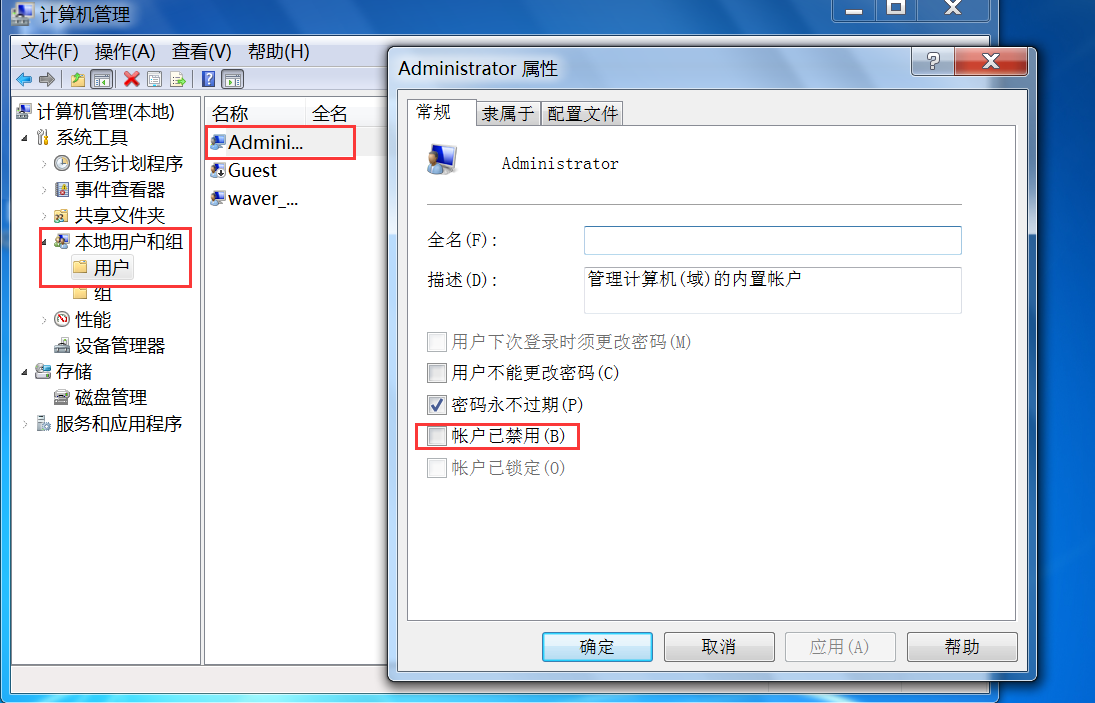
powershell是windows的高级命令，可以用来操作系统的高级硬件设置，比如网卡。

所以如果powershell中毒的情况下，我们可以直接卸载掉powershell来中断病毒传播。

windwos7：

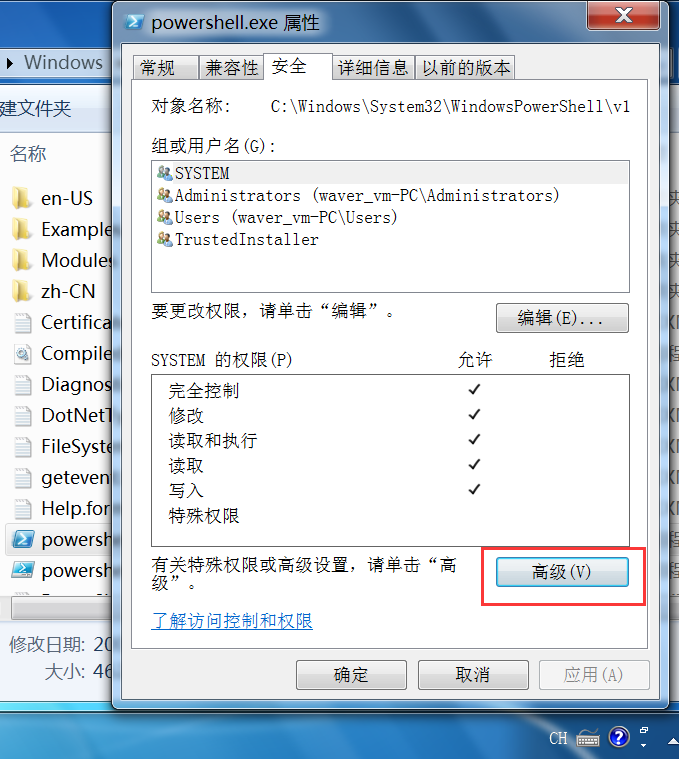
1、打开administrator超级管理员账户（已经是该账户的跳过）

计算机右键-》管理，打开administrator账户，然后注销，选择administrator账户登录。

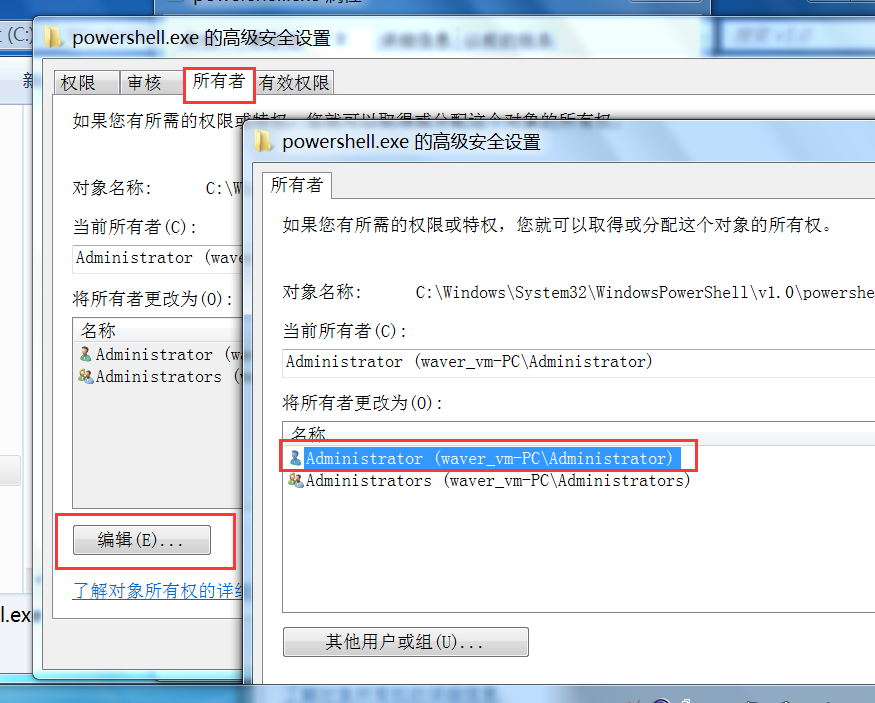


2、找到powershell路径：C:\Windows\System32\WindowsPowerShell\v1.0。注意64位系统存在两个路径：C:\Windows\SysWOW64\WindowsPowerShell\v1.0

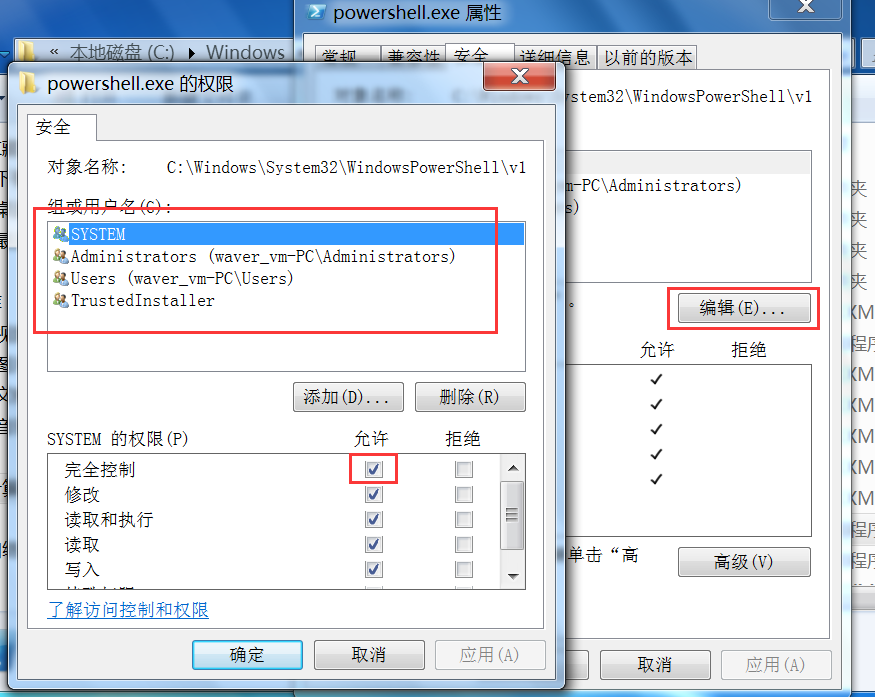
3、右键选择powershell.exe属性， 选择安全



4、点击高级-》所有者-》编辑，选中administrator账户点击应用。



5、回到安全界面，选择编辑，为所有用户授予完全控制的权限：



6、左键选中powershell.exe，shift+del彻底删除。注意64位系统有两个powershell.exe需要删除。

windows10：

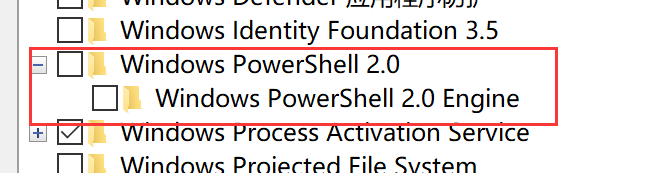
win10操作与win7差距不大，但是win10是以组件的方式注册到系统中的。

1、在windows组件中取消powershell。

打开程序和功能界面。（win10进入该界面的方式自己去搞，懒得写了）。点击启用或关闭windows功能。



2、取消掉powershell的勾。确定



3、切换到administrator账户（之后参考win7操作）