Android Hook

在最近的学习中，我们成功实现了在安卓模拟机下的进程Hook,在终端中进行测试。

一.Android虚拟机的搭建

我们使用的是Android Studio进行对应的应用开发，但是由于Android Studio自带的模拟器启动过于慢且占内存太大，故此我们采用另一种方法完成虚拟机的搭建，即利用Genymotion和VirtualBox完成。

Genymotion和VitualBox要安装在同一目录

1.Genymotion安装:

(1).进入Genymotion官网 https://www.genymotion.com 点击Trial跳转到登录注册页面

(2).进行注册（必须注册才能完成接下来的步骤）

(3).下载对应的Genymotion安装包(选择对应的without VirtualBox版本)

(4).进行安装

安装完成后会出现**Genymotion**和**Genymotion shell**两个图标

2.VirtualBox安装:

(1).进入VitrualBox官网 https://www.virtualbox.org/ 点击Download进行下载

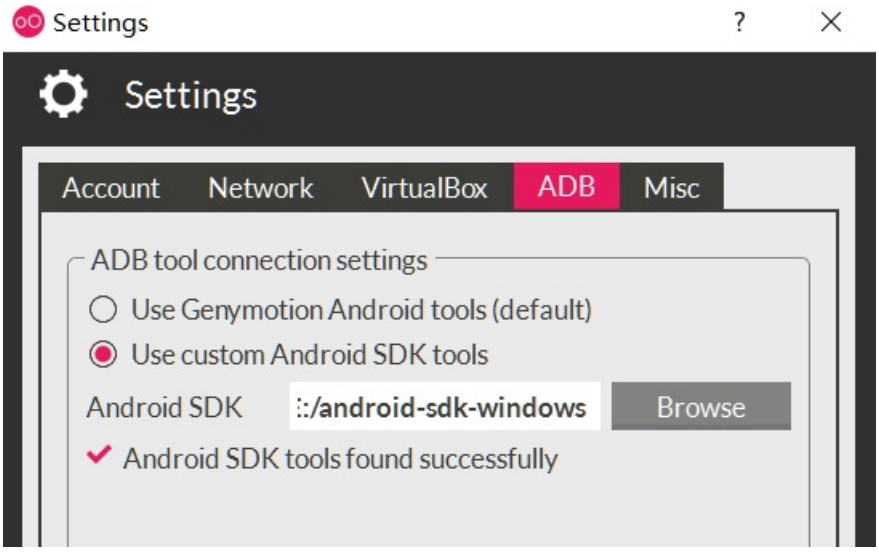
(2).进行安装

3.创建虚拟机:

(1).点击Genymotion图标

(2).点击Settings进行设置，找到ADB，勾选使用Android Studio自带的sdk文件夹

(3).设置好adb.exe的系统的环境变量。



(3).点击Add添加虚拟机并选择对应的参数并选择运行即可。

至此我们可以拥有一个**Android**虚拟机。

二。利用Android虚拟机进行Hook

利用adb工具可以实现将Native语言程序(.c .cpp)生成的二进制文件运行在Android终端中,实现对Android进程的Hook

1.生成二进制文件

首先要将对应的C/C++代码编译为二进制文件。在Linux中利用GCC等编译器进行编译。编译命令为:

```
gcc  -o filename filename.c -static
```

2.将二进制文件push入android模拟机中

adb命令的简介:
adb push 将电脑上的文件传入到Android虚拟机中，
adb devices 显示所连接的设备，包括虚拟机和USB调试的真机
adb shell 进入到终端中，默认是root权限。
adb pull 将Android虚拟机中的文件传入到电脑上

具体操作:

```
gcc -o des des.c -static                                    //编译des.c生成des二进制文件
gcc -o ptrace ptrace.c -static                              //编译ptrace.c生成ptrace二进制文件
adb push C:\Users\lenovo\Desktop\des dev/                    //将桌面上的des二进制文件push进Android模拟机的dev/目录下
adb push C:\Users\lenovo\Desktop\ptrace dev/                 //将桌面上的ptrace二进制文件push进Android模拟机的dev/目录下
adb shell                                                  //进入到模拟机所在的终端中
cd /dev                                                     //切换到dev目录下
chmod 777 des
chmod 777 ptrace                                              //赋予des ptrace可执行权限
./des                                                     // 运行des
ps                                                        //查看des所在进程的进程号为pid
./ptrace  pid                                               //运行ptrace可对des所在进程pid进行暂停。
```

至此完成了Android模拟机基于终端的Hook技术