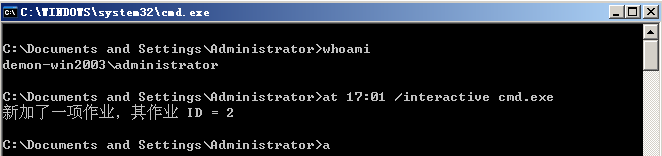
# 获取system用户权限

system用户是windows系统最顶端的权限，能做一些administrator用户做不了的操作，但不完全包括了administrator所拥有的权限，有少部分操作也是无法执行的，system用户一般用于去运行一些比较关键的进程，比如winlogon，conhost，svchost等关键进程。下面演示一些工具和命令来获取system用户的权限，也就是进入到上帝模式。

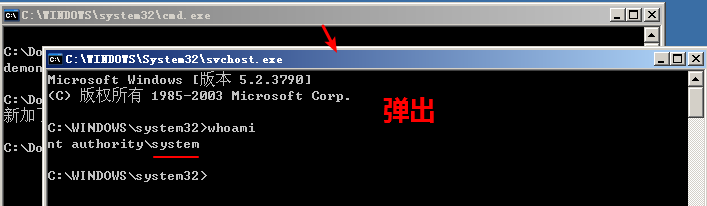
## 一，使用at命令提权

在用户administrator下运行at 命令，该命令在触发执行的时候是以system用户去运行。

at 17:01 /interactive cmd.exe

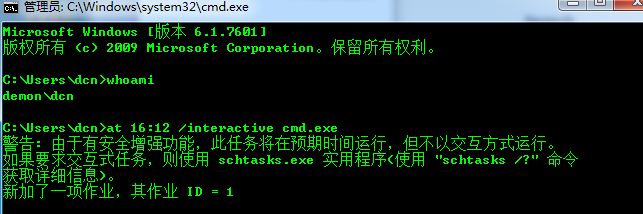


时间到了后就会以system用户弹出cmd.exe，此时的用户就是system了



该方法只适合win2003和winXP 对于比较新的系统，会有安全增强型保护机制

schtasks.exe实在是太难用了，暂时还没有找到对应提权的方法

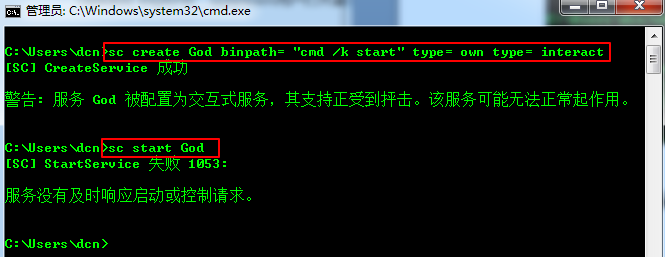


## 二，利用SC创建服务提权

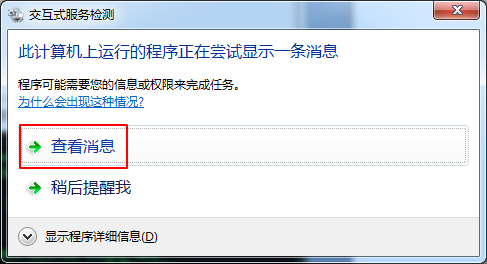
创建一个交互式任务，类型为自身，执行错误的任务，使得弹出交互式窗口进入Debug模式，Debug模式也是system用户来运行的，权限也比较高，注意命令等号后面有空格

sc create God binpath= "cmd /k start" type= own type= interact

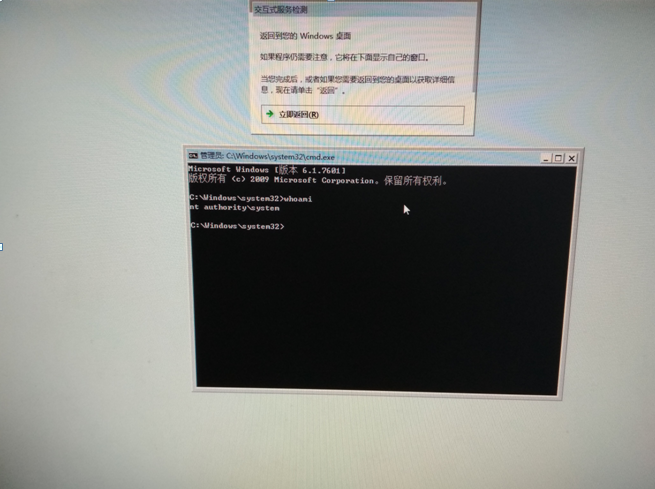
sc start God

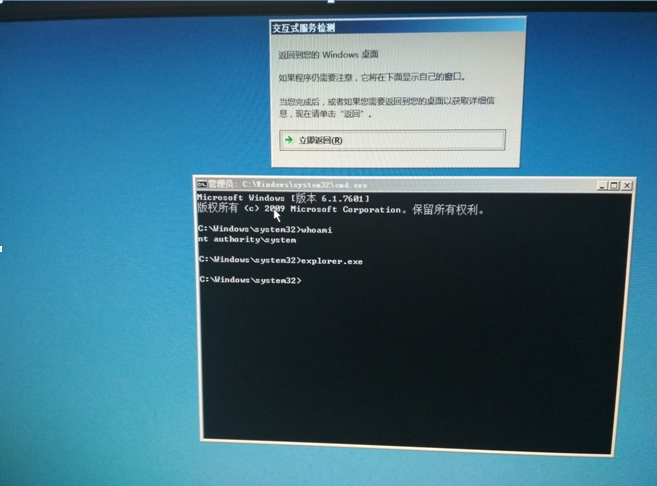


失败后会弹出是否进入Debug模式的框框，点查看消息就可以获得system权限了

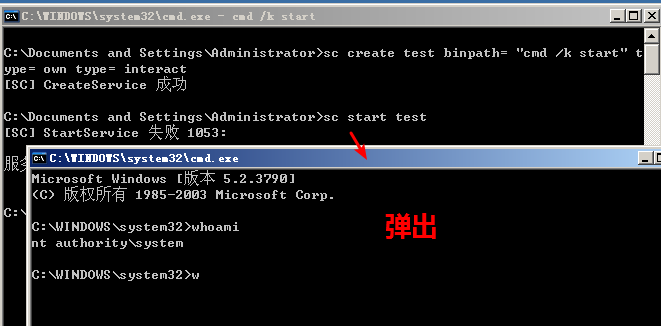


下面就是进入仙人模式的界面，虽然只是终端，也可以运行explorer.exe开启一个仙人桌面





该提权方式适合win7 和 xp及2k3 ，如果是2k3 直接弹出shell（system用户）



激活管理员的命令是：

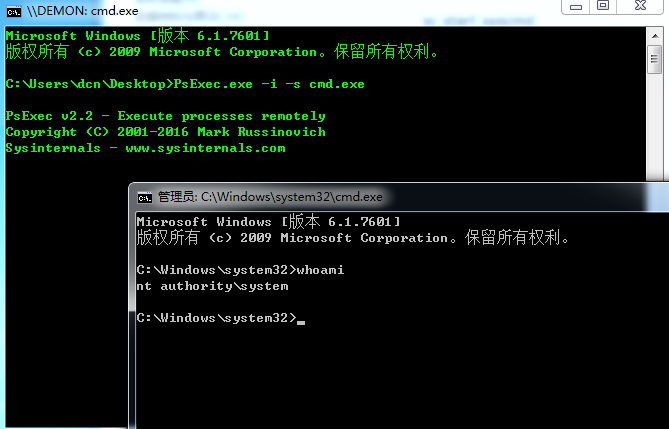
net user administrator /active:yes

## 三，利用工具提权

psExec工具，是Windows系统大牛 Mark Russinovich写的，他是工具包sysinternals里中的一个程序，下载地址：https://docs.microsoft.com/zh-cn/sysinternals/

将程序psExec.exe上传到目标机子上面即可，用法：

psExec.exe -i -s cmd.exe



pInjector.exe 注入工具

上面的psExec虽然可以提升权限，但是要是被其他用户在taskmgr上看到了，是可以杀的

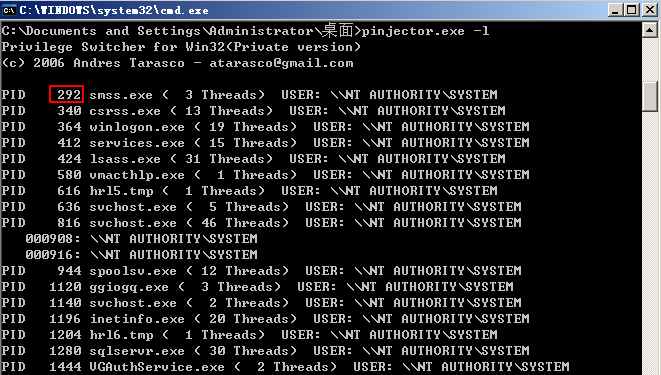
隐蔽性不怎么好，而pInjector.exe是直接注入到system用户运行的那些进程里头，隐蔽性很强，但是会被杀软给杀了。注入后会开启端口，可以从互联网上访问，可以说是后门了

http://www.tarasco.org/security/Process\_Injector

用法：

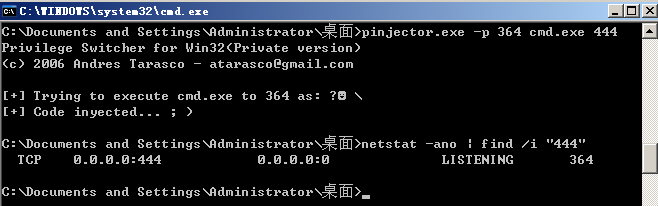
pInjector.exe -l 查看system用户所运行的进程及PID号

pInjector.exe -p 345 cmd.exe 444 注入进程345开启后门444端口

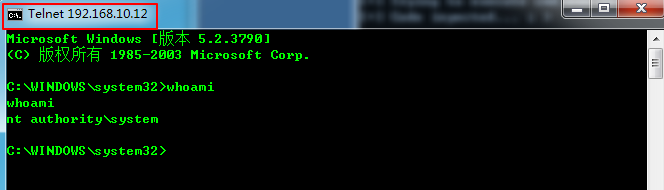


有一些进程可能因为空间太小无法注入，比如smss.exe





开启端口后可以使用telnet 连接，也是system 用户

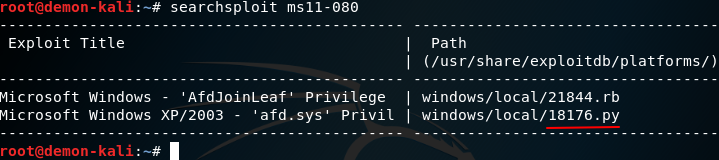


上面都是从administrator用户提权到system用户，下面则是普通用户提权到system用户

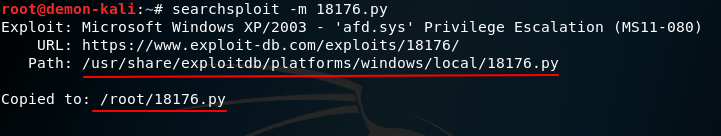
这个则需要利用系统漏洞来提权。

## 四，普通用户提权

利用微软的ms11-080漏洞来提权，在kali上可以通过searchsploit来搜寻漏洞号对应的py利用代码：searchsploit ms11-080



搜寻脚本位置：searchspoit -m  187176.py



但是我们不可能在目标机上安装py2.7的环境，所以我们需要把18176.py打包成exe文件

需要安装下面三个软件（windows下安装）：

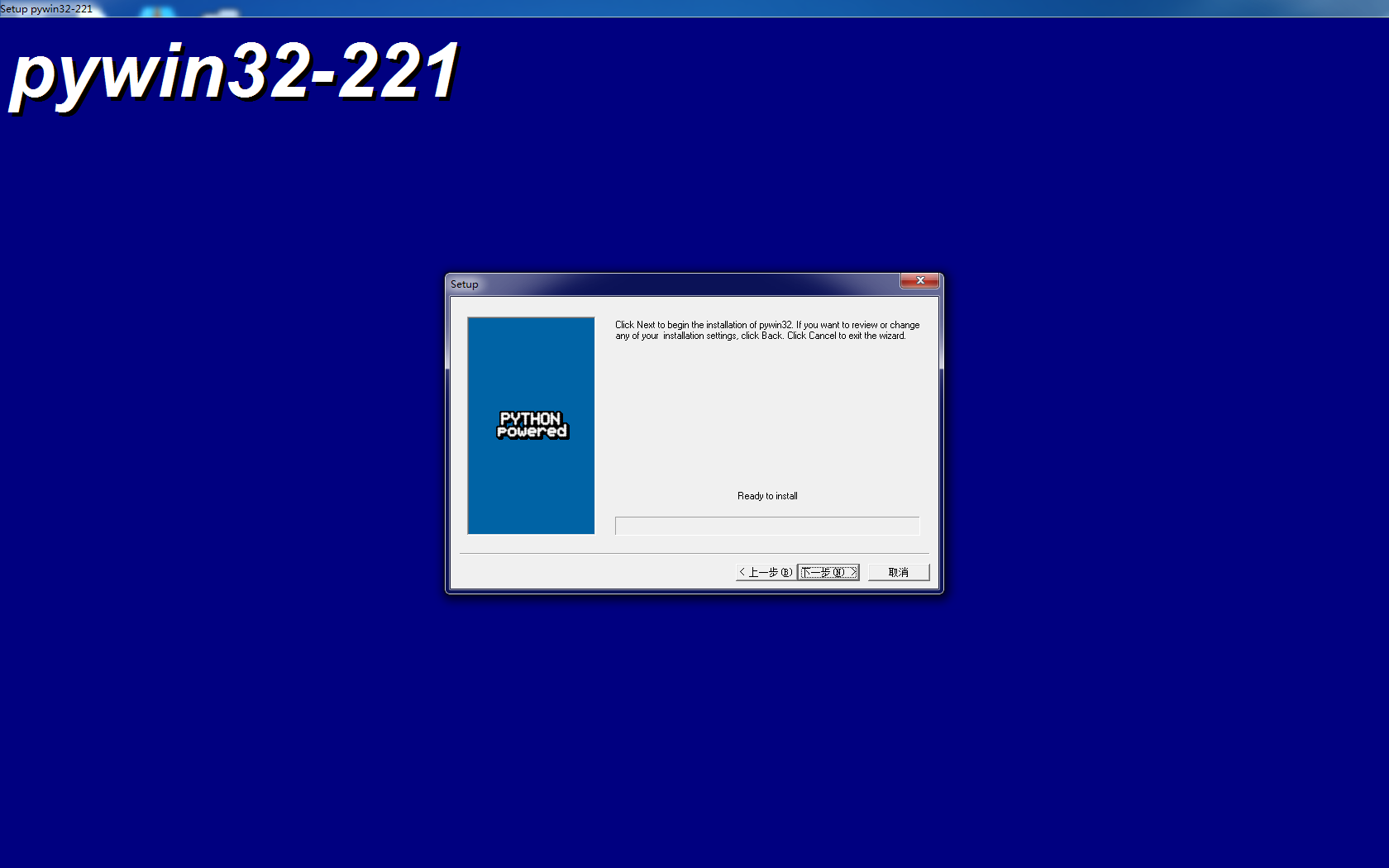
python2.7

pyinstaller.zip

pywin32-221.win32-py2.7.exe

安装好后把 18176.py 拖到windows系统的pyinstall目录

执行：python pyinstaller.py --onefile 18176.py 就会生成exe文件了



使用pyinstaller.py 的时候会缺少一些模块而终止，使用pip来安装这些模块

如果允许pip弹出无此命令则说明没有安装pip，如下：

1 先安装setuptools

   下载地址：https://pypi.python.org/pypi/setuptools#downloads

　将下载后的tar文件解压，用CMD模式进入到解压后的文件所在的目录执行命令：python setup.py install

2 安装pip

　下载地址：https://pypi.python.org/pypi/pip#downloads

   将下载后的tar文件解压，用CMD模式进入到解压后的文件所在的目录执行命令:python setup.py install

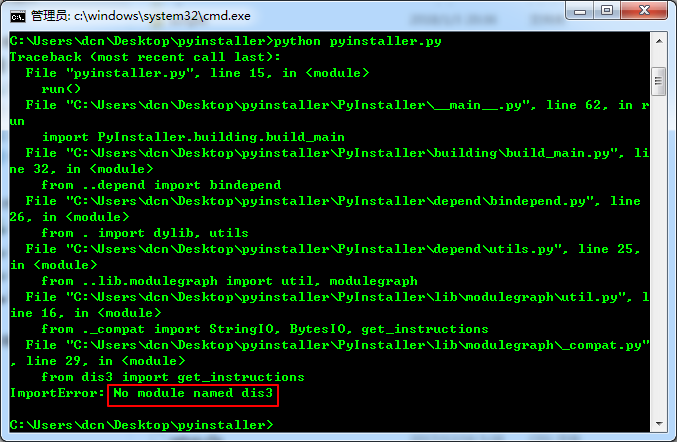
 安装完成，将python环境目录下的script路径添加到环境变量，就可以直接使用pip来运行命令了

安装好后将下面的模块使用pip来安装

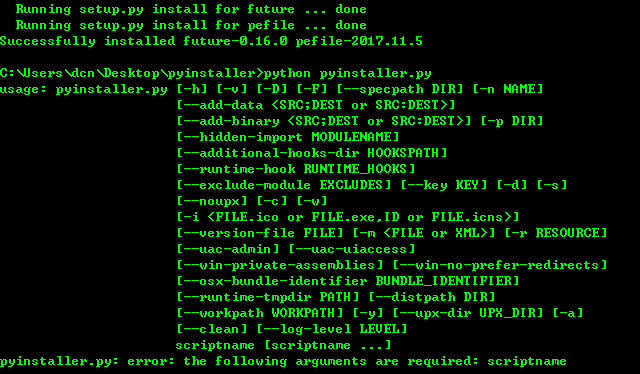
pip install dis3

pip install pypiwin32

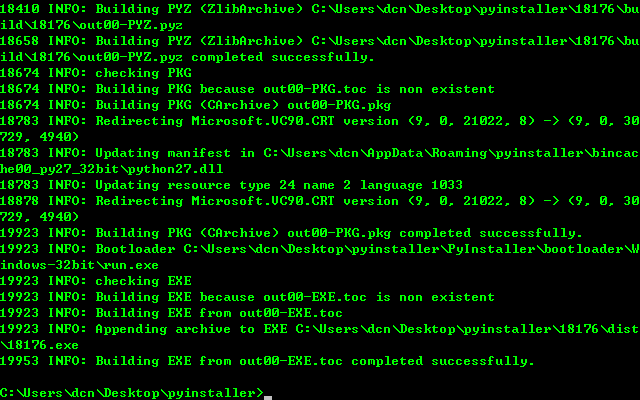
pip install pefile



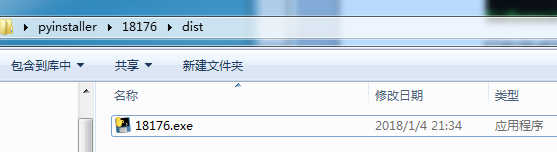
当出现python pyinstaller.py 的时候出现帮助信息时说明可以使用了



打包当文件成exe的命令：python pyinstaller.py --onefile 18176.py



打包完成后会在当前目录生成一个18176的目录，将里边的exe文件复制到目标机子中



将程序复制2k3，cmd执行弹出帮助，-O指定为2K3即可获取system用户权限

