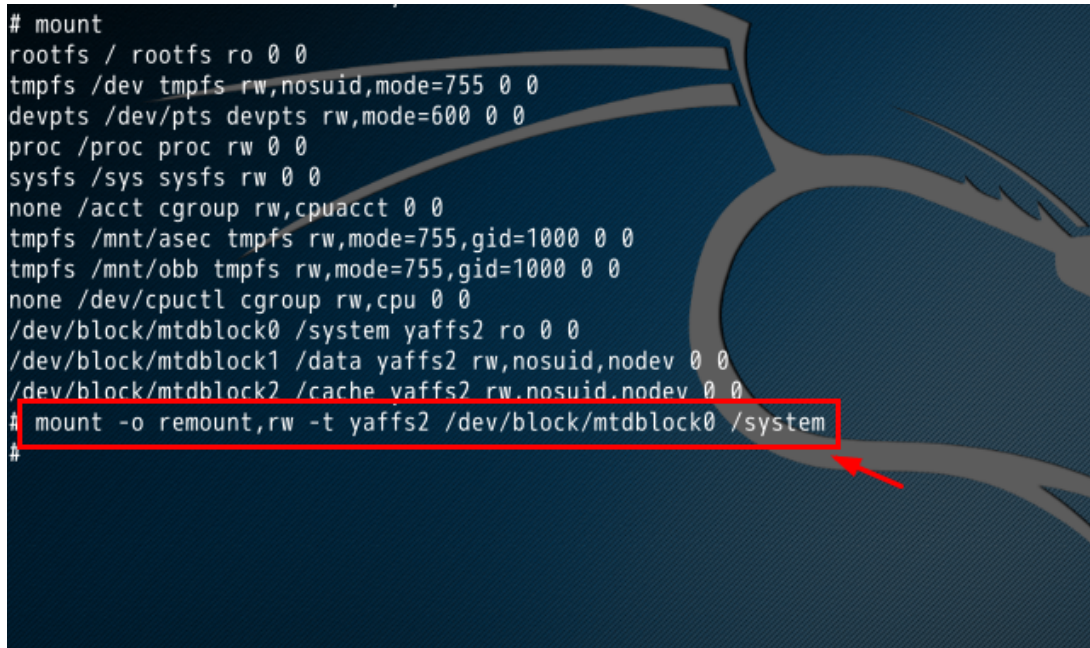


图 5查看挂载

## 6、把系统盘挂载为读写

使用命令：“mount -o remount,rw -t yaffs2 /dev/block/mtdblock0 /system”如图 6



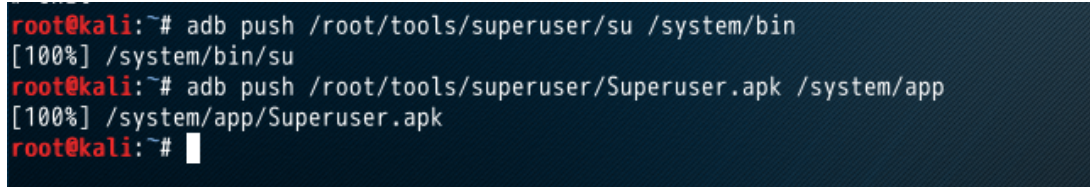


```
# mount
rootfs / rootfs ro 0 0
tmpfs /dev tmpfs rw,nosuid,mode=755 0 0
devpts /dev/pts devpts rw,mode=600 0 0
proc /proc proc rw 0 0
sysfs /sys sysfs rw 0 0
none /acct cgroup rw,cpuacct 0 0
tmpfs /mnt/asec tmpfs rw,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,mode=755,gid=1000 0 0
none /dev/cpuctl cgroup rw,cpu 0 0
/dev/block/mtdblock0 /system yaffs2 ro 0 0
/dev/block/mtdblock1 /data yaffs2 rw,nosuid,nodev 0 0
/dev/block/mtdblock2 /cache yaffs2 rw,nosuid,nodev 0 0
# mount -o remount,rw -t yaffs2 /dev/block/mtdblock0 /system
#
```

图 6挂载系统盘为读写

## 7、把su工具和Superuser.apk传到模拟器的系统文件夹

使用命令：“adb push /root/tools/superuser/su /system/bin”->“adb push /root/tools/Superuser.apk /system/app”如图 7

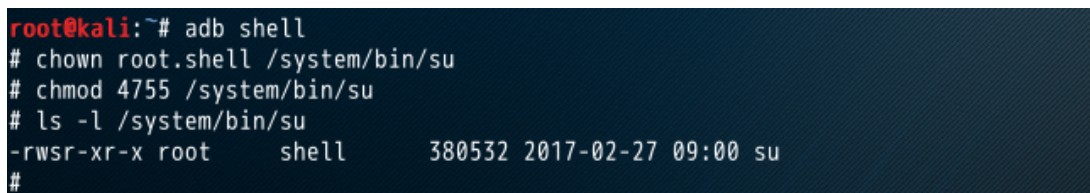


```
root@kali:~# adb push /root/tools/superuser/su /system/bin
[100%] /system/bin/su
root@kali:~# adb push /root/tools/superuser/Superuser.apk /system/app
[100%] /system/app/Superuser.apk
root@kali:~#
```

图 7上传su和Superuser

## 8、赋予su工具权限

使用命令：“adb shell”->“chown root.shell /system/bin/su”->“chmod 4755 /system/bin/su”->“ls -l /system/bin/su”如图 8




```
root@kali:~# adb shell
# chown root.shell /system/bin/su
# chmod 4755 /system/bin/su
# ls -l /system/bin/su
-rwsr-xr-x root shell 380532 2017-02-27 09:00 su
#
```

图 8赋予权限

## 9、赋予Superuser.apk权限

使用命令：“chown root.root /system/app/Superuser.apk”->“chmod 644 /system/app/Superuser.apk”->“ls -l /system/app/Superuser.apk”如图 9



```
# chown root.root /system/app/Superuser.apk
# chmod 644 /system/app/Superuser.apk
# ls -l /system/app/Superuser.apk
-rw-r--r-- root root 1468798 2017-02-27 09:00 Superuser.apk
#
```

图 9赋予权限

10、删除SdkSetup.apk

使用命令：“cd /system/app”->“rm SdkSetup.apk”->“ls -l SdkSetup.apk”如图 10

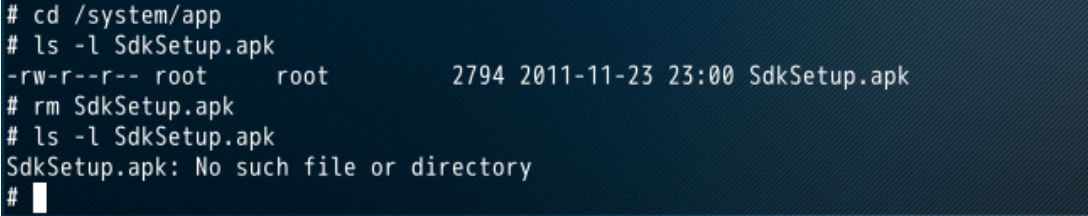


图 10删除SdkSetup

11、在超级终端输入su命令，然后弹出超级用户请求界面，点击允许，如图 11



图 11 超级用户请求

12、成功获取root权限，如图 12



图 12成功获取root

## 思考总结

本实验通过向模拟器传送su工具，su指令想取得系统最高权限的时候，Superuser就会自动启动，拦截该动作并作出询问，当用户认为该程序可以安全使用的时候，那么我们就选择允许，否则，可以禁止该程序继续取得最高权限。

1. 获取root权限还有什么方法呢？
2. 手机被root后的危害和好处有哪些？