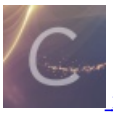
封神台靶场-第六章

原创

Mr H 于 2020-07-11 23:42:20 发布 736 收藏

分类专栏： 封神台-第六章 文章标签： 渗透测试靶场

本文链接：https://blog.csdn.net/Mr_helloword/article/details/107292259



第六章-SYSTEM！POWER！

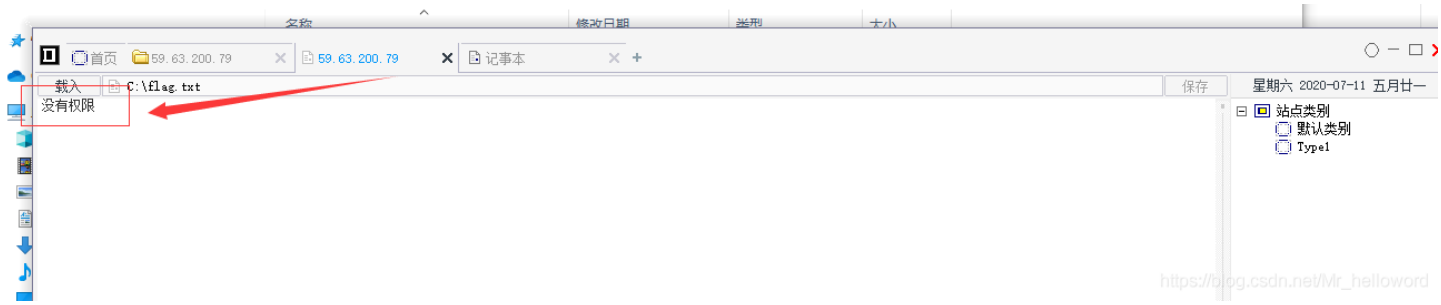
Tips:

1、提权！

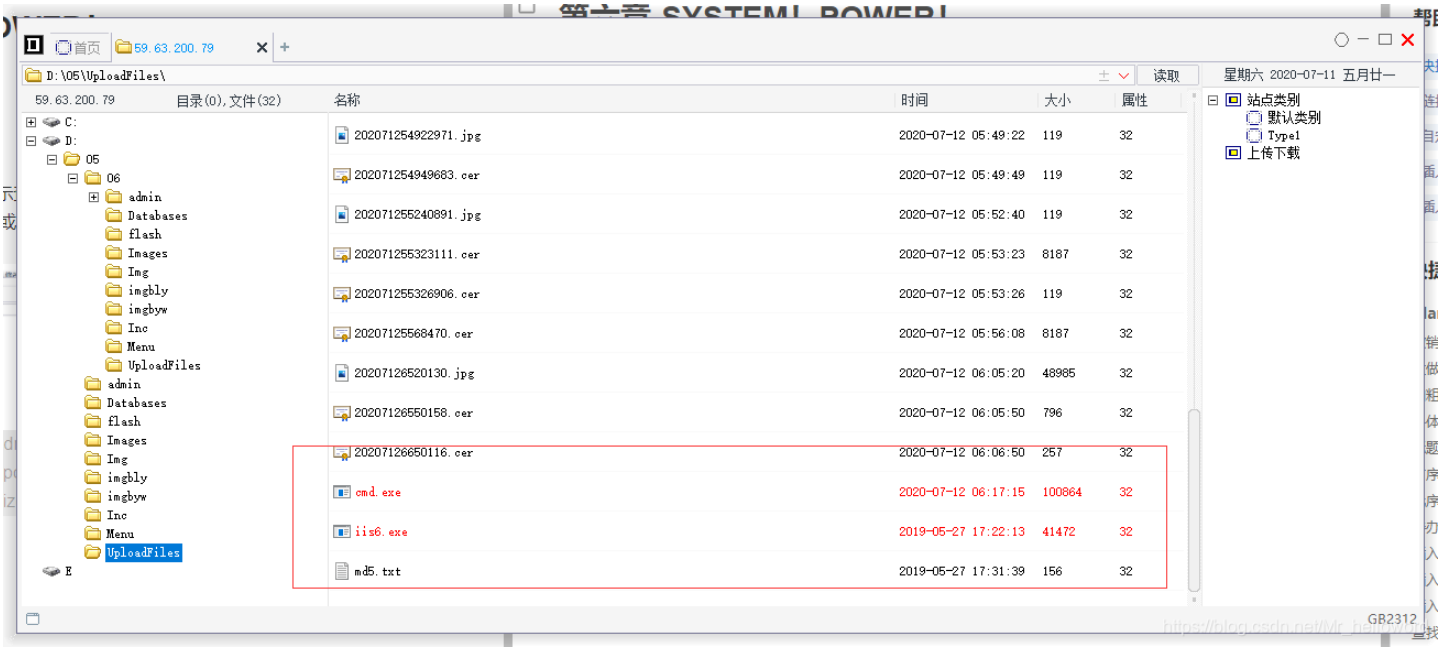
2、FLAG在C盘根目录下！

1.在第五章的基础上用菜刀连接，根据提示查看flag，发现没有权限，这里想到提权，这是本章重点（

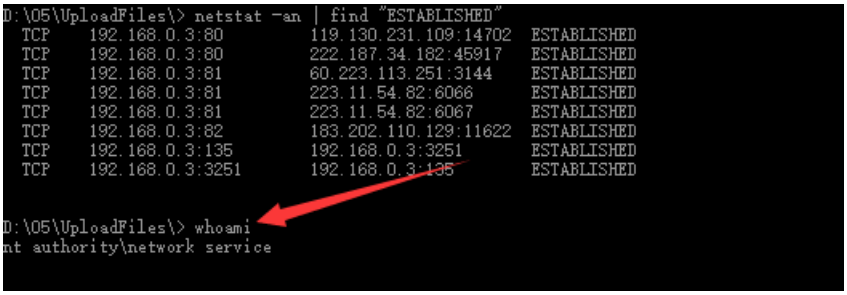
注：如果中途出现掉线，重新连接菜刀，或重新上传木马连接）



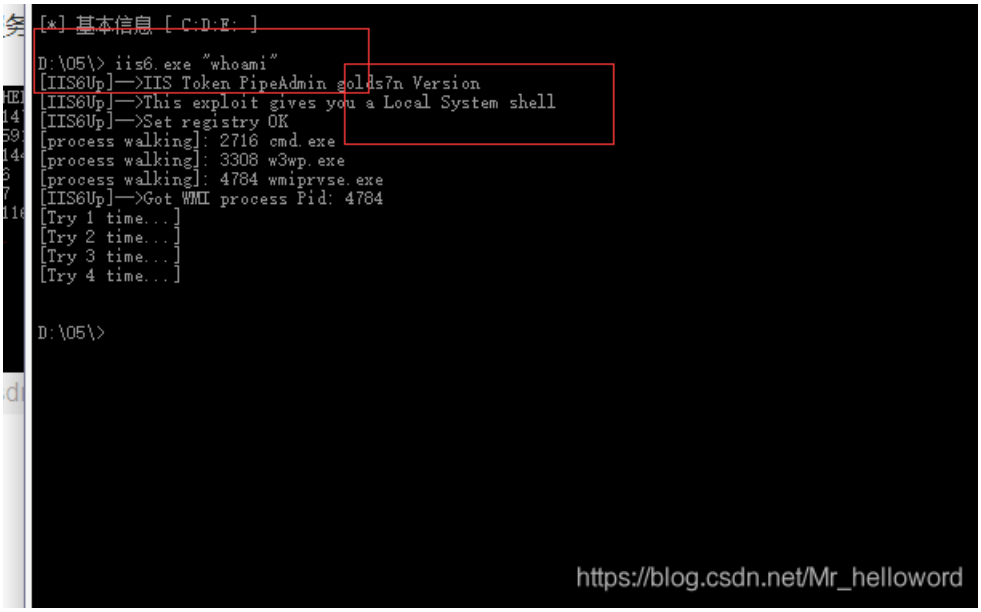
2.上传cmd.exe,iis6.exe文件（在upfile这里上传这俩个文件）



3.打开cmd命令，想法：创建管理员组新用户成员，奈何权限低。
whoami查看当前用户：发现为web应用服务组成员，权限低

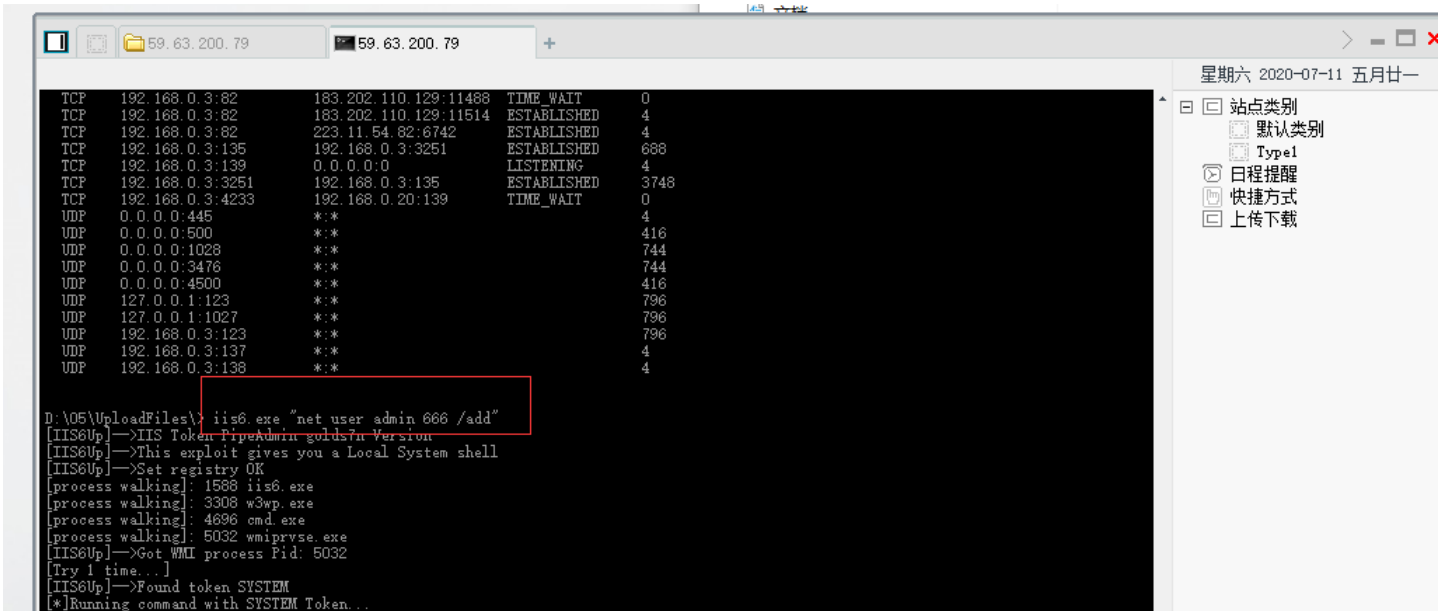


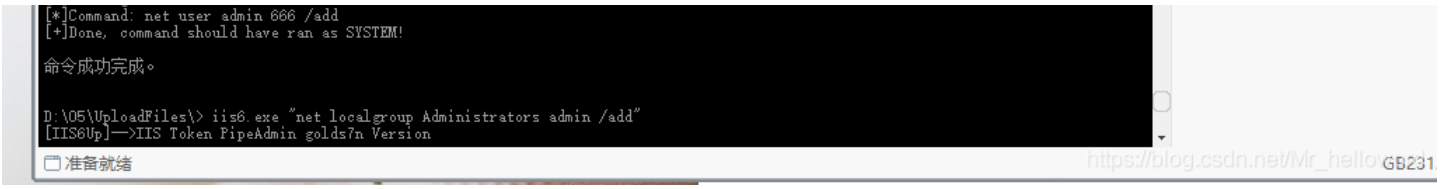
我们想到还有一个iis6，我们查看该用户发现为system权限：
命令：iis6.exe “whoami”

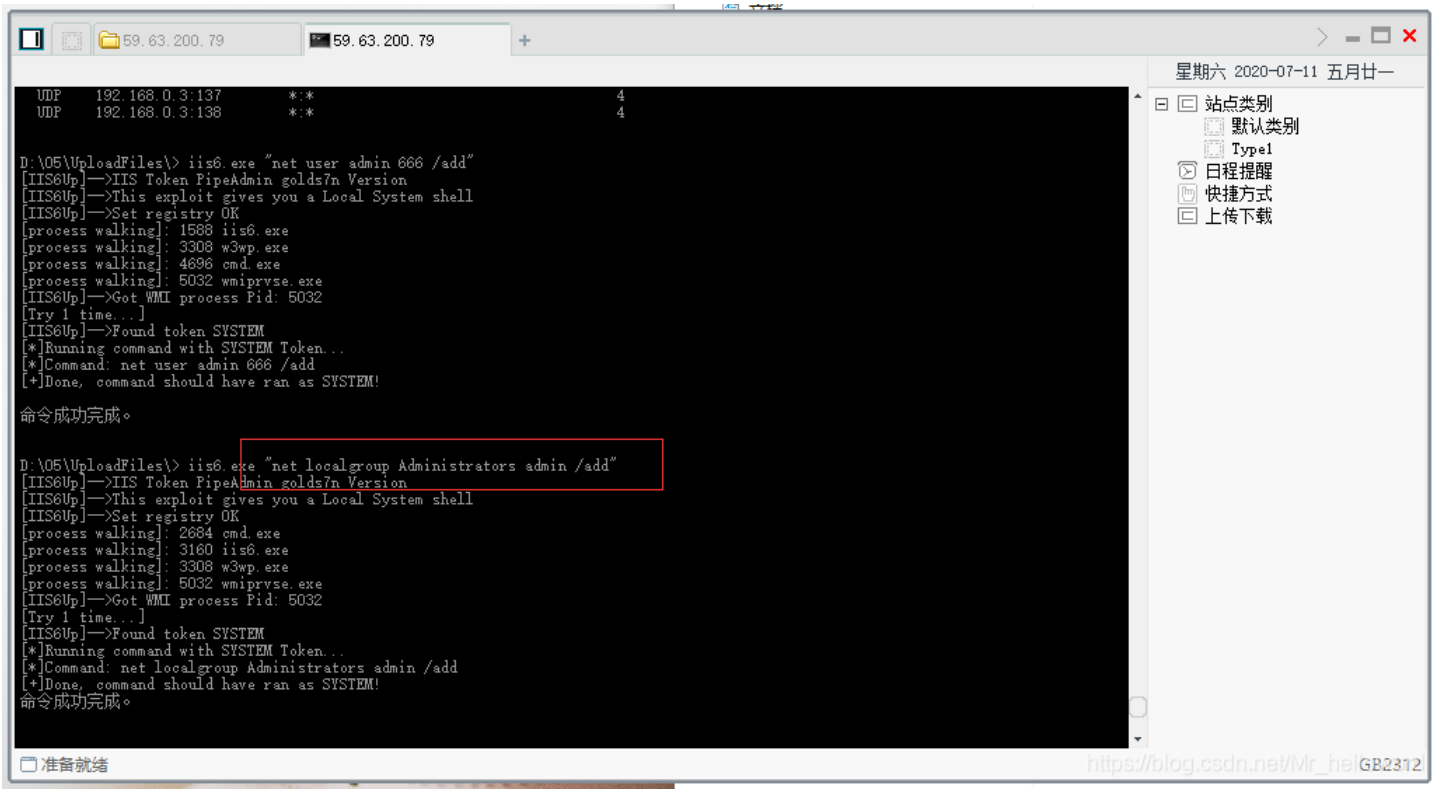


4.利用iis6desystem权限创建新用户，加入Administrators组：

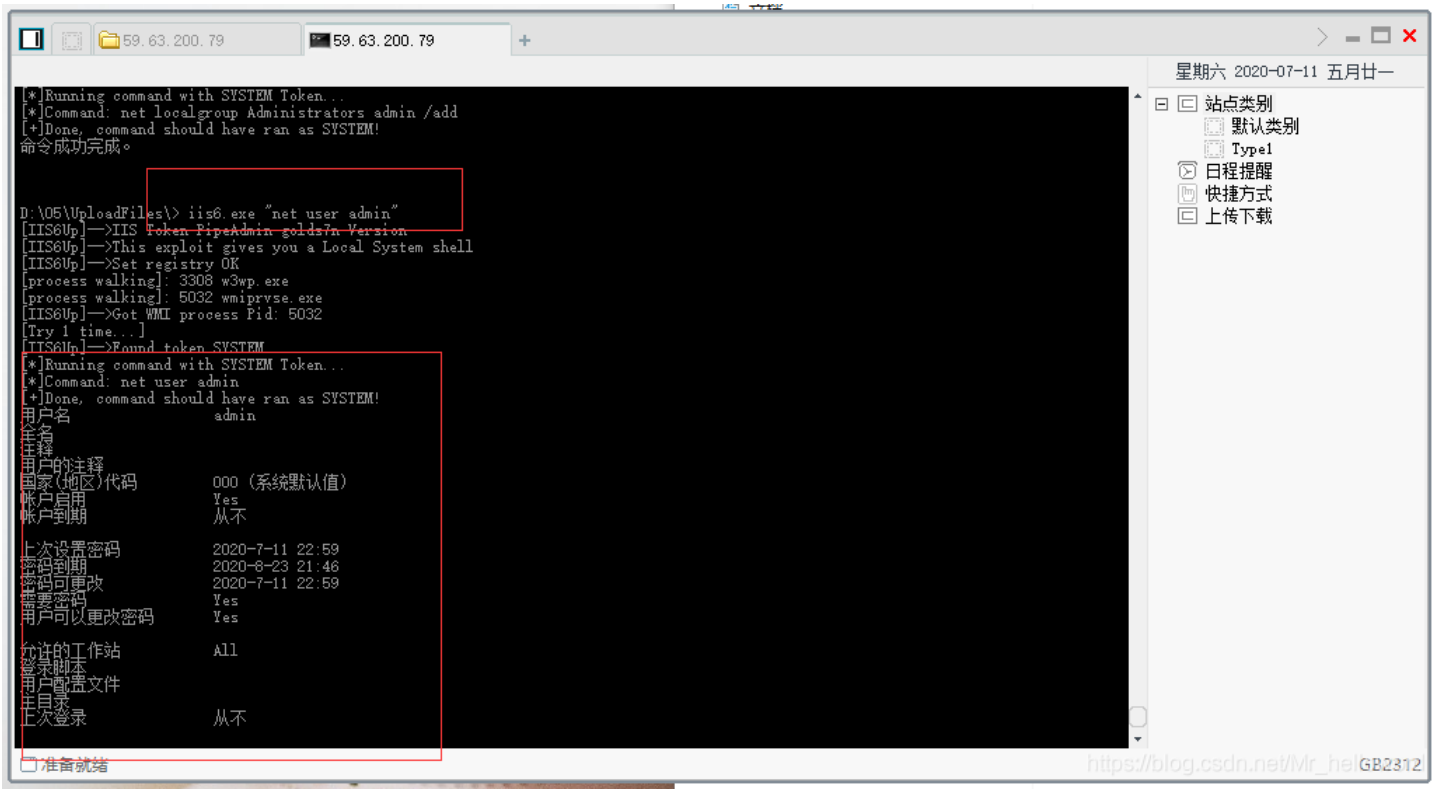
```
iis6.exe "net user admin 666 /add"
iis6.exe "net localgroup Administrators admin /add"
```





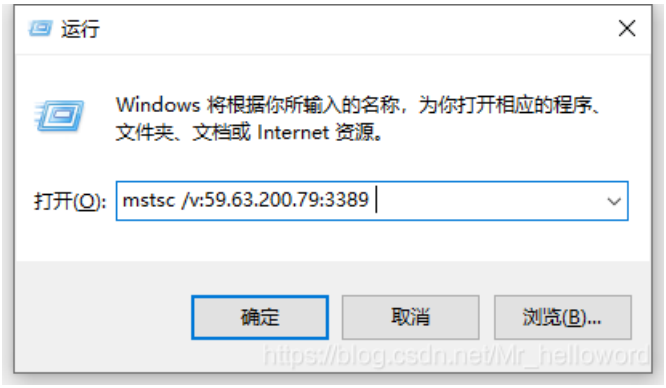


如下表示已经成为管理员用户



5.这里想着进行远程登陆，远程登陆的端口号默认为3389我们尝试登陆结果可以登陆（注:如果发现端口错误，不是3359，说明端口号被改了，我们可以通过第六点查看远程登陆端口号）

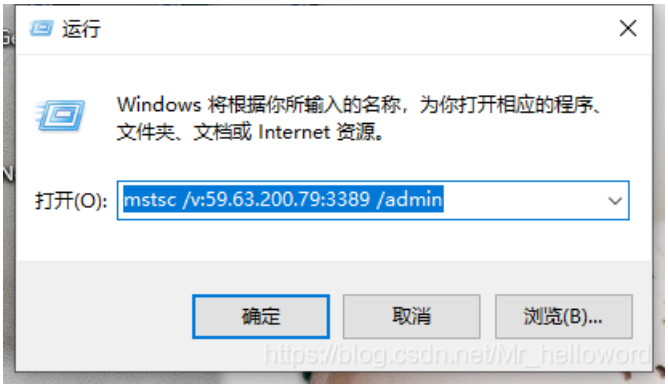
打开win的控制终端win+r



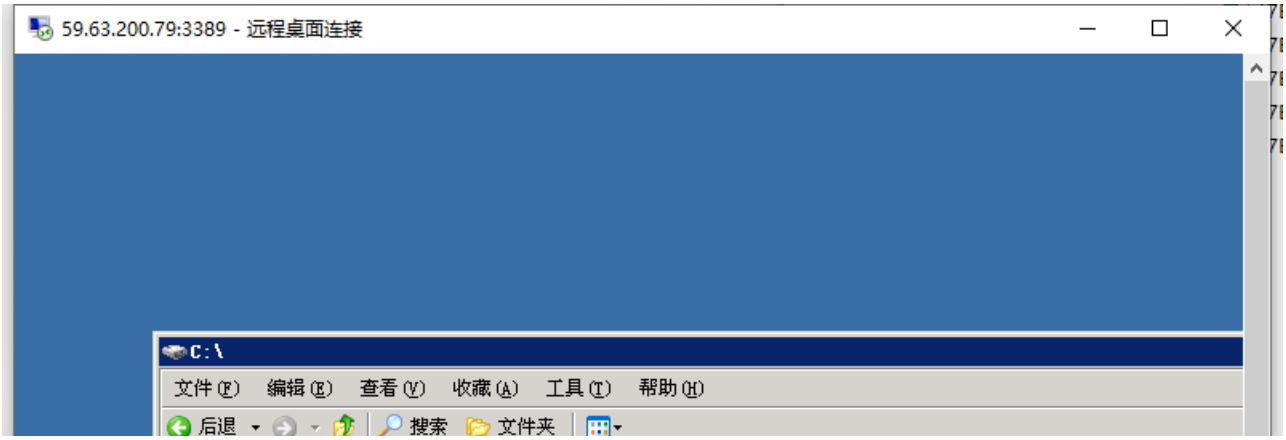
输入账号密码登陆发现新的新的困难又来了：服务中断由于很多人登陆靶场连接，登陆用户登陆后没有注销导致，在这里友情提示登陆后及时注销。最后办法总比困难多遇到问题可以多查查解决如下

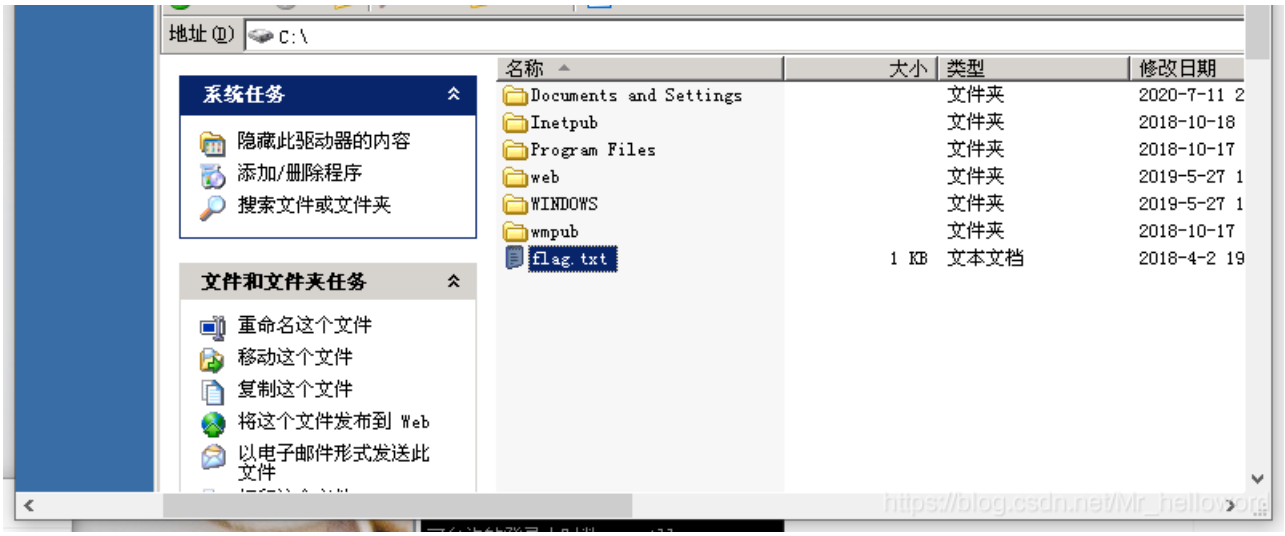
当出现这个问题的时候，解决方法要与您本地使用的操作系统有关系
如果您本地使用的是Windows XP、Windows 2008、Windows 7/8/8.1操作系统，那么在远程的时候在IP 后面添加参数 /admin 远程即可，（就是强制登陆）

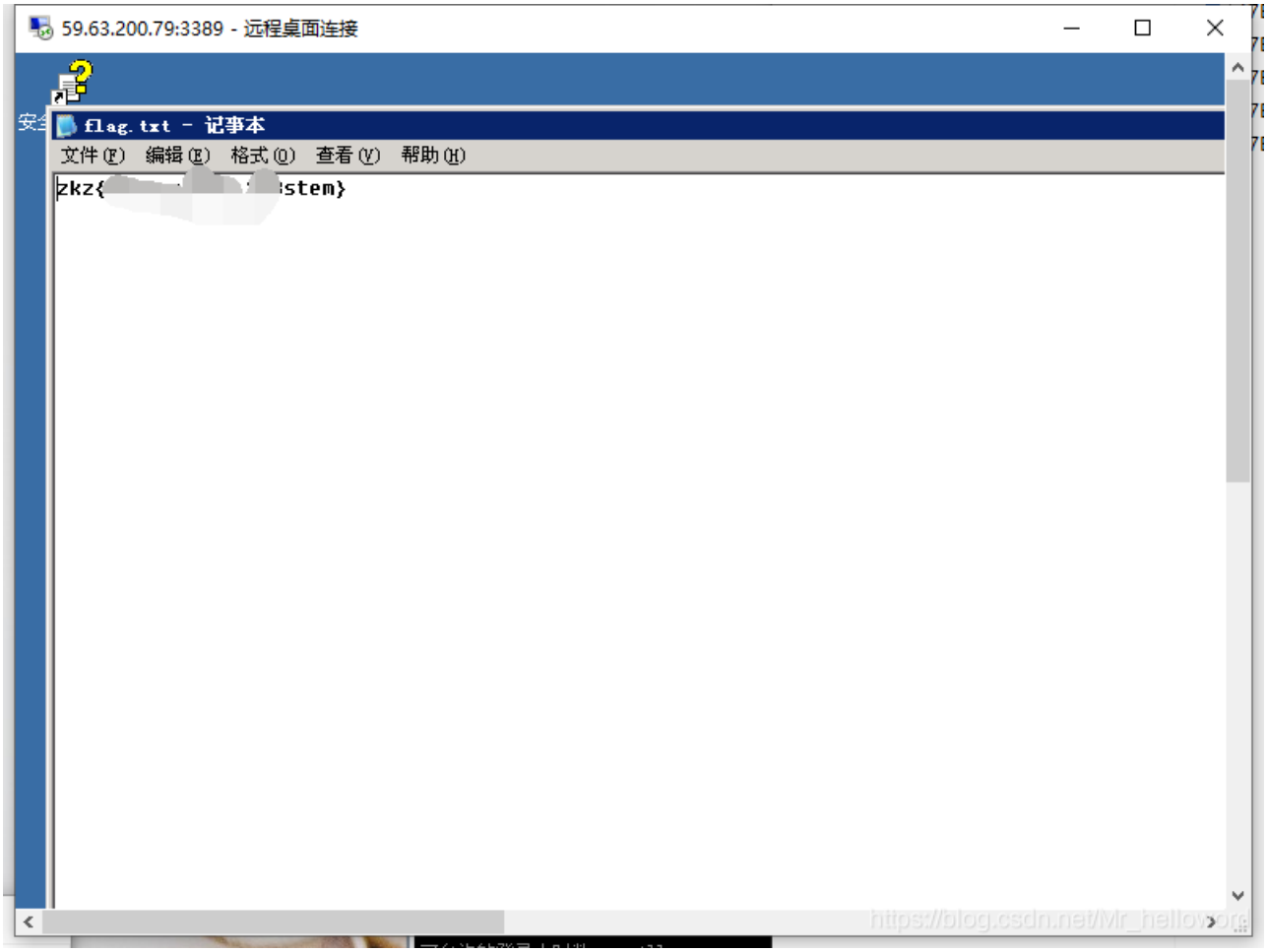
mstsc /v:59.63.200.79:3389 /admin



登陆查找flag







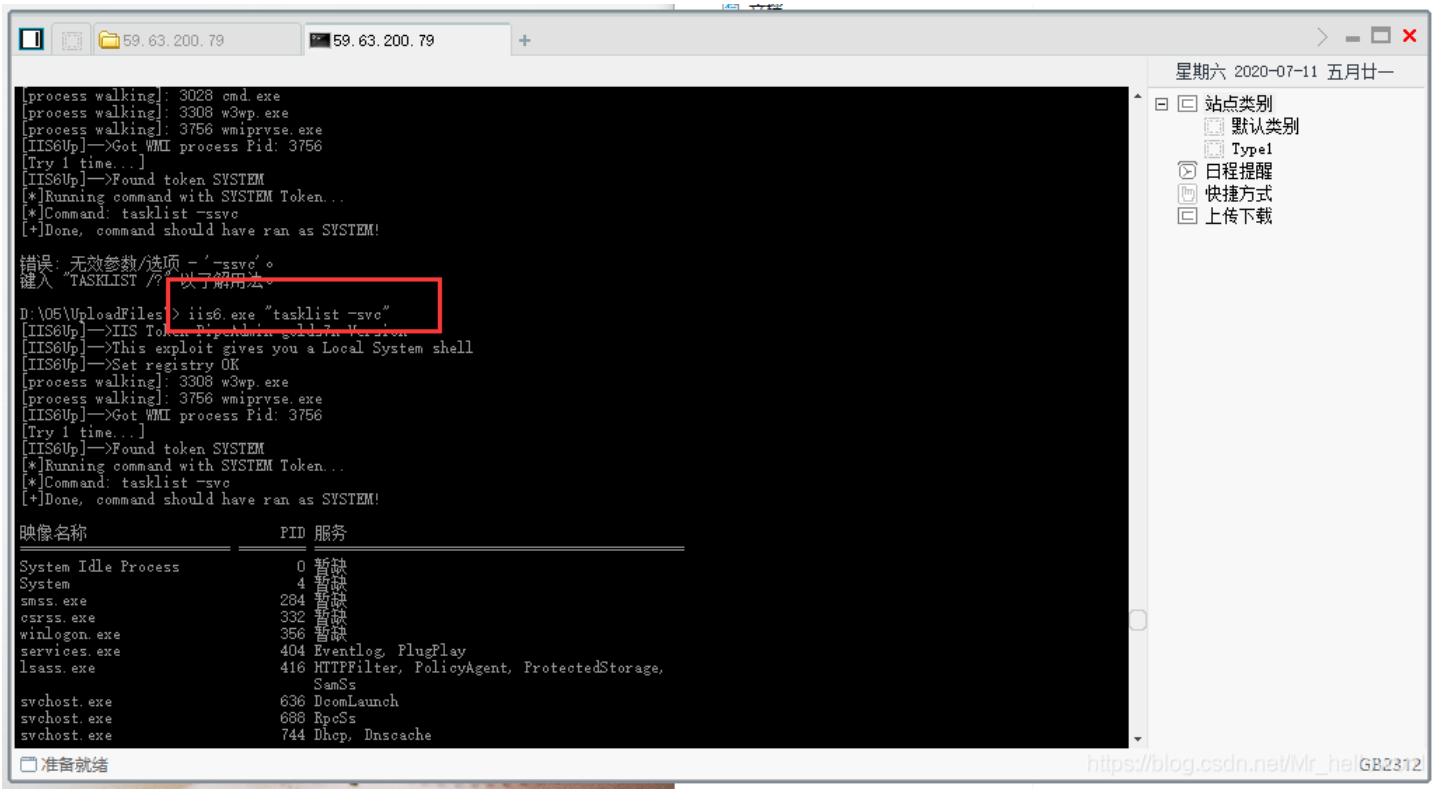
6.查找远程登陆端口号

思路：先查看进程-----找到远程登陆进程-----查找进程的pid------再根据pid查看端口号

```bash

```bash
iis6.exe "tasklist -svc"
iis6.exe "netstat -ano"
```
```

查找远程登陆进程的pid（TermService pid 2260）



根据进程号2260查看端口为3389