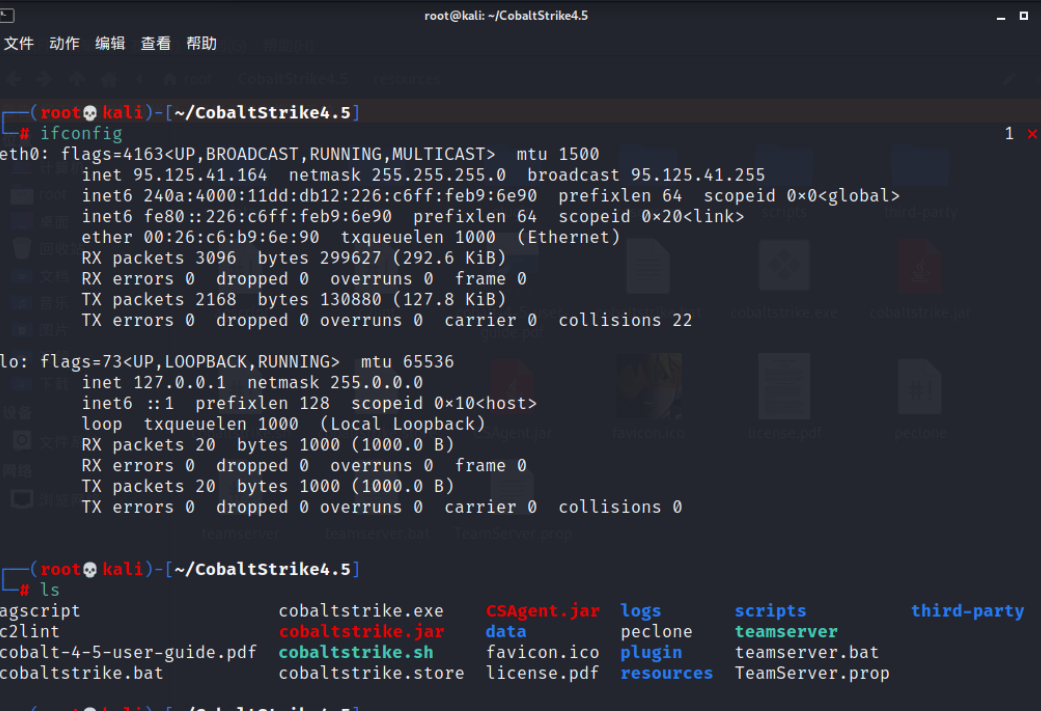
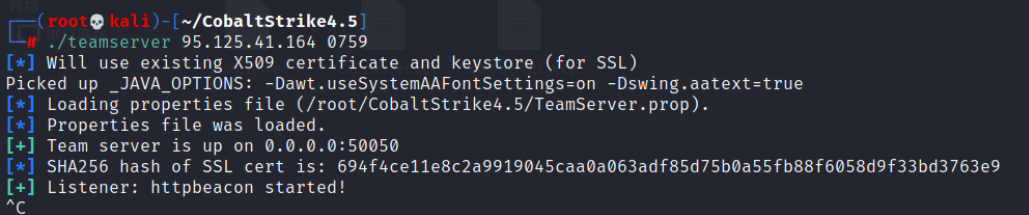
基于cs的域渗透

首先查看本机ip



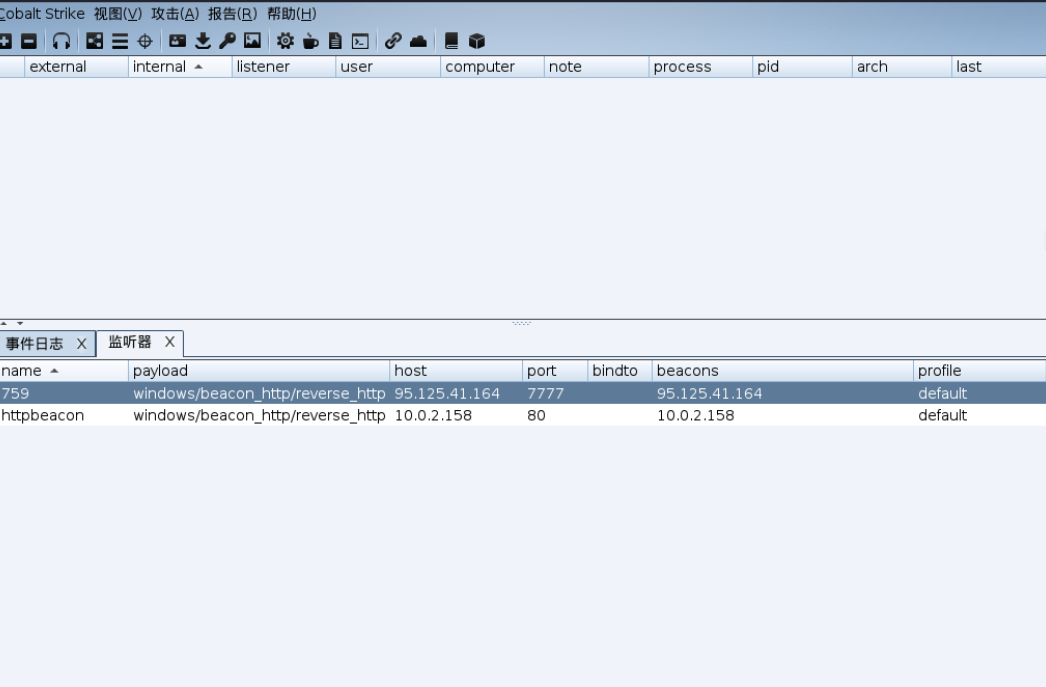
开启cs的teamserver ./teamserver+本机ip+密码



在通过./..sh开启cs

进入cs后，首先配置监听器



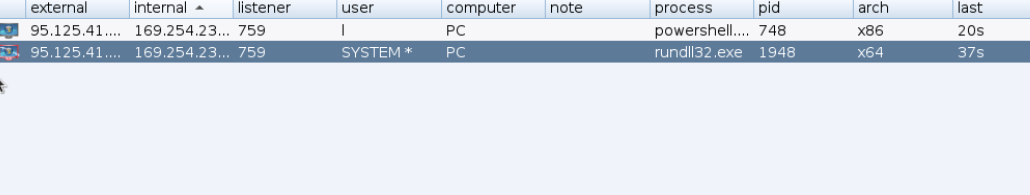


配置完成后，便可在本机开启监听

Cs自带后门生成



通过文件托管，可以生成钓鱼网站，当目标机访问后，便会留下后门，在cs上上线。



Cs自带有攻击模块，但攻击不一定成功，因为需要管理员权限，可以通过提升权限来解决



Cs可以安装插件，插件提供了许多一键渗透的功能



