webshell控制目标：对服务器进行提权以访问远程服务器

原创

Zeker62 于 2021-08-03 10:00:06 发布 71 收藏 1

分类专栏： 网络安全学习 文章标签： 安全 数据库 web

什么是提权

提权是提取/提高权限的意思
一般作为访问者，权限比较低，需要提高权限进一步操作。
最想拥有的是管理员的权限。

提权原理：

访问服务器的时候，直接访问一般权限很低。
这个时候我们可以通过一些权限比较高的软件/用户/进程等来操作我们的账户，让我们账户的权限提高。

EXP和POC

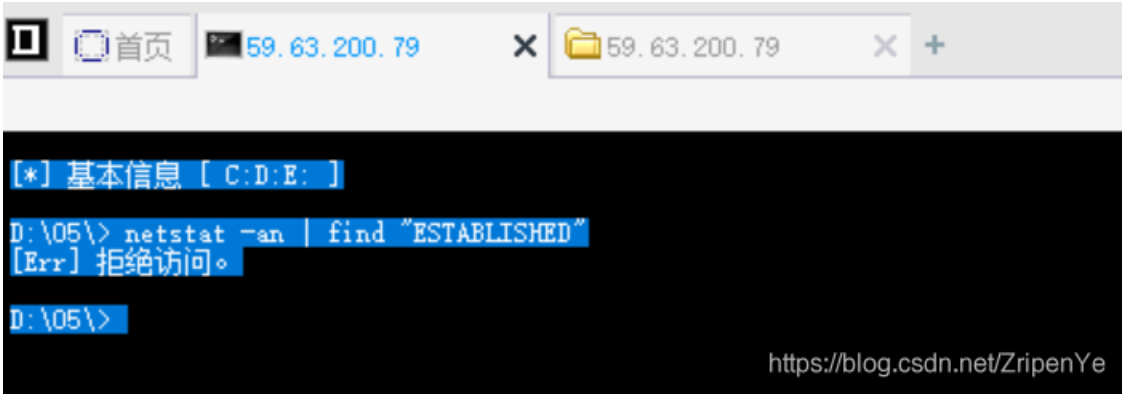
- exp：是指漏洞可以利用代码，运行后直接利用相应的漏洞
- poc：是指漏洞可以验证代码，检测是否存在漏洞。

提权过程

靶场：封神台：https://hack.zkaq.cn/battle/target?id=3eb7bec4a7e95297

在一句话木马进行完成之后：https://blog.csdn.net/ZripenYe/article/details/119189996

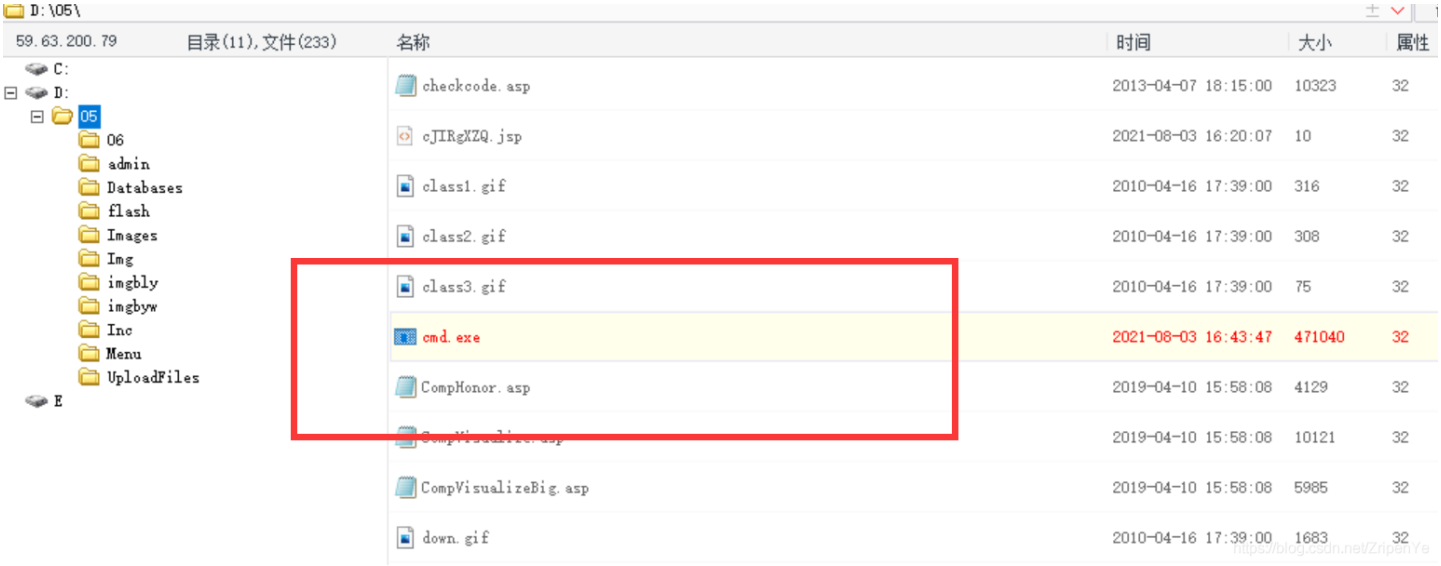
我们发现，单纯地使用cmd是没有权限的，因为我们此时是作为访问者访问对方服务器。



不论输入什么都是拒绝访问，这个时候就需要提权了。

因为cmd是存在于C:\Windows\system32，这是个系统盘，没有较高的权限是无法使用cmd的。

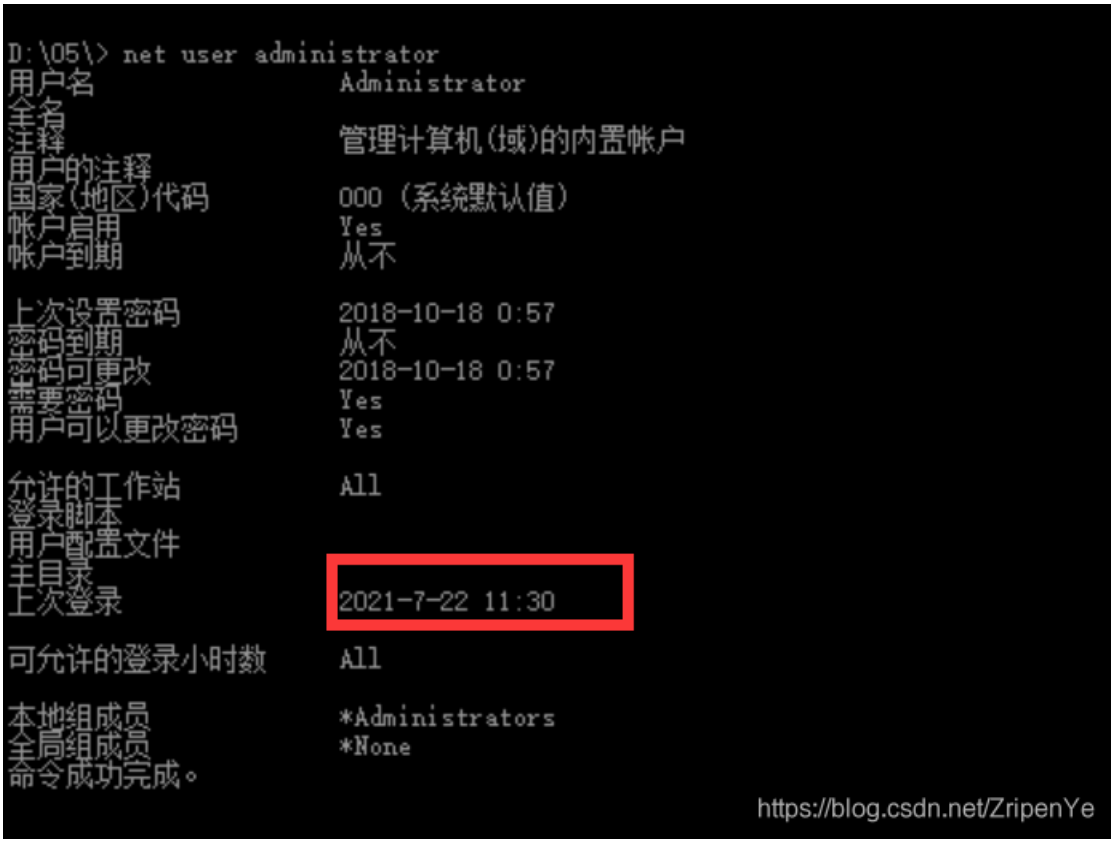
我们可以在我们可以操作的d盘里面放一个cmd，通过这个cmd，我们就可以操作了。



都可以进行相应的操作

查看管理员的信息

看一下管理员账户的信息，重点关注一下上次登录：
如果上次登录的时间离现在较为接近，建议快跑

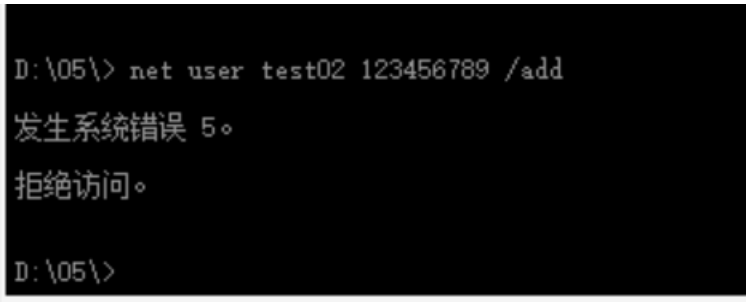


使用exp进行账户添加

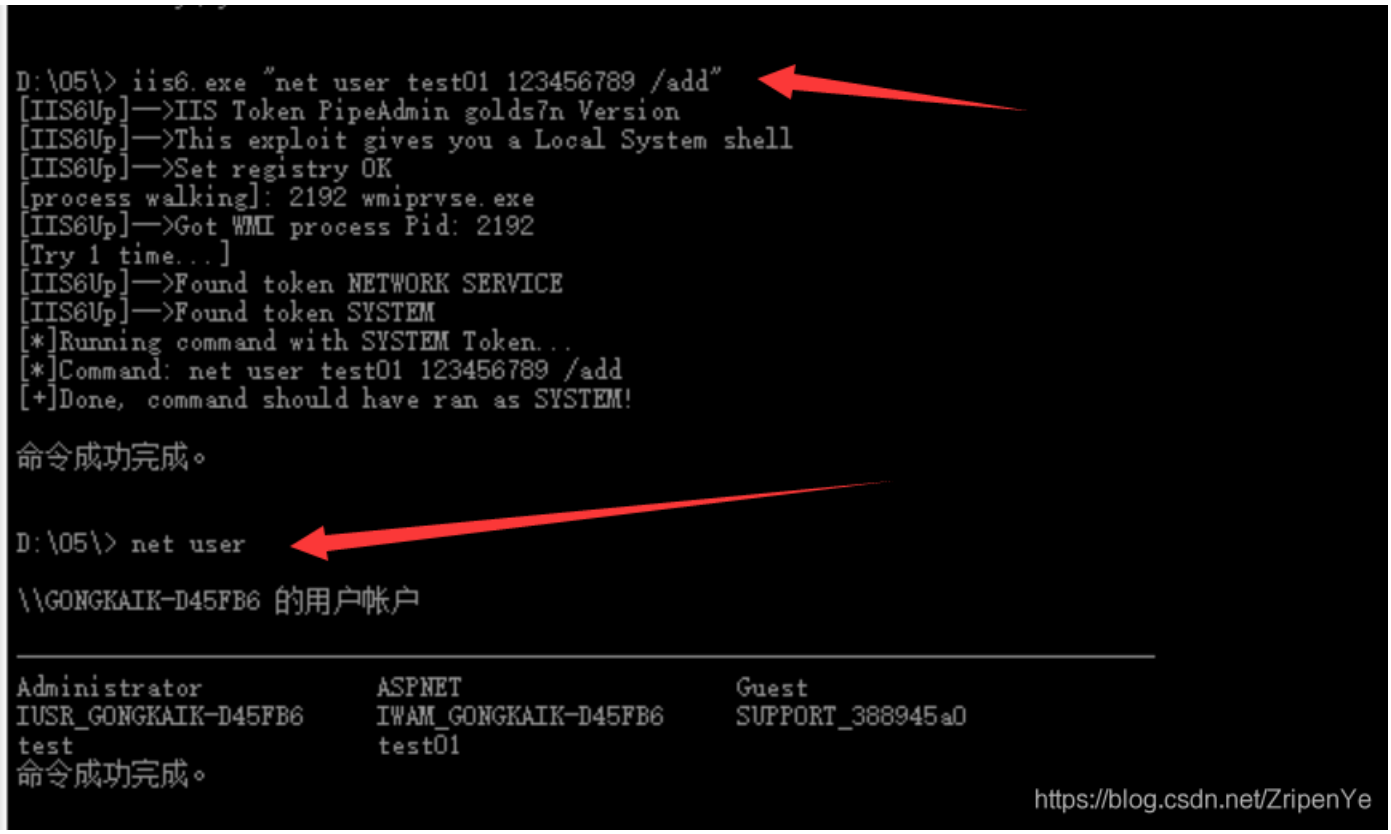
在文件下方有一个iis6的exe文件，这是一个exp文件，使用这个文件，我们可以利用相应的漏洞进行账户的操作，而我们并不需要知道是什么漏洞以及原理，直接使用工具就可以了。

可以看见，我们通过iis6这个软件可以更加清楚地看见一些信息

尝试添加账户，先来普通版的

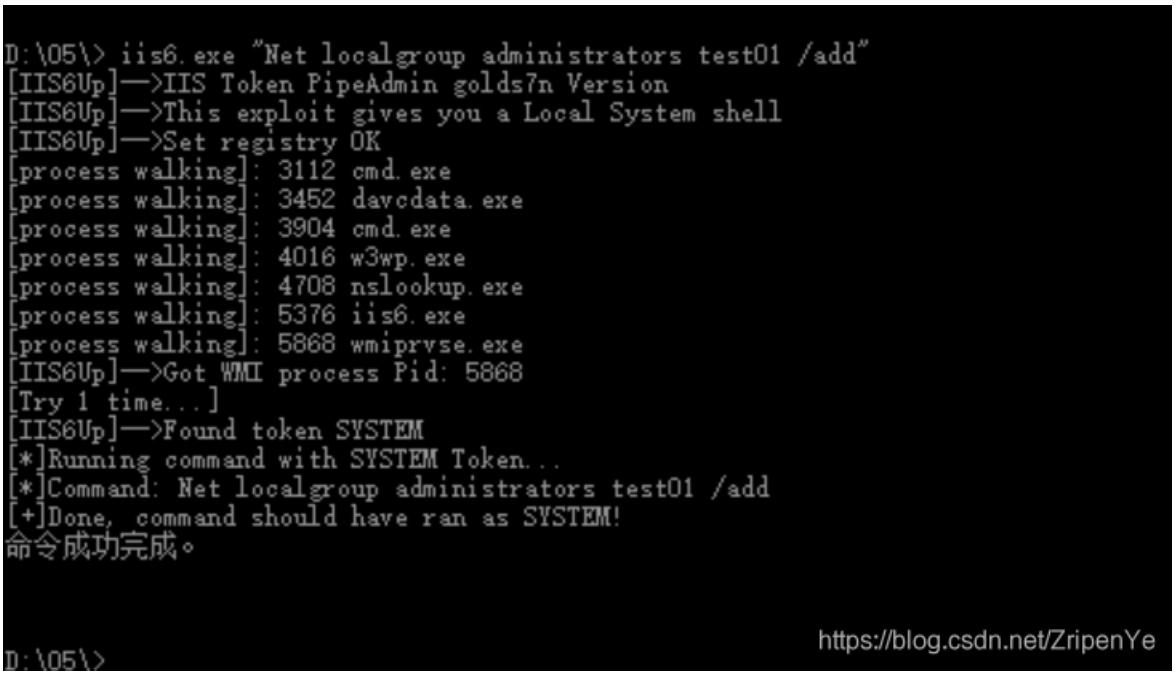


果然不允许，所以我们使用iis06试试看



成功

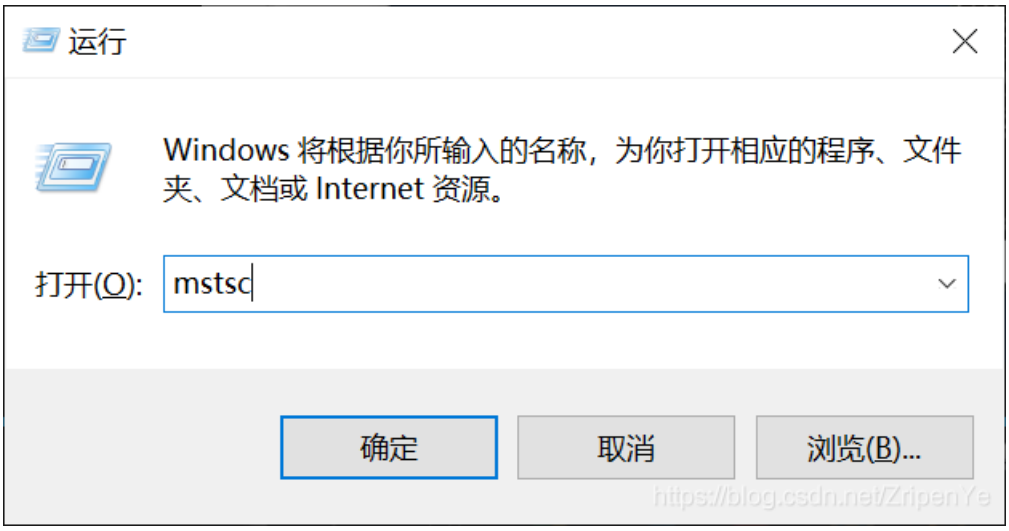
此时的权限还不够，这样并不是管理员的权限，我们需要更高的权限，执行指令：Net localgroup administrators 用户名 /add



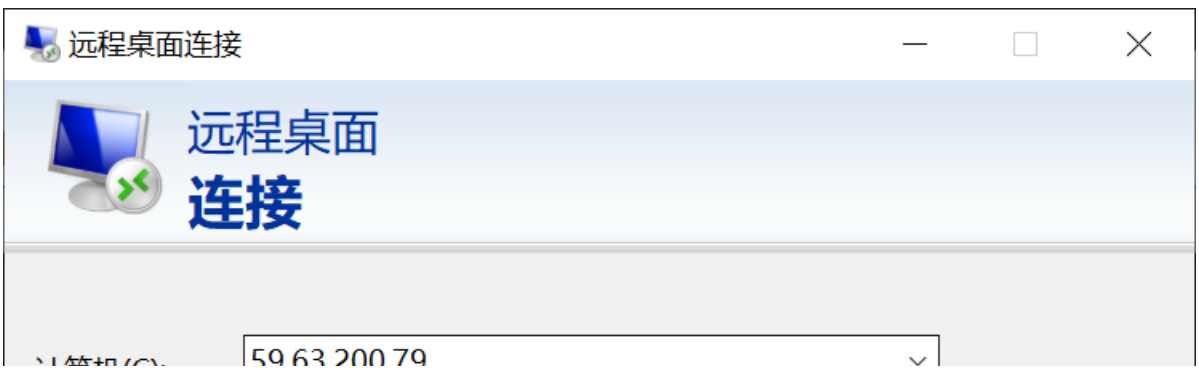
成功

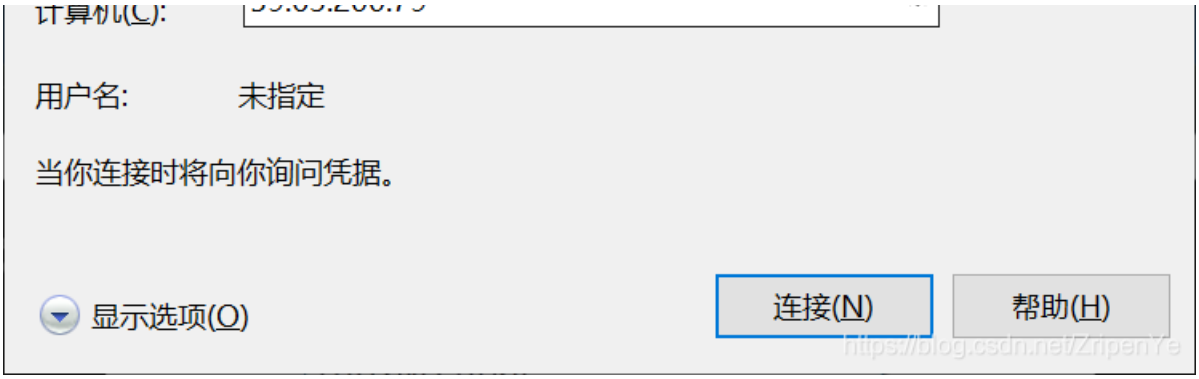
尝试远程访问桌面

远程桌面：

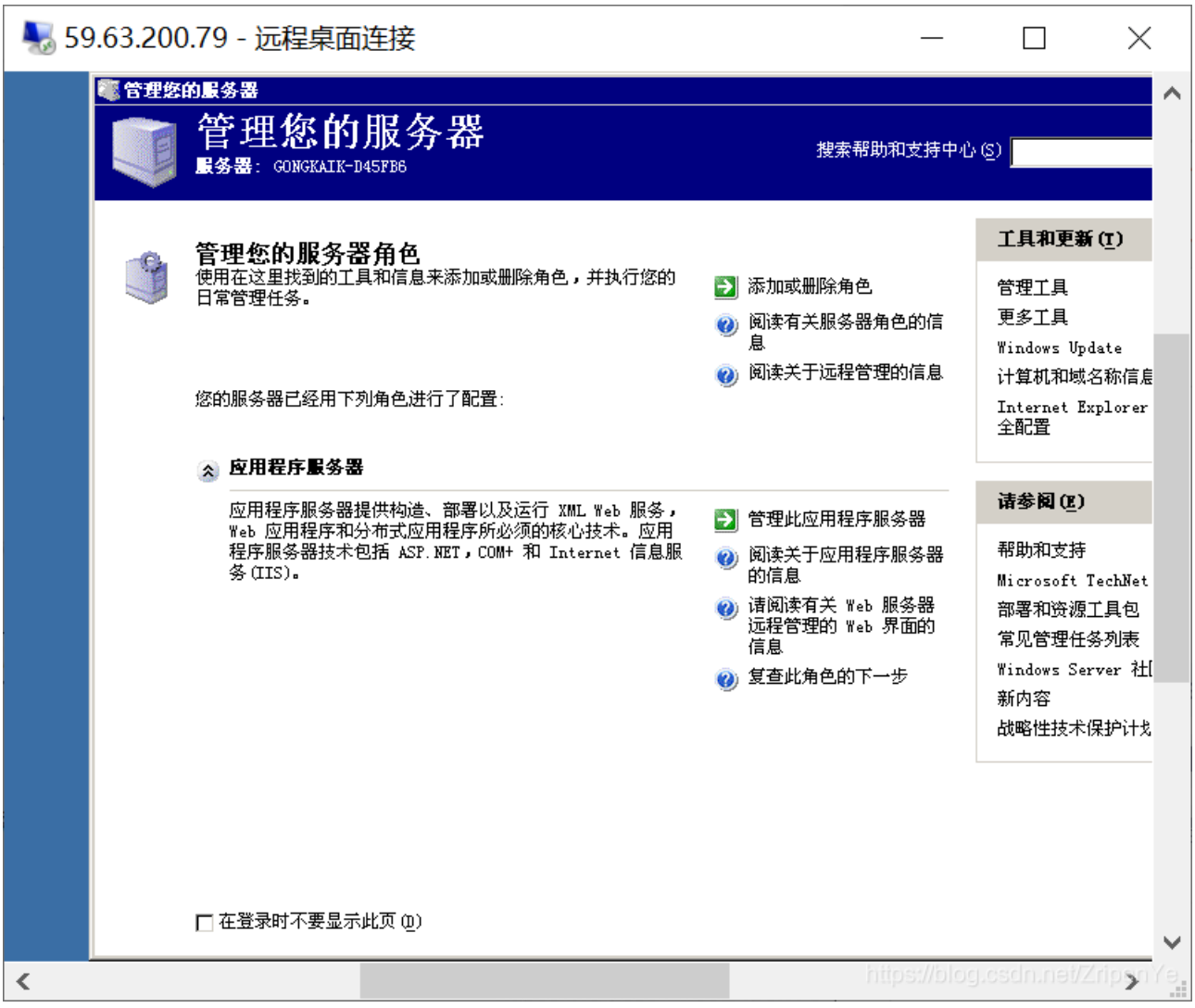


直接输入IP地址

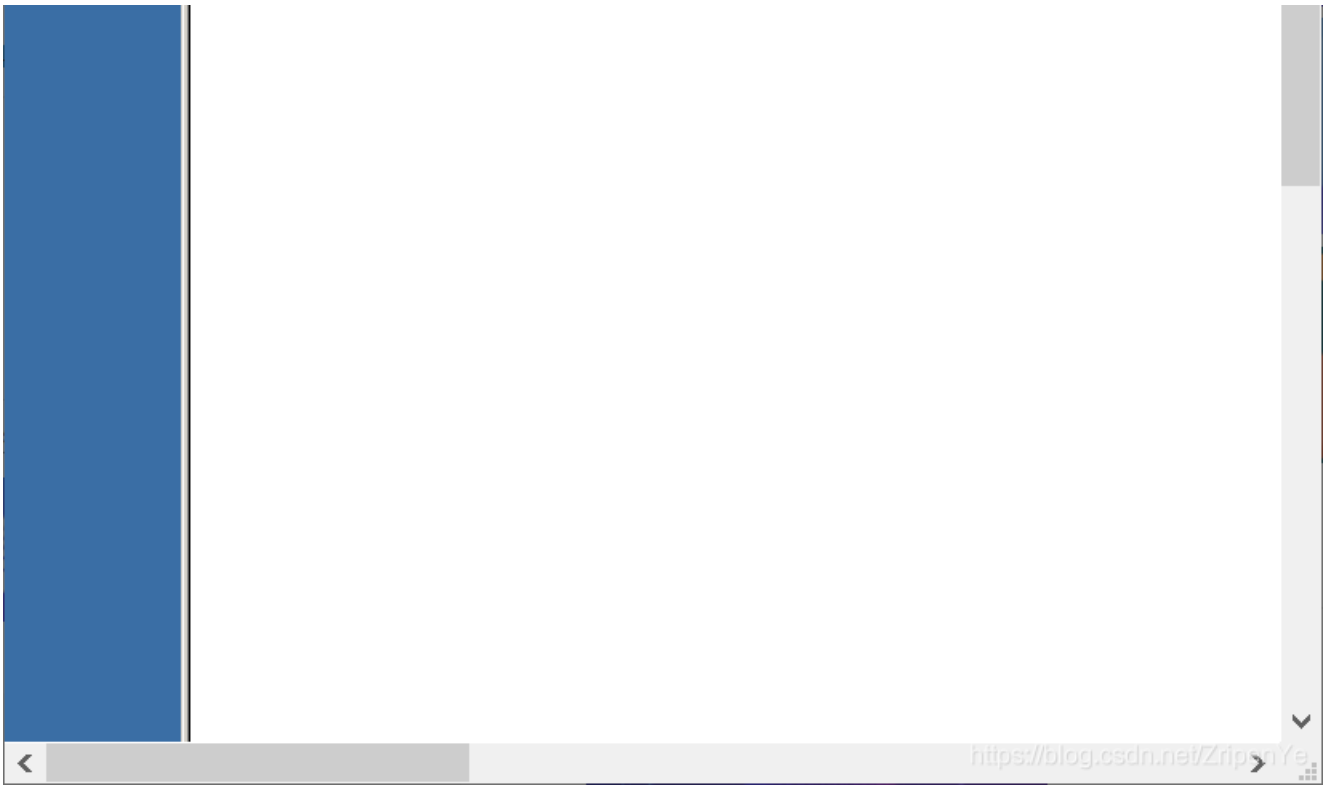




进入服务器



甚至在C盘里可以直接找到flag


https://blog.csdn.net/ZripenYe