**CobaltStrike基础使用**

**1、下载链接：**

TRY博客

https://www.nctry.com/1744.html

搜索引擎：

博客：

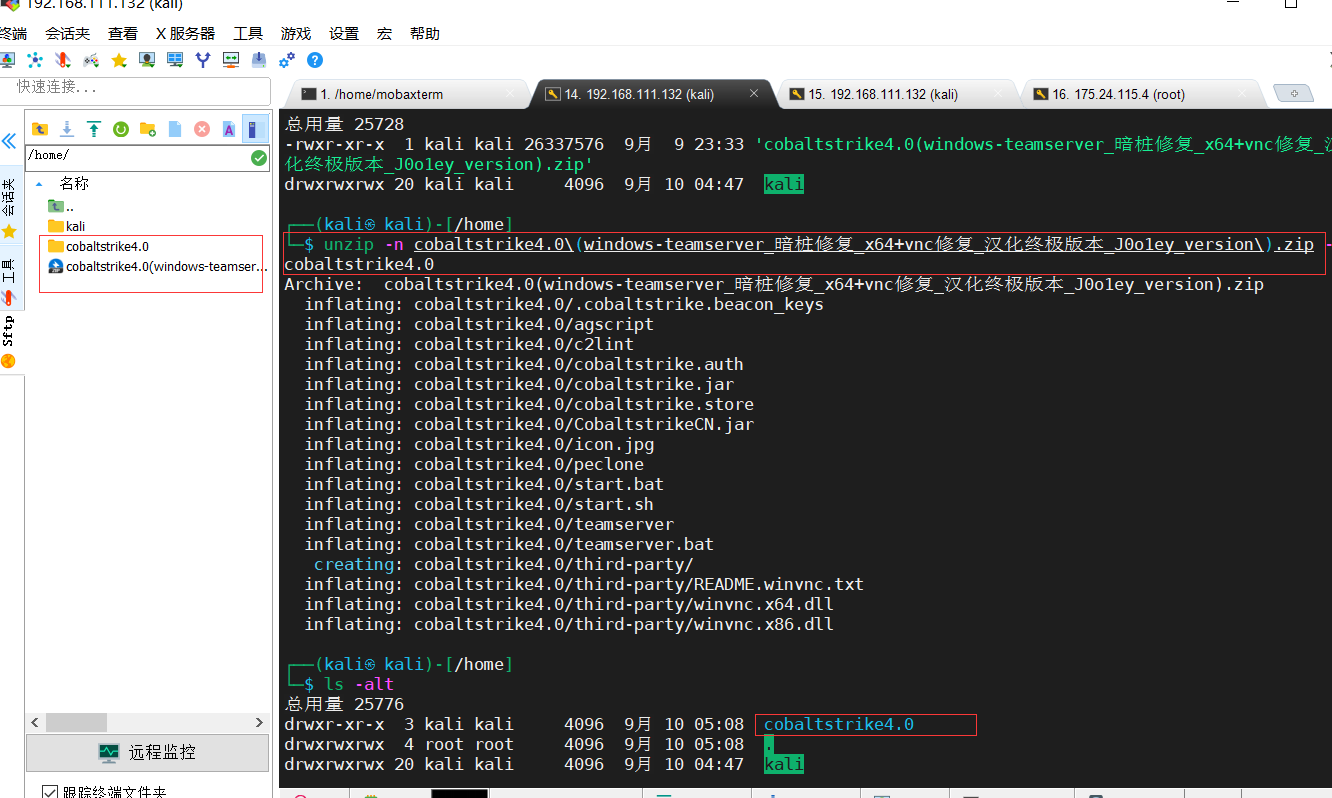
https://www.cnblogs.com/ssooking/p/12535998.html

工具链接：

[https://gitee.com/ssooking/cobaltstrike-cracked.git](https://gitee.com/ssooking/cobaltstrike-cracked.git" \t "https://www.cnblogs.com/ssooking/p/_blank)

**2、解压：**

unzip -n cobaltstrike4.0\(windows-teamserver\_暗桩修复\_x64+vnc修复\_汉化终极版本\_J0o1ey\_version\).zip -d ./cobaltstrike4.0

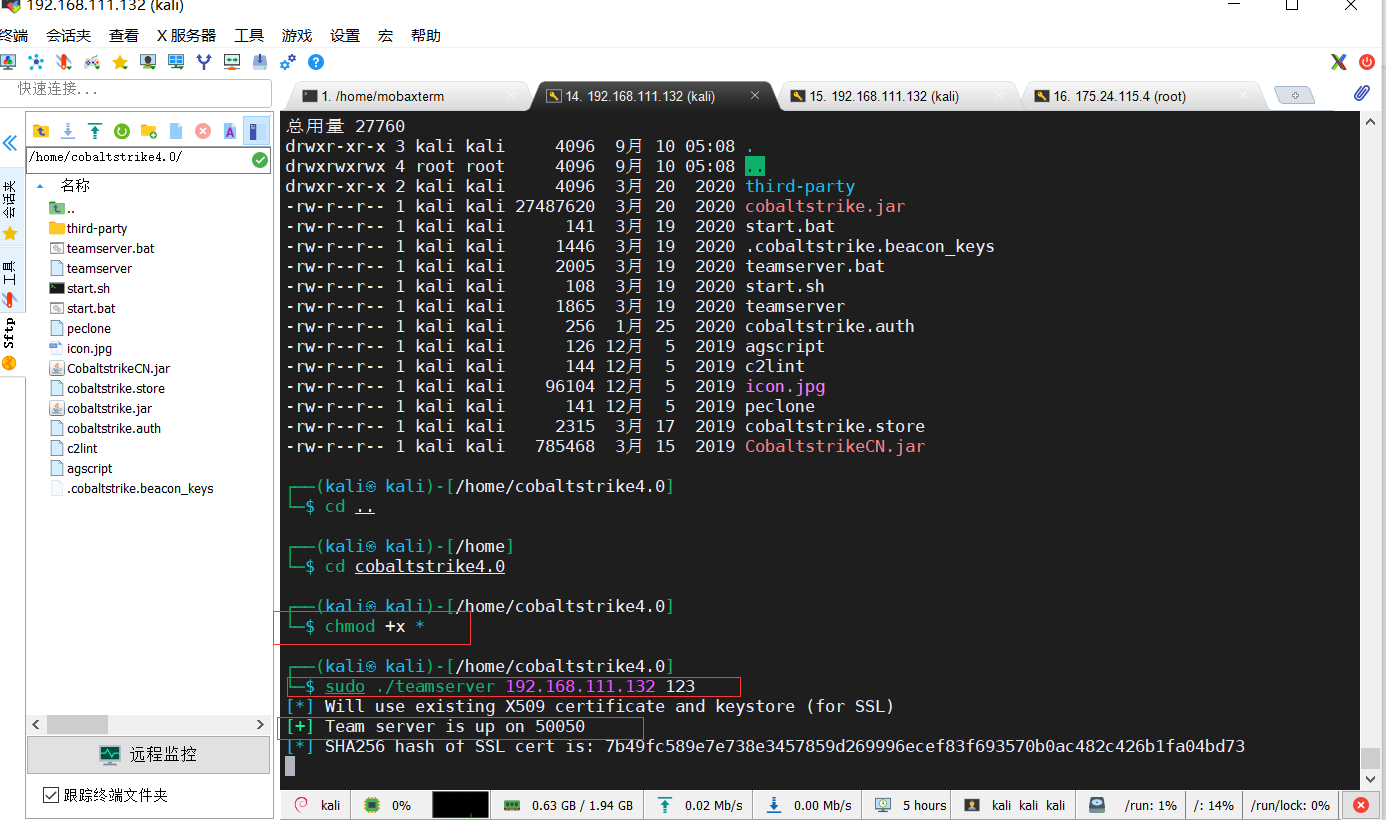


**3、启动CobaltStrike服务器，服务器ip:192.168.111.132，密码：123，在teamserver脚本里，默认监听：50050端口**

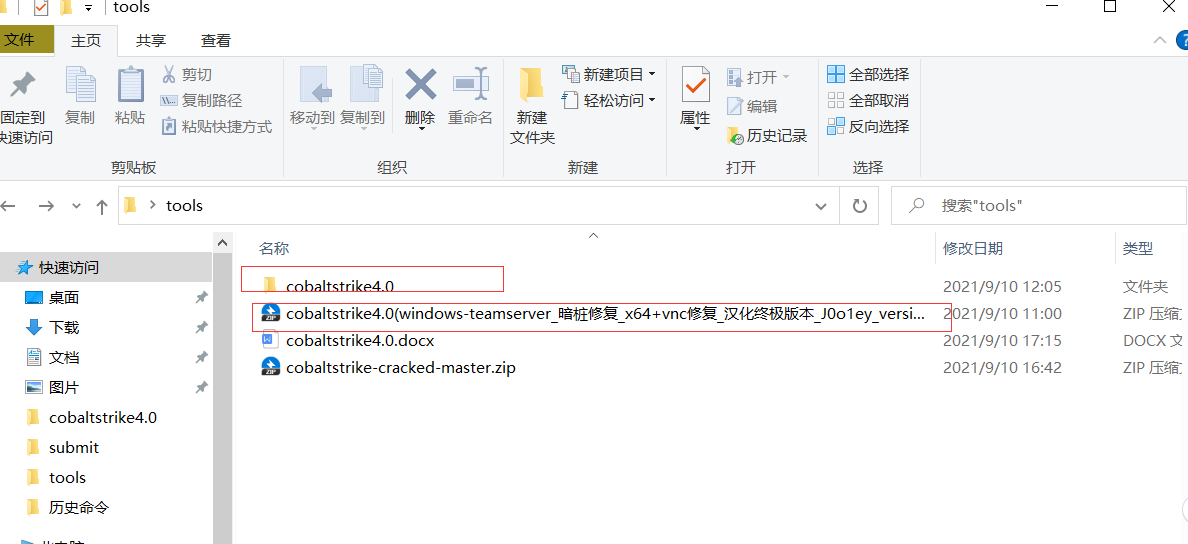
cd cobaltstrike4.0

chmod +x \*

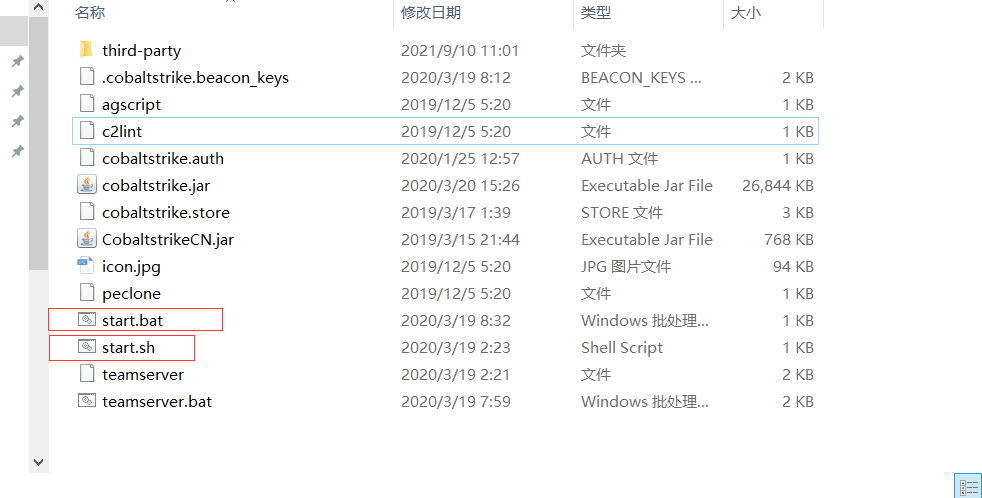
sudo ./teamserver 192.168.111.132 123



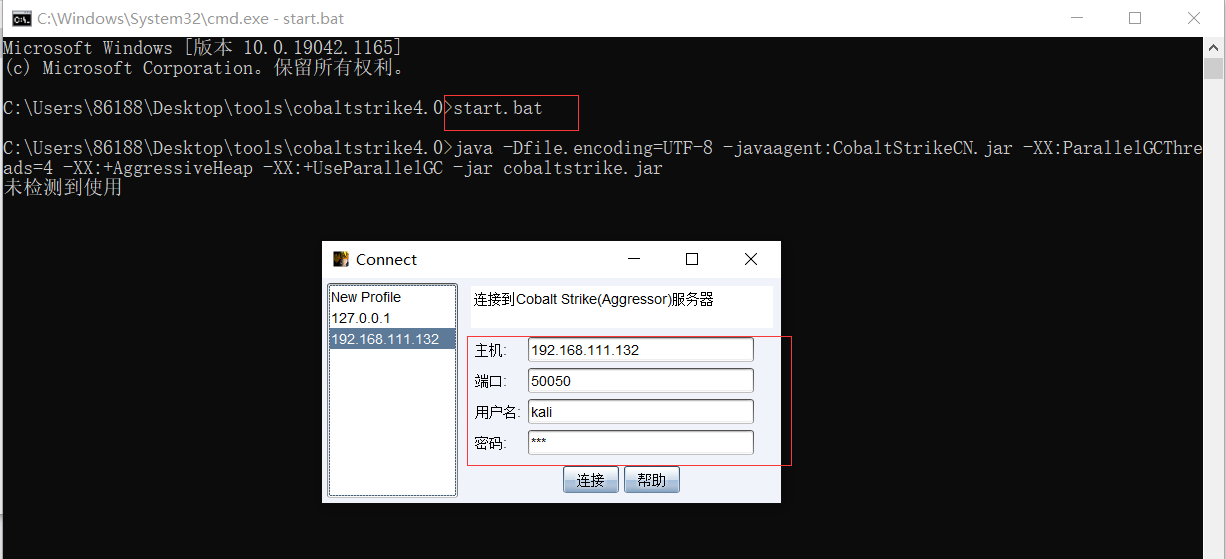
**4、启动CobaltStrike客户端，Windows上解压至cobaltstrike4.0文件夹**



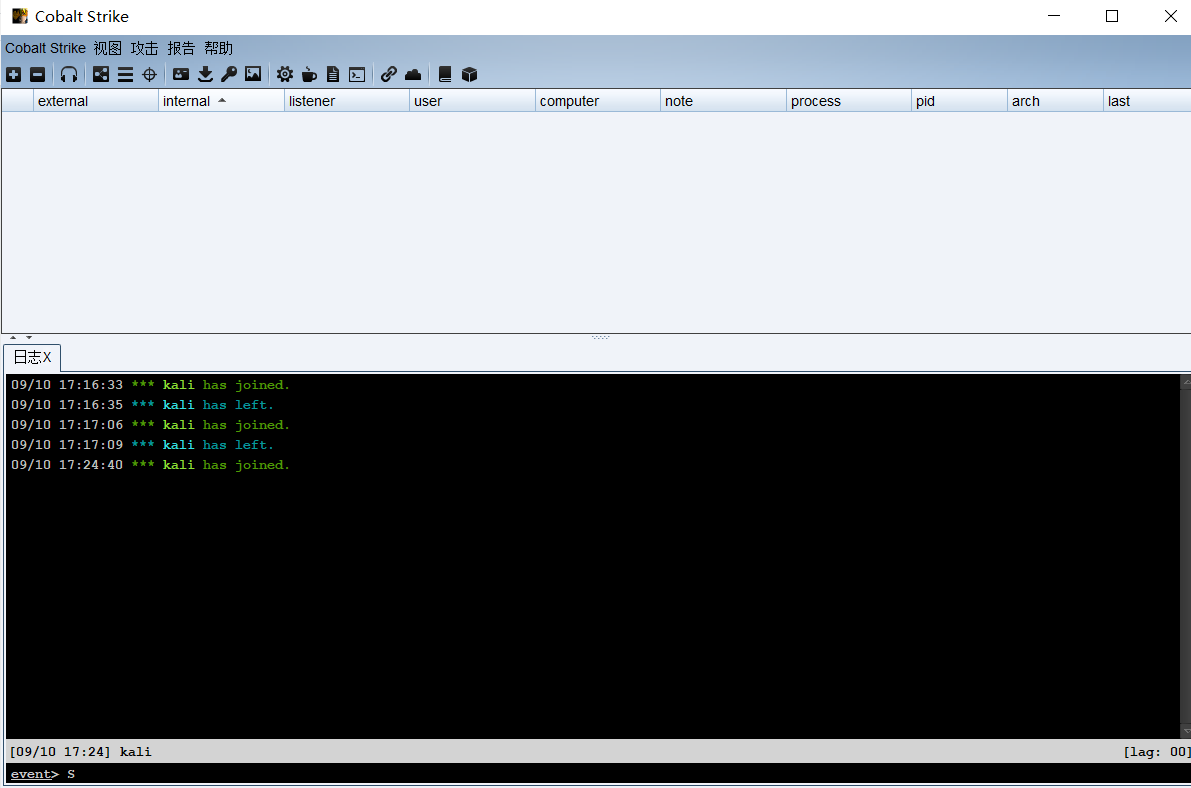
**5、进入cobaltstrike4.0文件夹，Start.bat为windows版CobaltStrike客户端启动脚本，start.sh为linux版CobaltStrike客户端启动脚本**



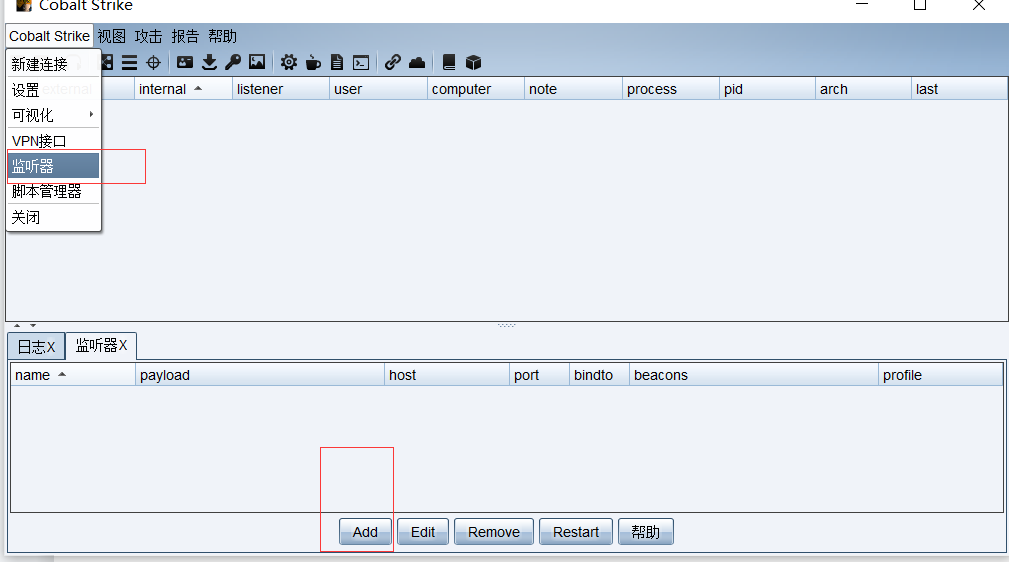
**6、打开cmd.exe，输入命令：start.bat，主机：CobaltStrike服务器ip：192.168.111.132,端口：CobaltStrike服务器监听端口：50050，用户名：服务器用户名：kali，密码：之前设置的服务器连接密码：123，点击连接**



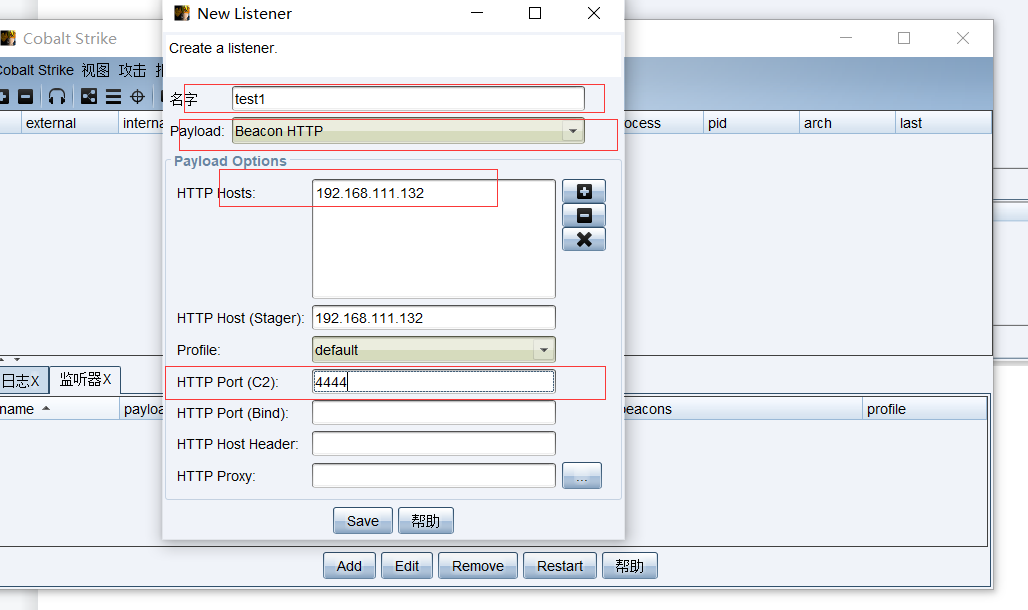
**7、连接成功：**



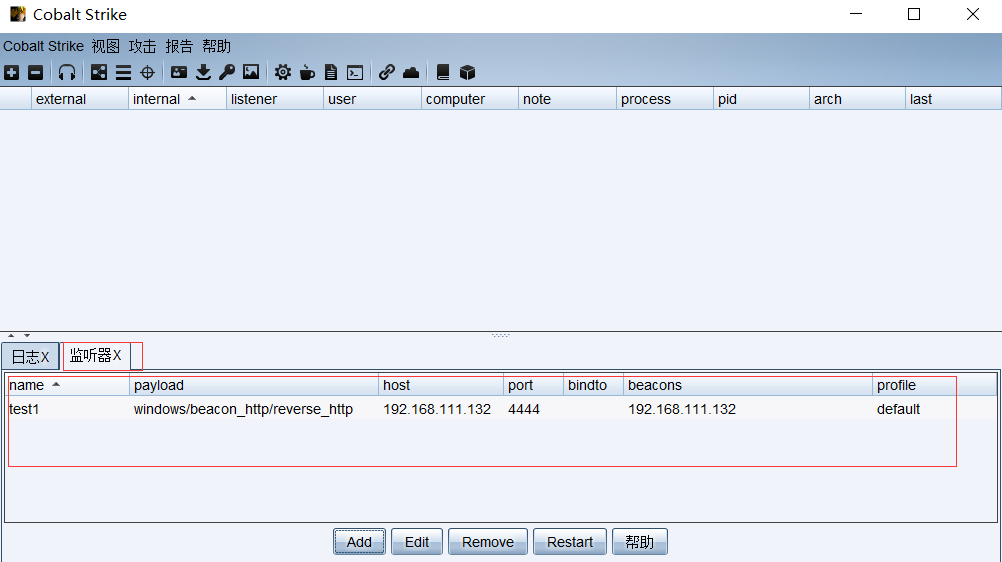
**8、创建shell监听端口：CobaltStrike--->监听器，然后点击add**



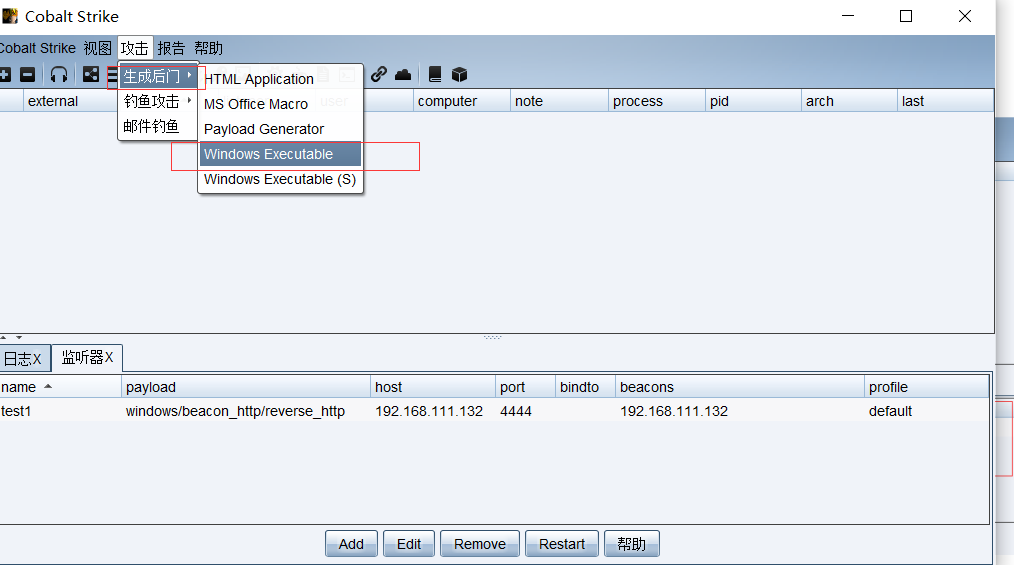
**9、选择Payload类型(本次默认)，ip为CobaltStrike服务器：192.168.111.132，监听端口：4444，点击save**



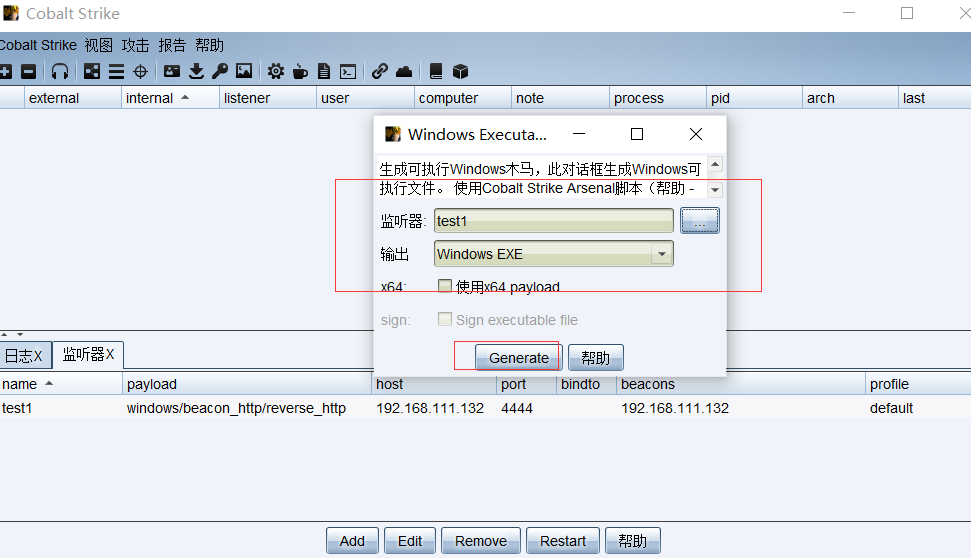
**10、可以看到监听器创建成功**



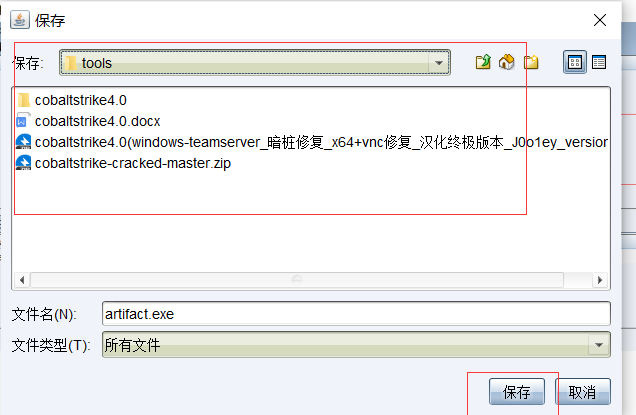
**11、生成后门：点击攻击-->生成后门-->windows Executable**



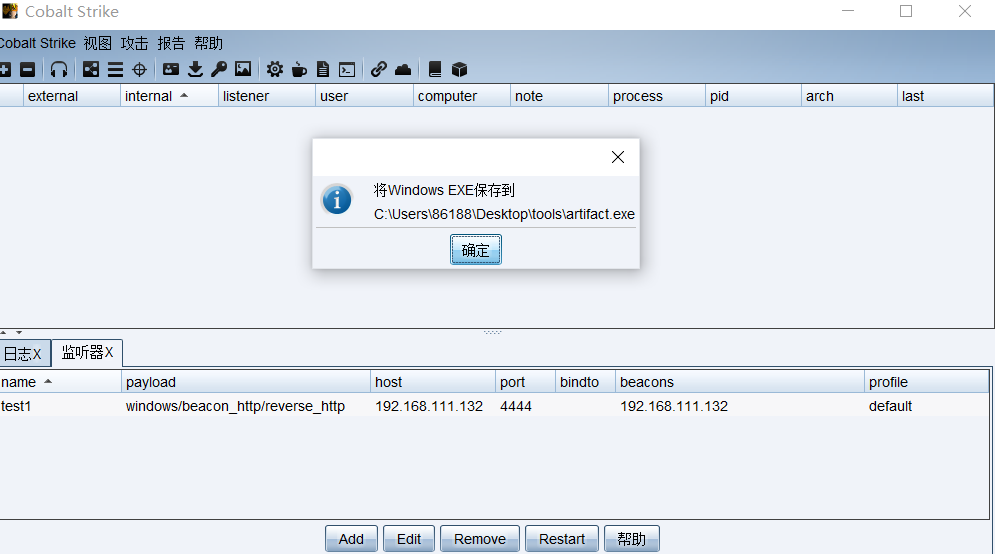
**12、选择刚刚创建的监听器，点击Generate**



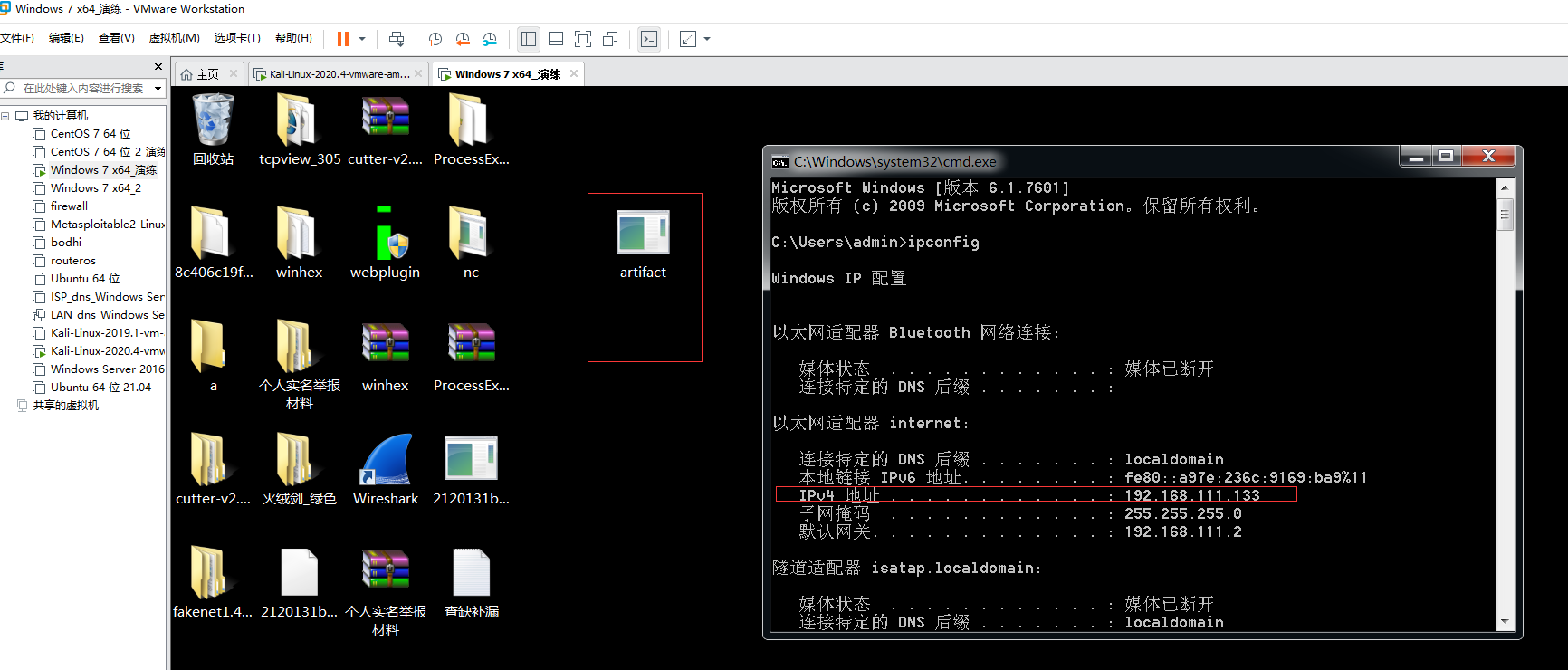
**13、选择合适的路径，点击保存**



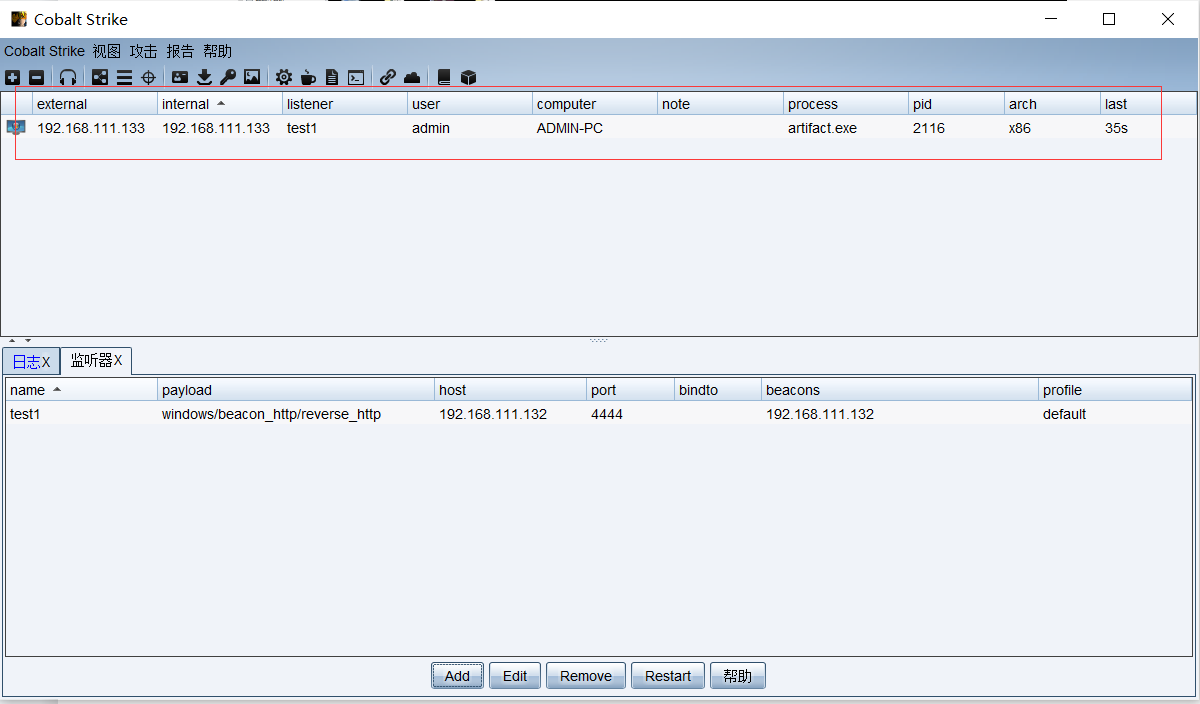
**14、生成后门成功**



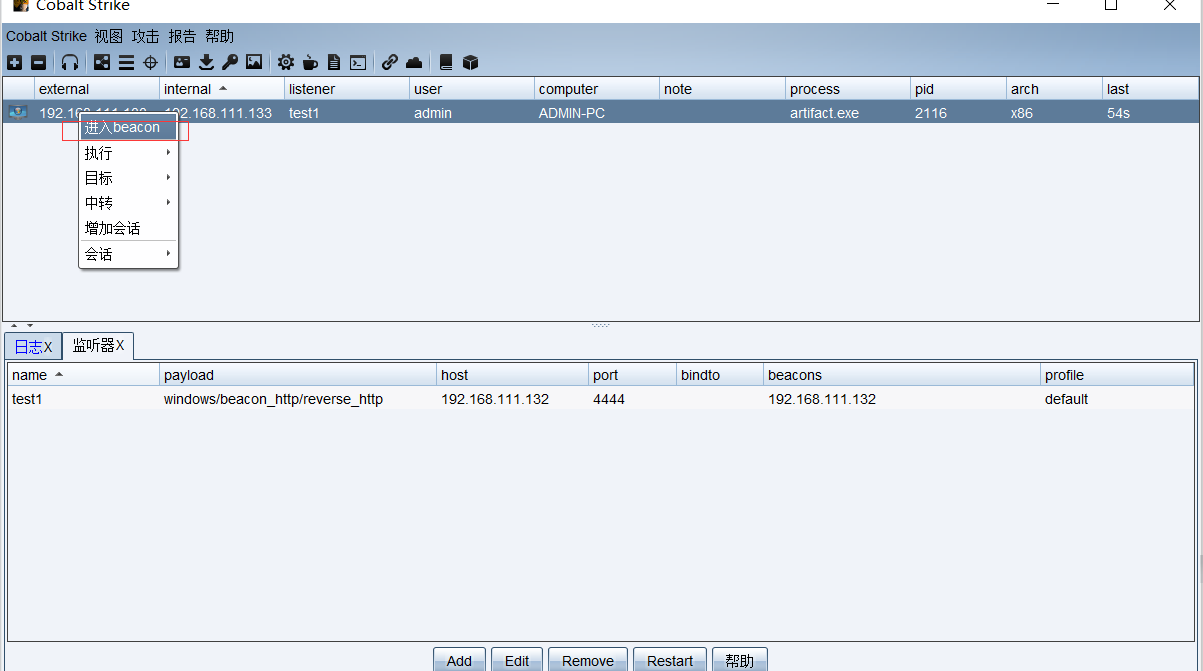
**15、将后门artifact.exe复制到受害者机器上ip:192.168.111.133,并双击运行**



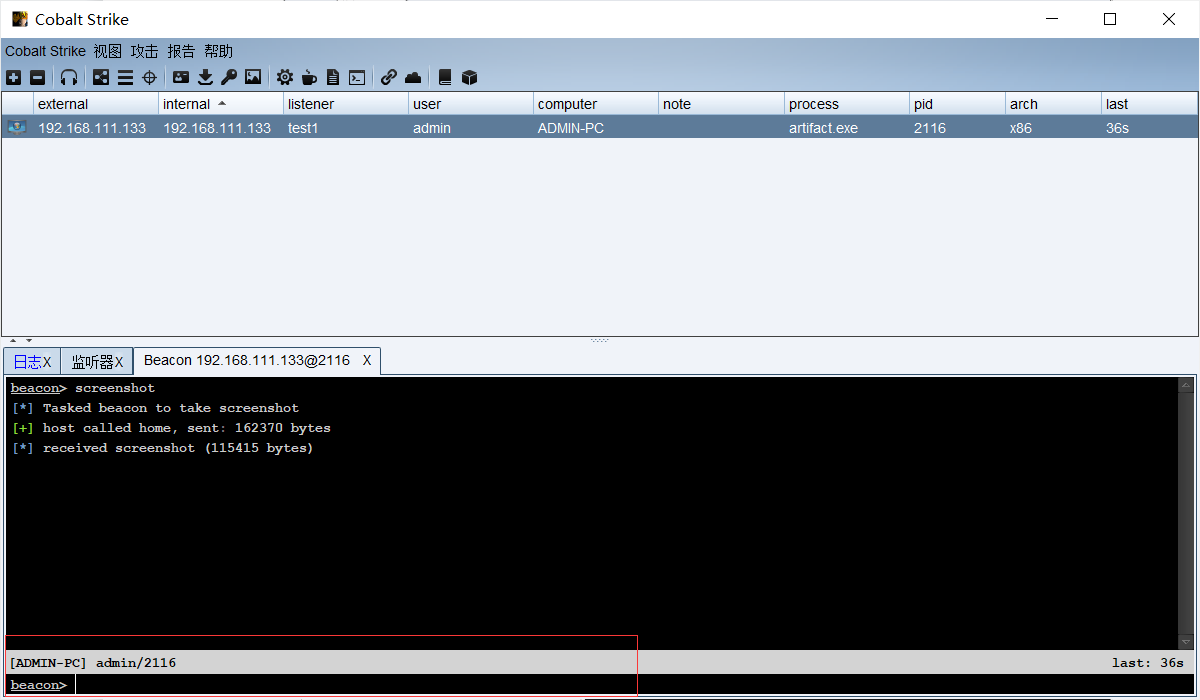
**16、上线成功，可以看到CobaltStrike客户端出现受害者ip:192.168.111.133的上线信息**



**17、右键肉鸡，选择进入beacon：是一种交互shell**



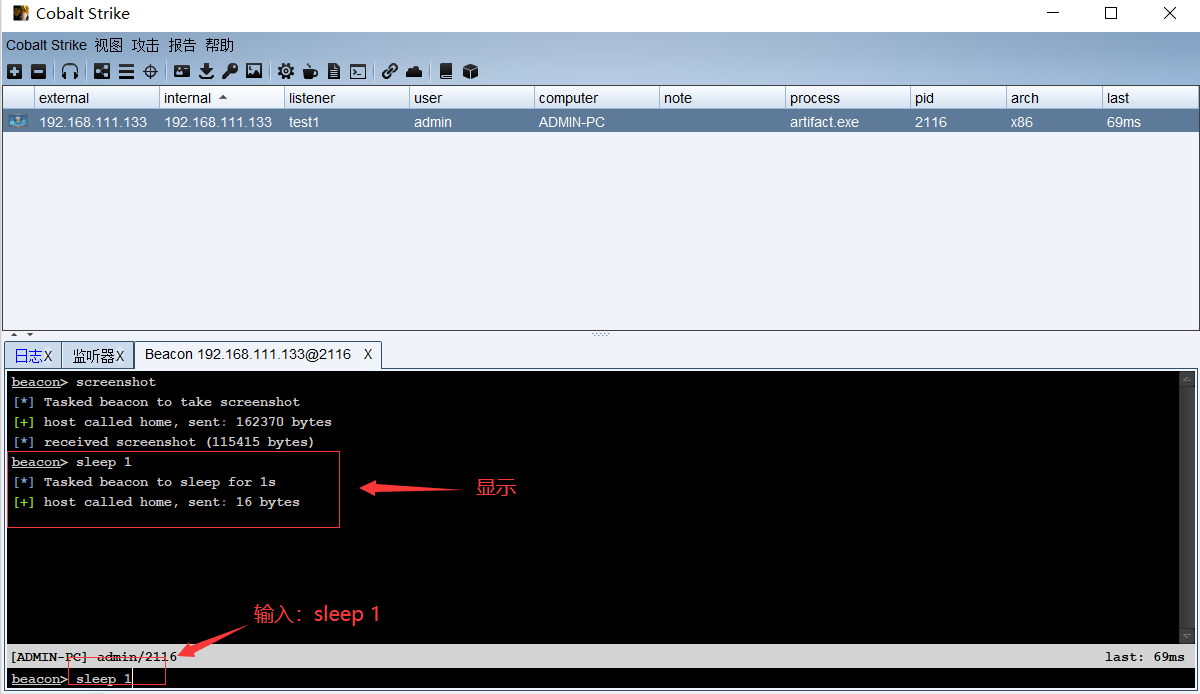
**18、进入成功：**



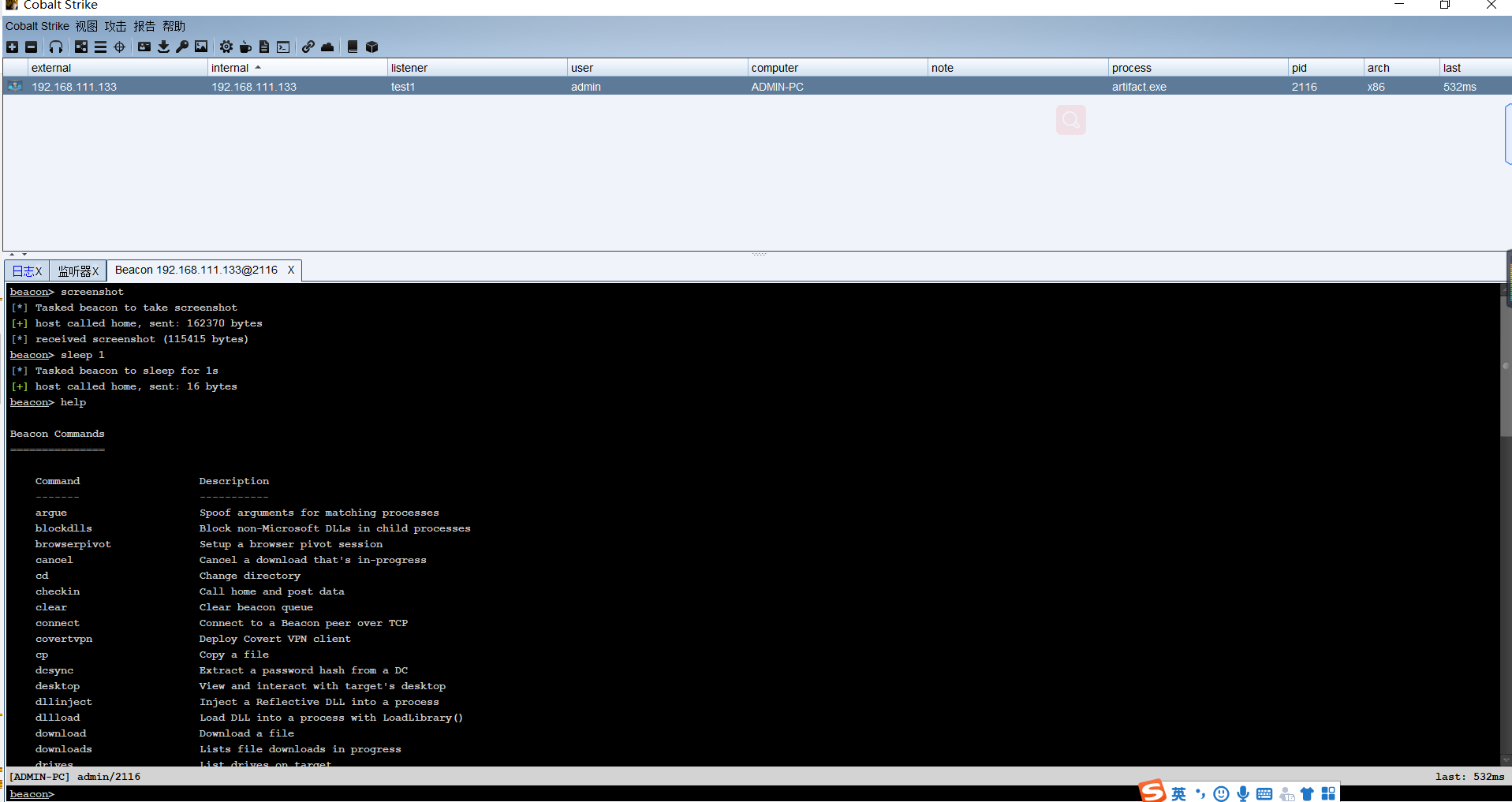
**19、修改CS默认的心跳时间**

进入beacon模式之后，我们首先要修改CS默认的心跳时间（sleep）。一般情况下CS默认的心跳时间为60s，即每一分钟目标主机与我们的Teamserver服务器进行交互。那这样的话就会让我们执行操作的响应速度会变慢。如果实战中就建议不要太快，不然流量会被很快发现。如果是实验，那我们一般都是设置为0或者1,如图：

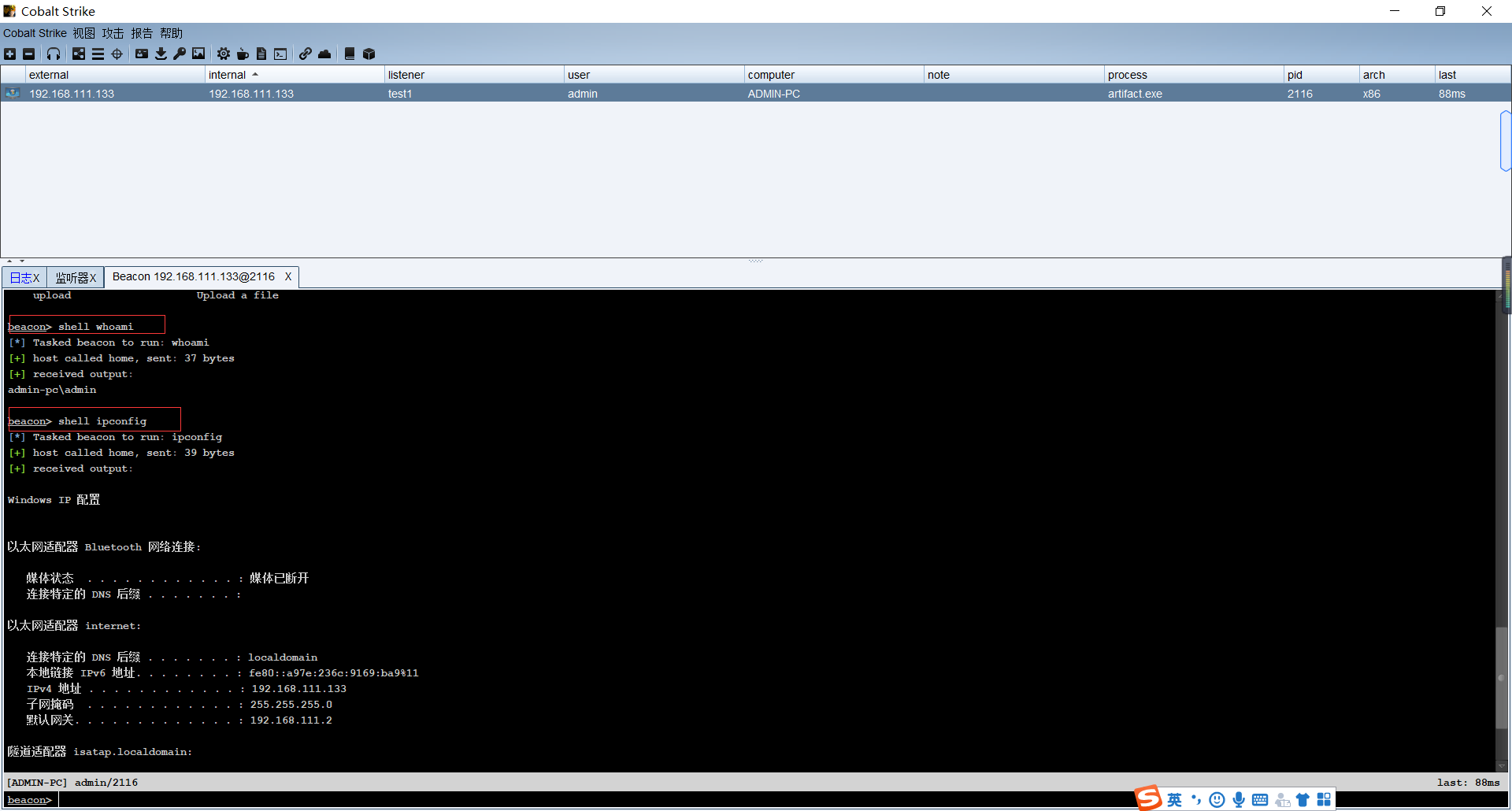
输入：sleep 1



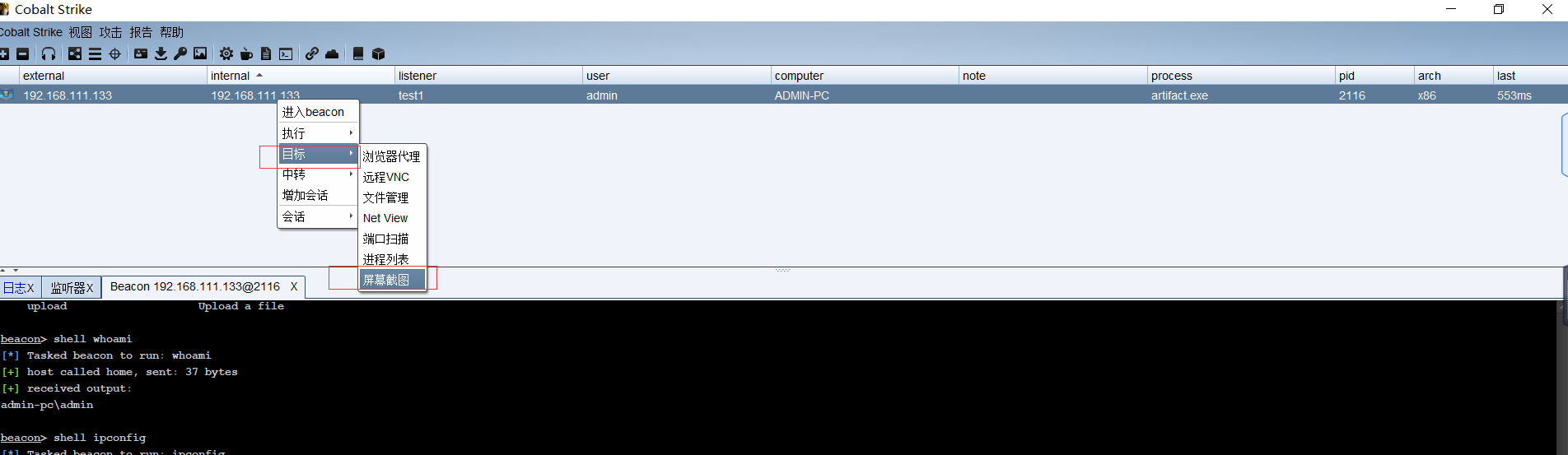
**20、输入：help,可以查看帮助信息**



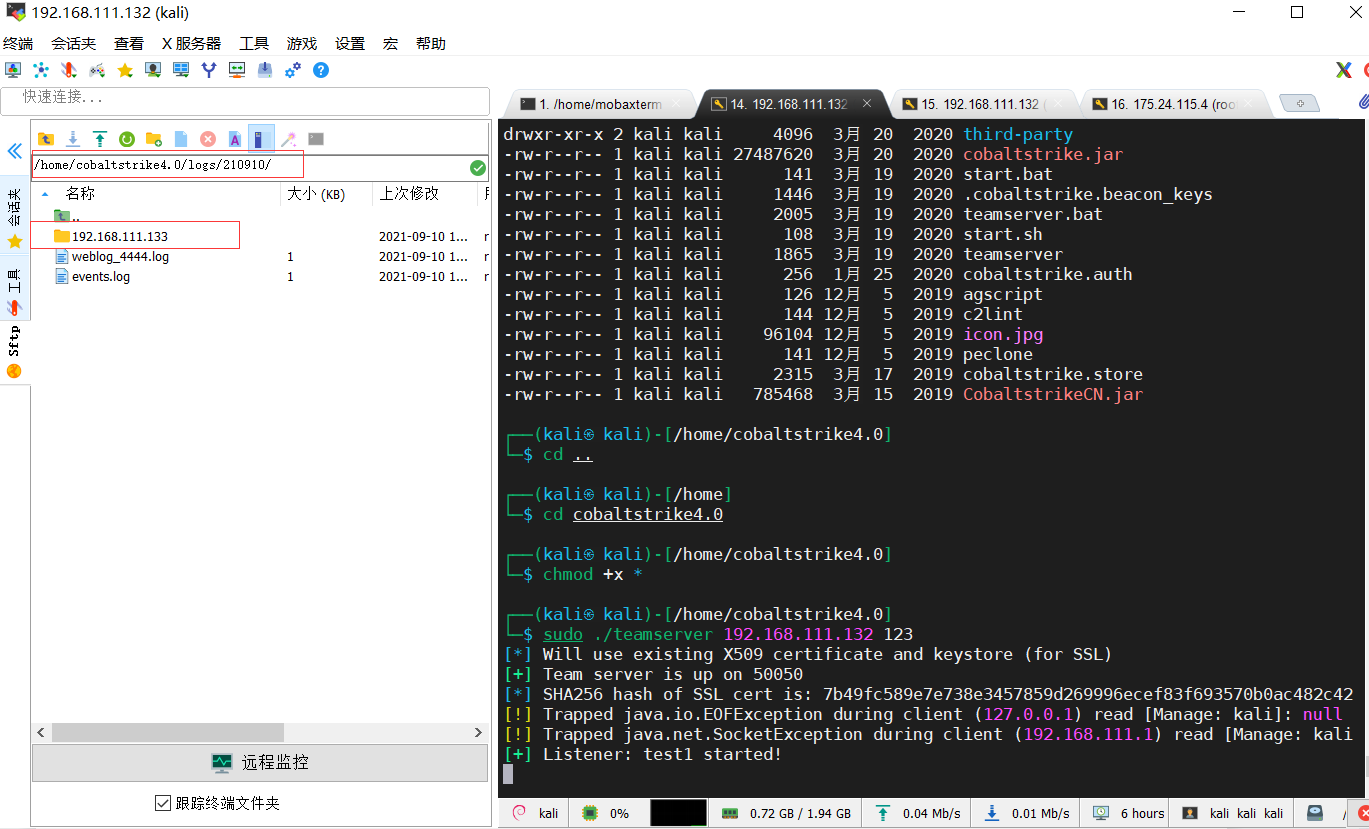
**21、执行命令：shell whoami和shell ipconfig**



**22、右键点击选择:目标-->“屏幕截图”：**

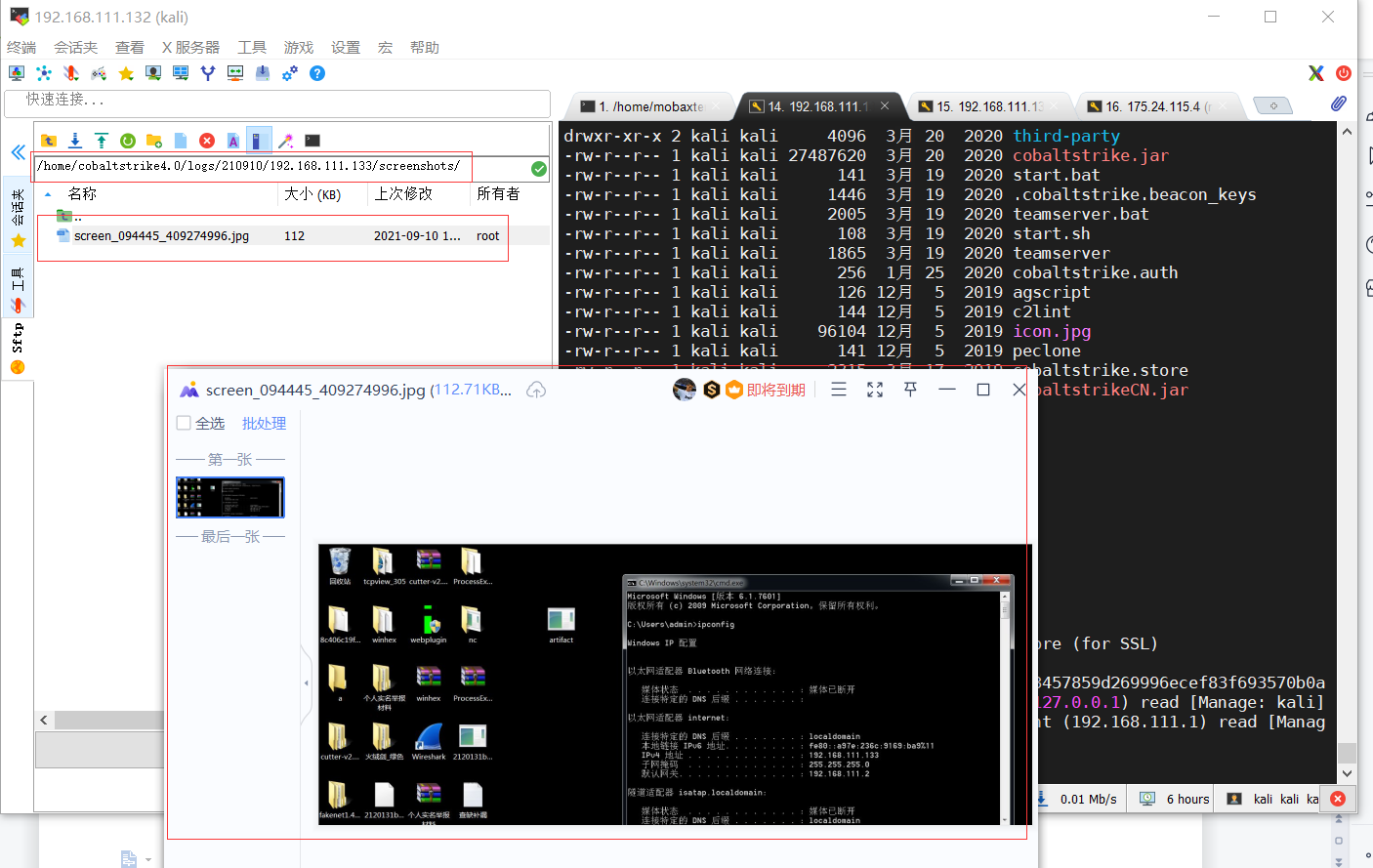


**23、在CobaltStrike服务器路径：/home/cobaltstrike4.0/logs/210910/下，可以查看关于肉鸡192.168.111.133记录信息：**

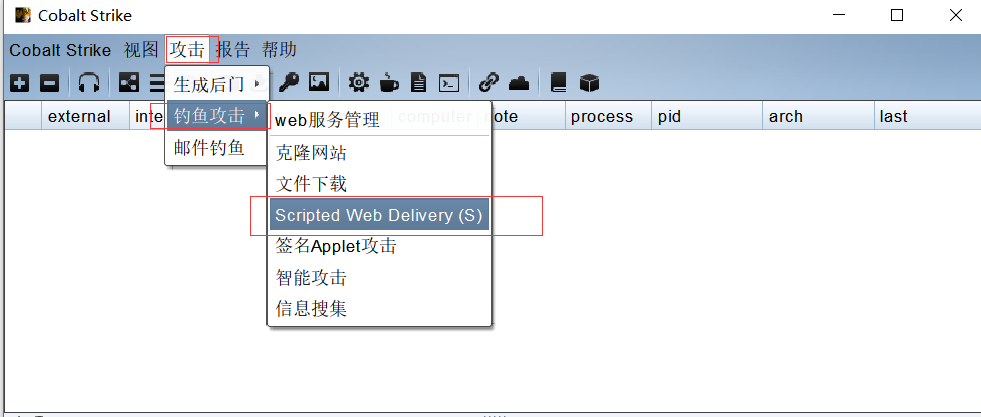


1. **可以看到刚刚的截图在服务器路径下：**

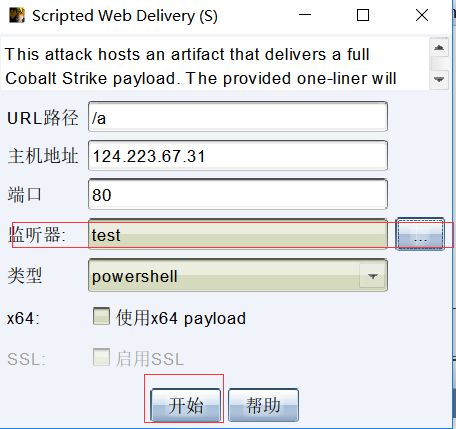
**/home/cobaltstrike4.0/logs/210910/192.168.111.133/screenshots/**



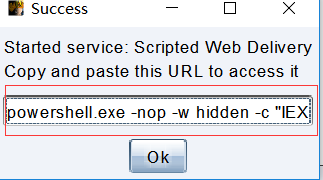
1. **钓鱼攻击之Scripted Web Delivery**



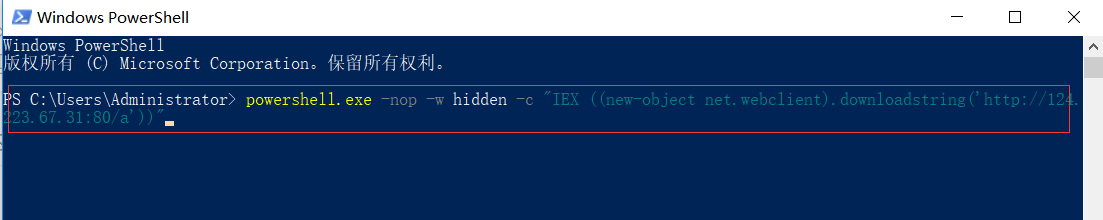
1. **选择监听器，点击开始**



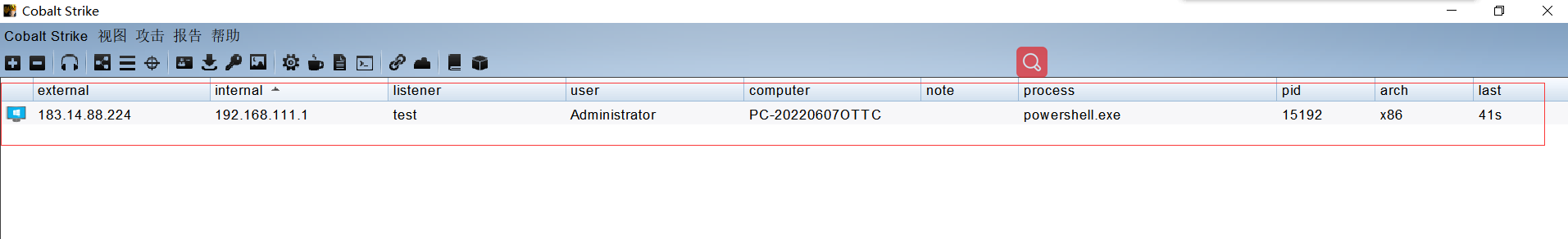
1. **复制命令**



1. **Powershell执行命令**



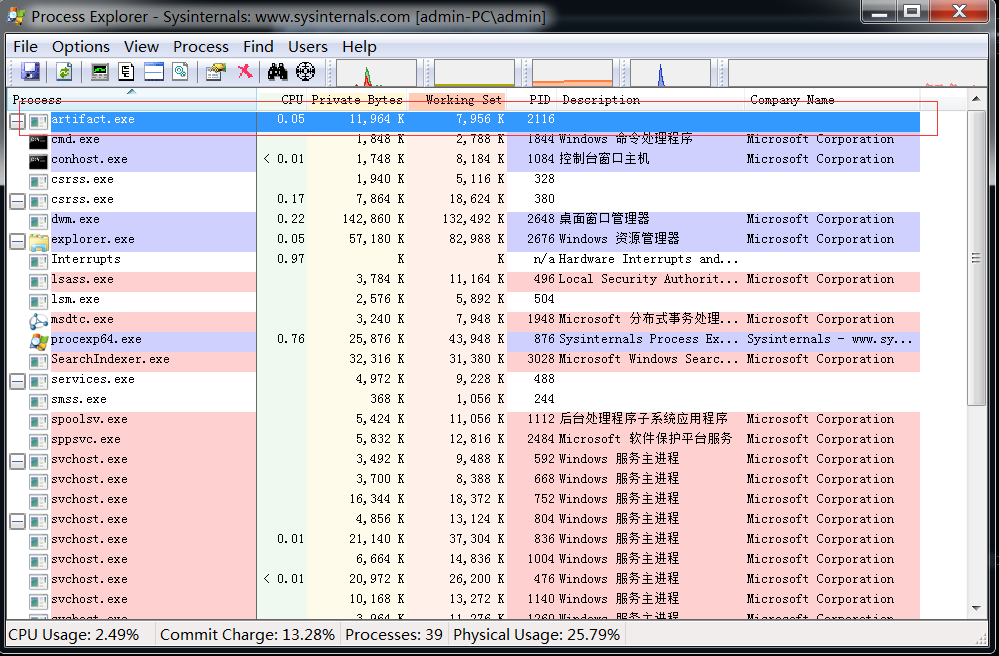
1. **成功上线**



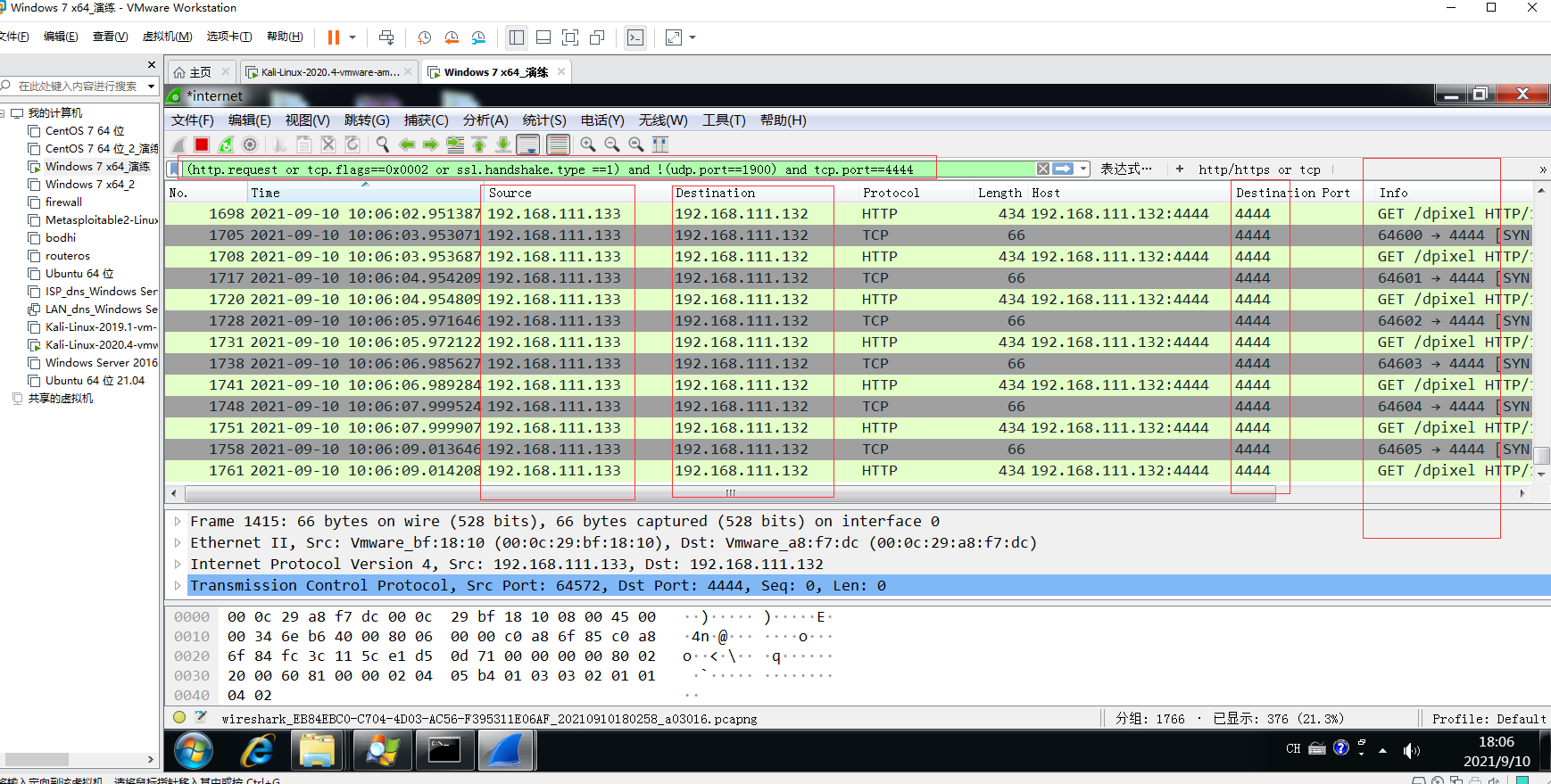
**结束！**

**排查篇：**

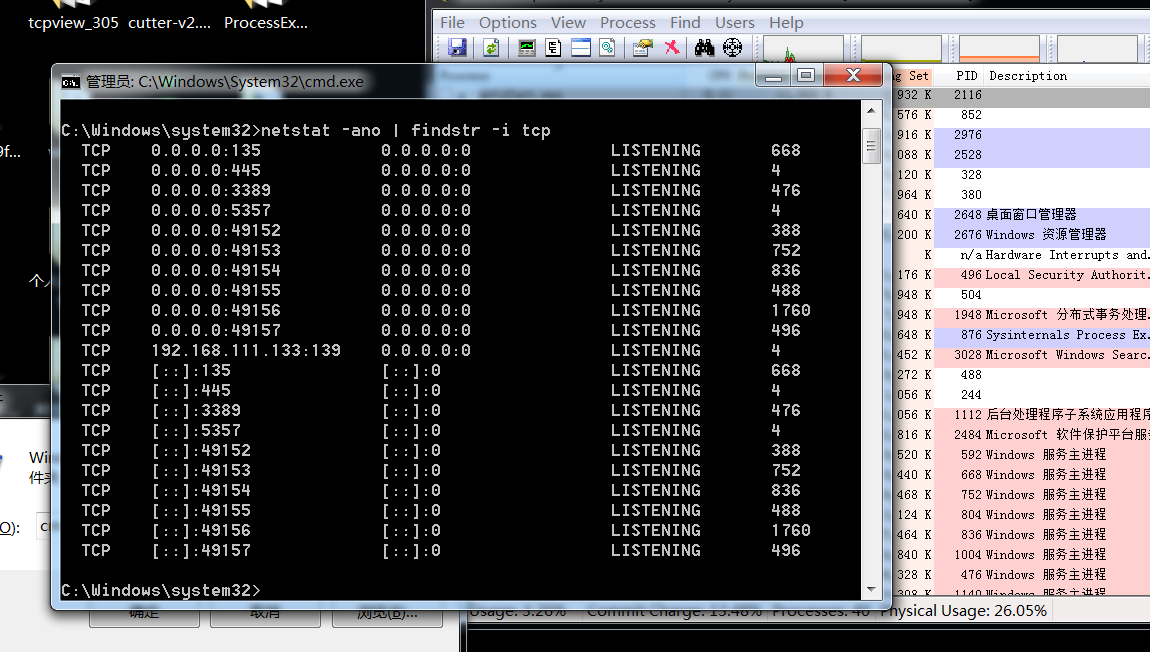
**1、进程：Process explorer工具可以看到进程：**



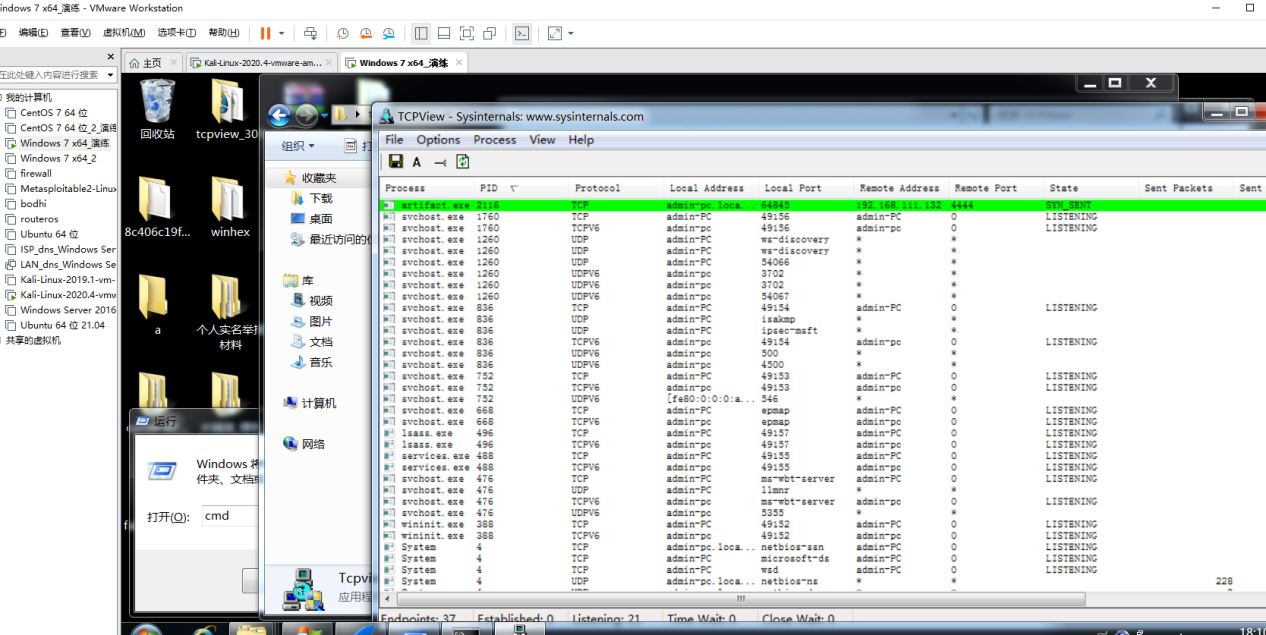
**2、网络：Wireshark抓包，可以看到心跳包，受害者一秒连一次CobaltStrike服务器**



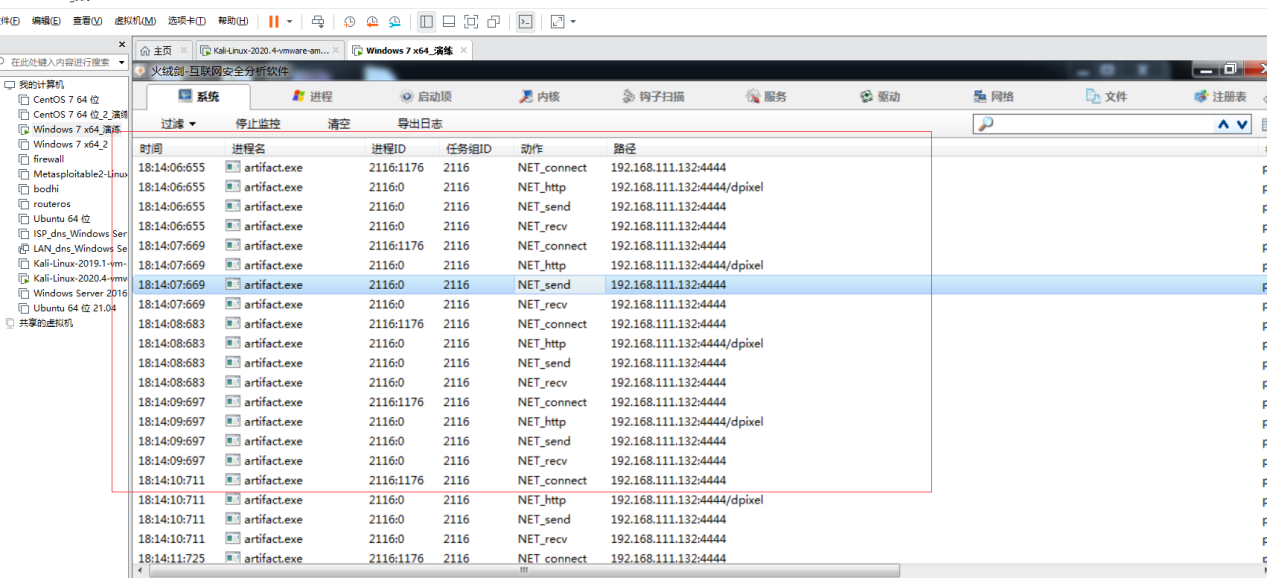
**3、网络：命令：netstat -ano | findstr -i tcp，看不出artifact.exe pid:2216的网络连接**



**4、网络：用tcpview工具打开等待观察，可以发现捕获到短暂出现的artifact.exe pid:2216的网络连接：然后又消失了**



**5、网络：用火绒剑工具，开启监控网络连接，可以发现artifact.exe pid:2216的实时异常连接**



**结束！**

参考：

https://github.com/aleenzz/Cobalt\_Strike\_wiki