NETSH端口转发

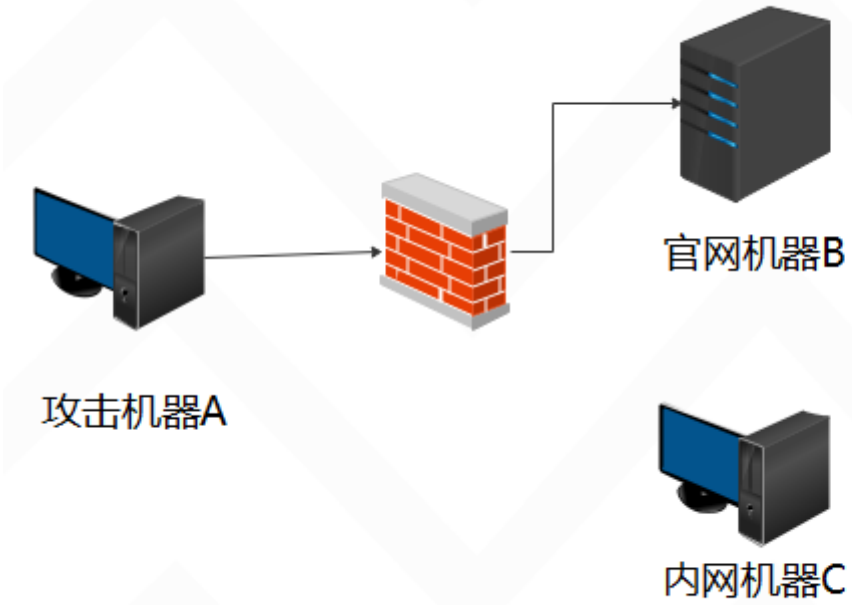
NETSH介绍

netsh是windows系统自带命令行程序，攻击者无需上传第三方工具即可利用netsh程序可进行端口转发操作，可将内网中其他服务器的端口转发至本地访问运行这个工具需要管理员的权限

```
C:\>netsh /?

用法: netsh [-a AliasFile] [-c Context] [-r RemoteMachine] [-u [DomainName\]UserName] [-p Password | *]
            [Command | -f ScriptFile]

下列指令有效:

此上下文中的命令:
?               - 显示命令列表。
add             - 在项目列表上添加一个配置项目。
advfirewall     - 更改到 'netsh advfirewall' 上下文。
bridge          - 更改到 'netsh bridge' 上下文。
delete          - 在项目列表上删除一个配置项目。
dhcpclient      - 更改到 'netsh dhcpclient' 上下文。
dnsclient       - 更改到 'netsh dnsclient' 上下文。
dump            - 显示一个配置脚本。
exec            - 运行一个脚本文件。
firewall        - 更改到 'netsh firewall' 上下文。
help            - 显示命令列表。
http            - 更改到 'netsh http' 上下文。
interface       - 更改到 'netsh interface' 上下文。
ipsec           - 更改到 'netsh ipsec' 上下文。
lan             - 更改到 'netsh lan' 上下文。
mbn             - 更改到 'netsh mbn' 上下文。
namespace       - 更改到 'netsh namespace' 上下文。
netio           - 更改到 'netsh netio' 上下文。
nlm             - 更改到 'netsh nlm' 上下文。
p2p             - 更改到 'netsh p2p' 上下文。
ras             - 更改到 'netsh ras' 上下文。
rpc             - 更改到 'netsh rpc' 上下文。
set             - 更新配置设置。
show            - 显示信息。
trace           - 更改到 'netsh trace' 上下文。
wcn             - 更改到 'netsh wcn' 上下文。
wfp             - 更改到 'netsh wfp' 上下文。
winhttp         - 更改到 'netsh winhttp' 上下文。
winsock         - 更改到 'netsh winsock' 上下文。
wlan            - 更改到 'netsh wlan' 上下文。

下列的子上下文可用:
 advfirewall bridge dhcpclient dnsclient firewall http interface ipsec lan mbn namespace netio nlm p2p ras rpc trace wcn wfp winhttp winsock wlan

若需要命令的更多帮助信息，请键入命令，接着是空格，
后面跟 ?。
```

实验场景

现在有如下的网络，电脑A是攻击机器，可以直接访问电脑B,但是访问不了机器C,可以借助B机器上的netsh命令进行端口转发访问机器C，这里注意只能访问端口



机器信息

实验机器的信息如下：

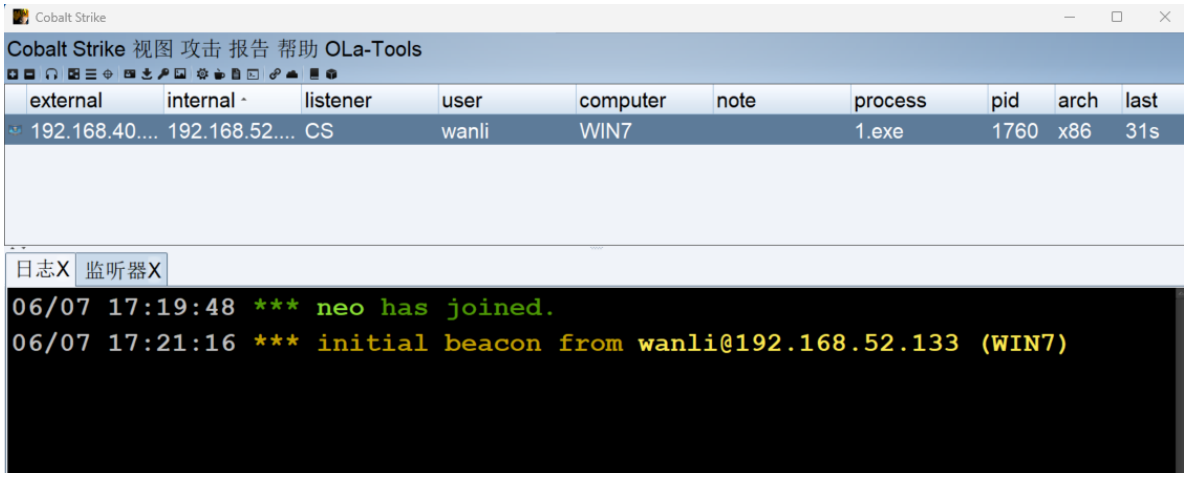
机器名字	机器IP	机器类型
攻击机器A	192.168.40.22	WIN11
官网机器B	192.168.41.231/192.168.52.133	WIN7
内网机器C	192.168.52.132	centos

网络情况如下：

```
A可以访问B
B可以访问C
A不能访问C
```

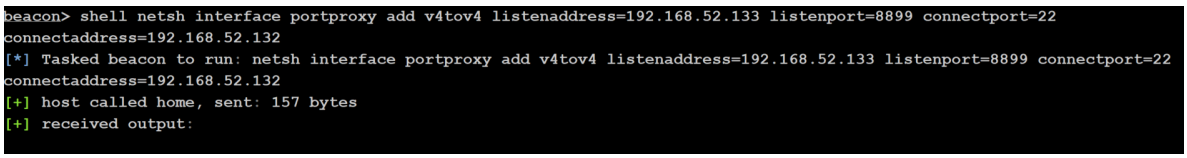
实验步骤

1、我们通过webshell或者CS远控对方电脑



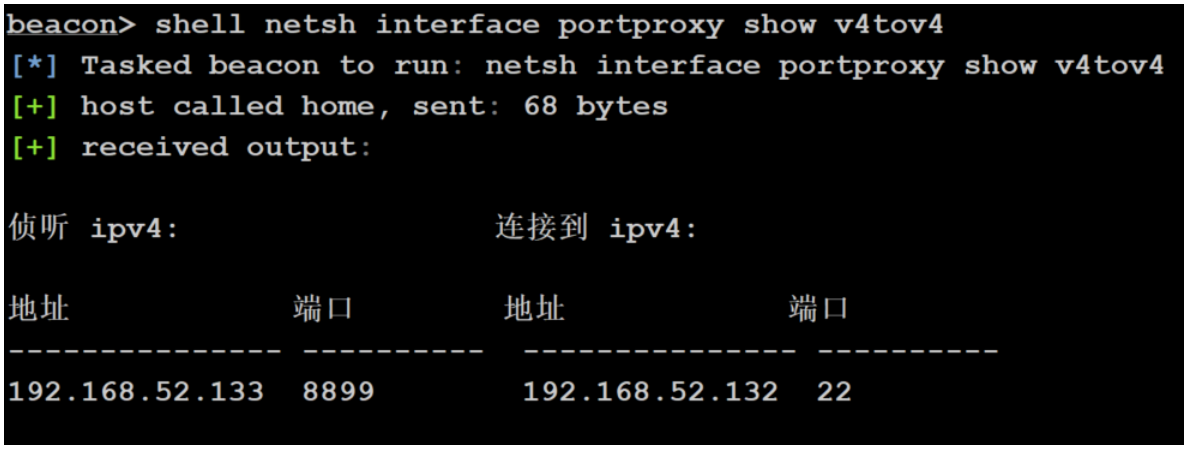
2、通过远控攻击在B上执行如下的命令（只有管理员才能执行哦）

```
netsh interface portproxy add v4tov4 listenaddress=192.168.41.213
listenport=9999 connectport=22 connectaddress=192.168.52.132
```



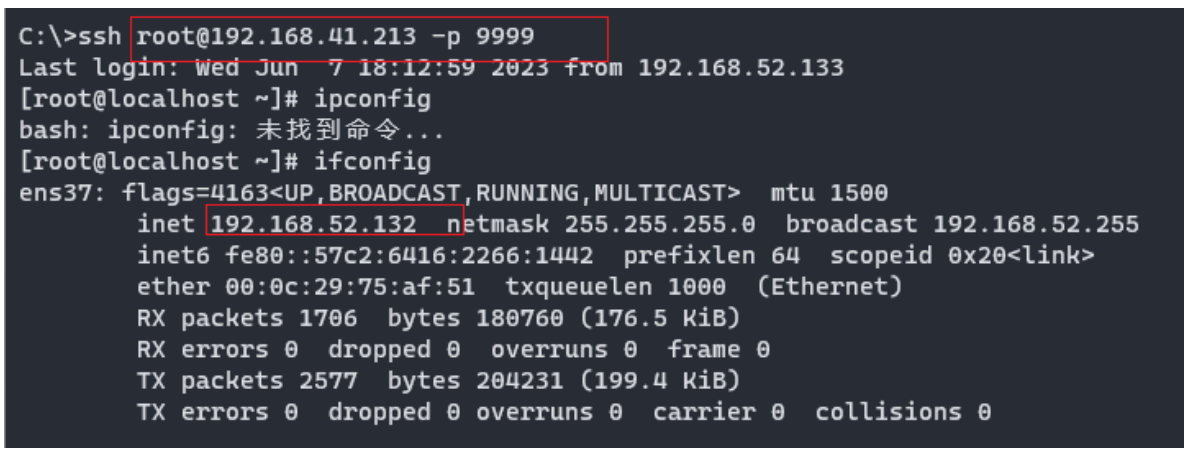
4、查看是否开启转发

```
netsh interface portproxy show v4tov4
```



5、在攻击机器A上运行连接靶机C的端口

```
ssh root@192.168.41.213 -p 9999
```



6、删除转发如下

```
netsh interface portproxy delete v4tov4 listenaddress=192.168.41.213
listenport=9999
```