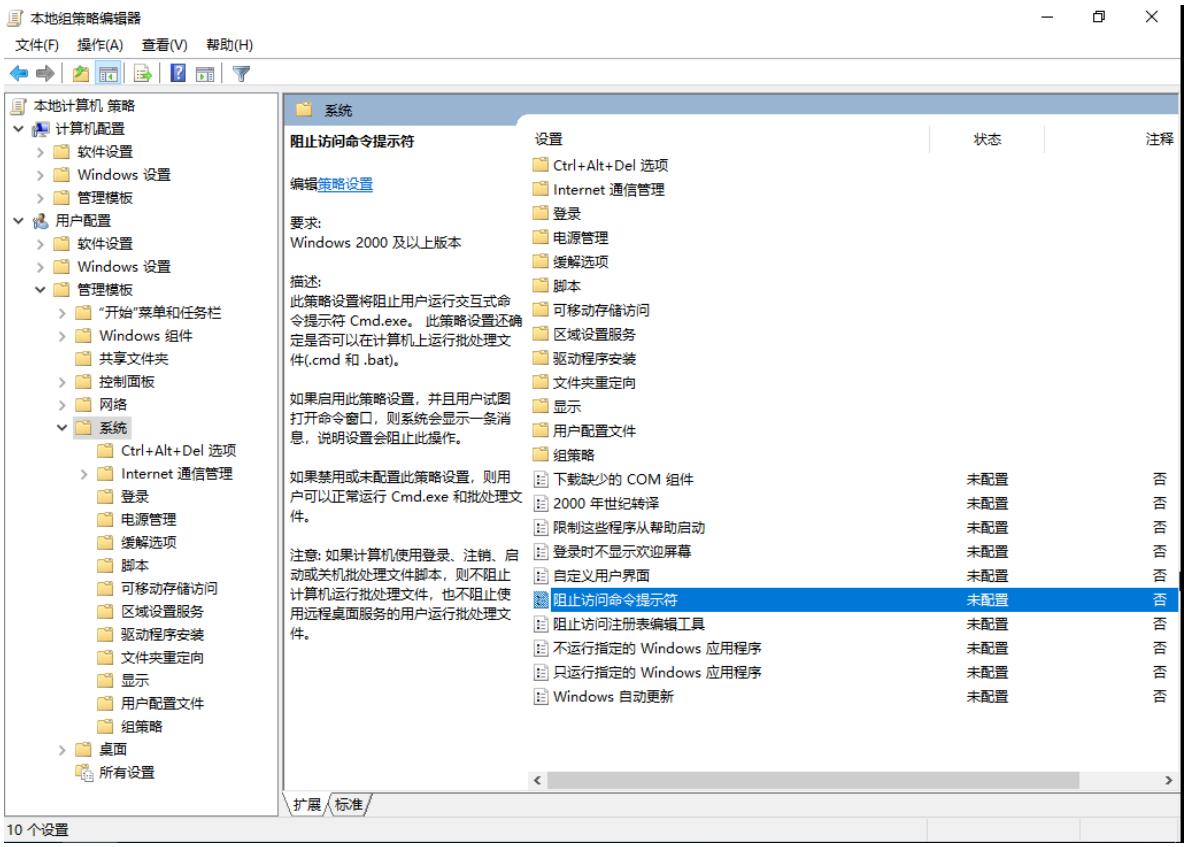
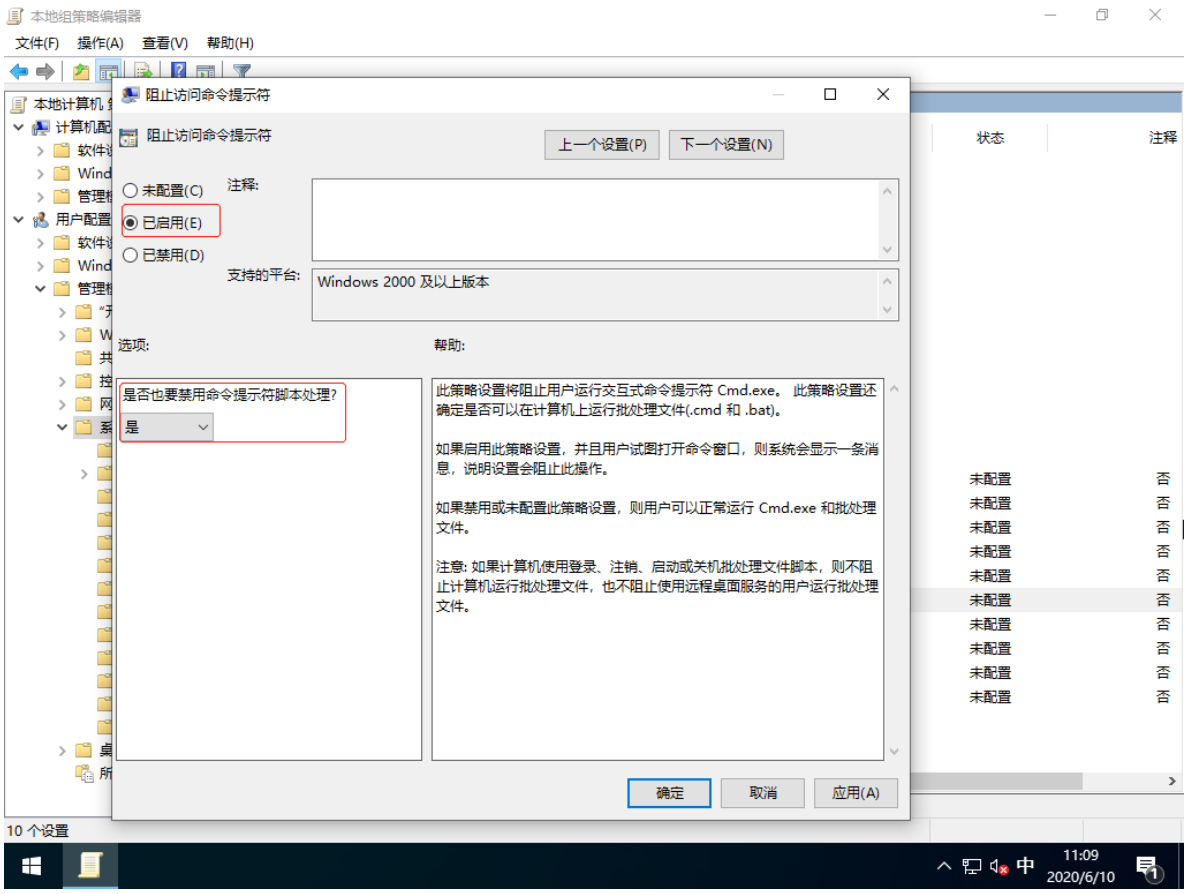
绕过管理员设定的组策略设置

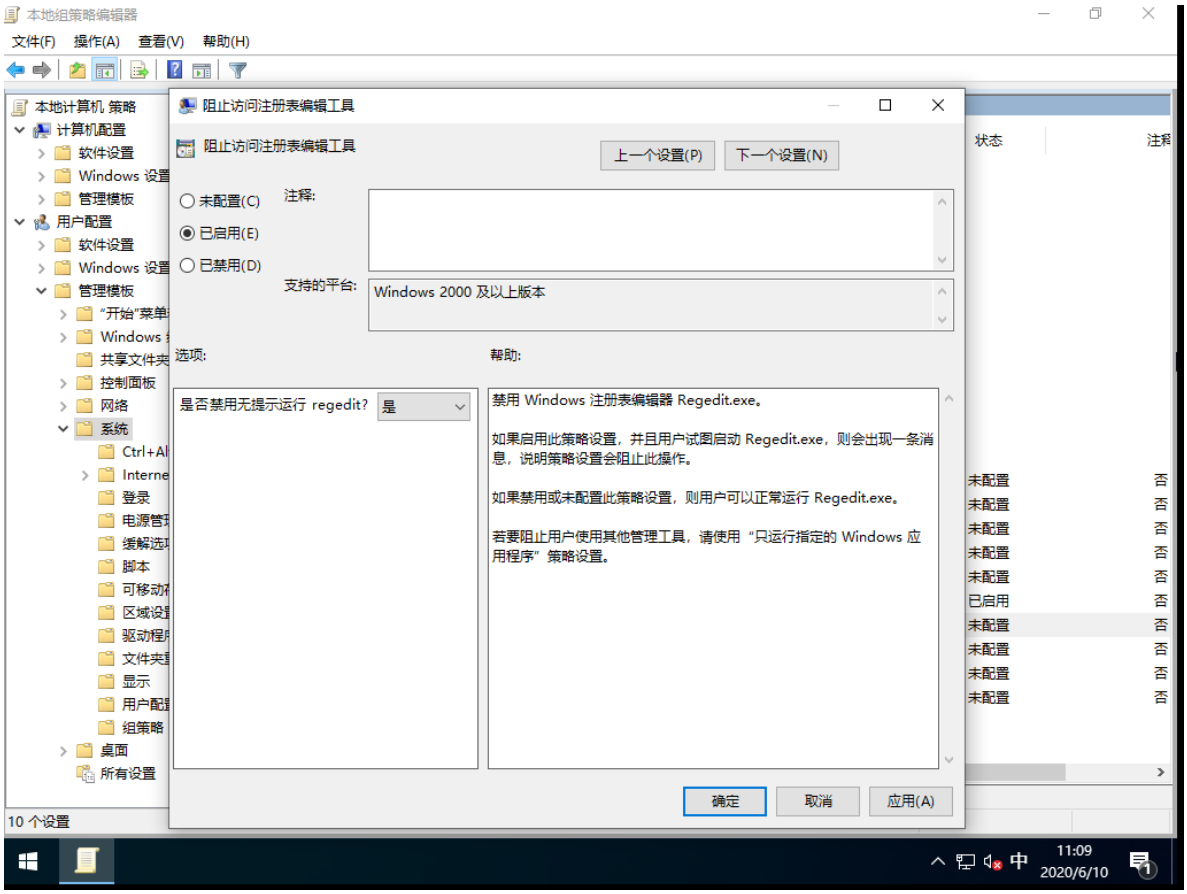
禁止访问命令提示符和注册表编辑工具

在“用户配置>策略>管理模板>系统”下找到它们，它们分别称为“防止访问命令提示符”和“防止访问注册表编辑工具”

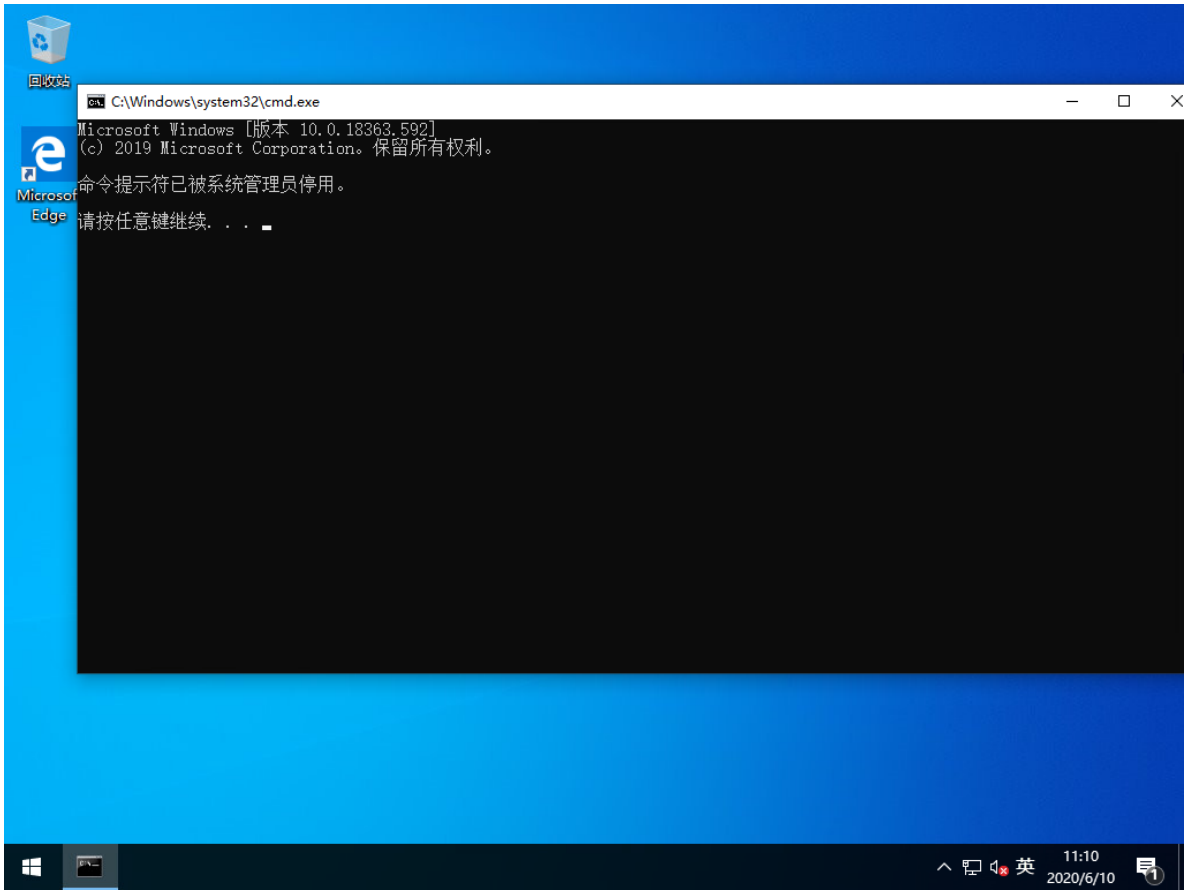


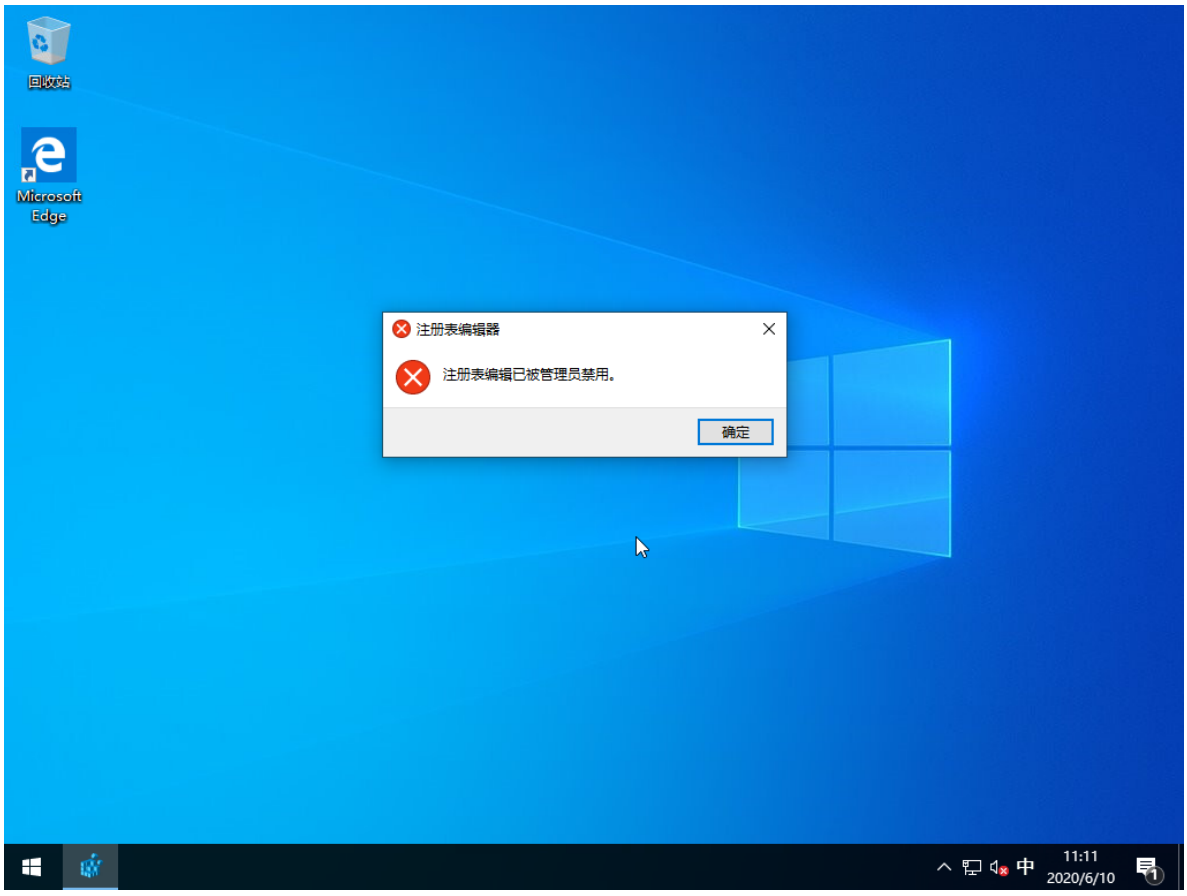
我们将它们设置为如下





我们再使用命令打开发现：





禁用命令提示符并启用脚本处理：

方法一：

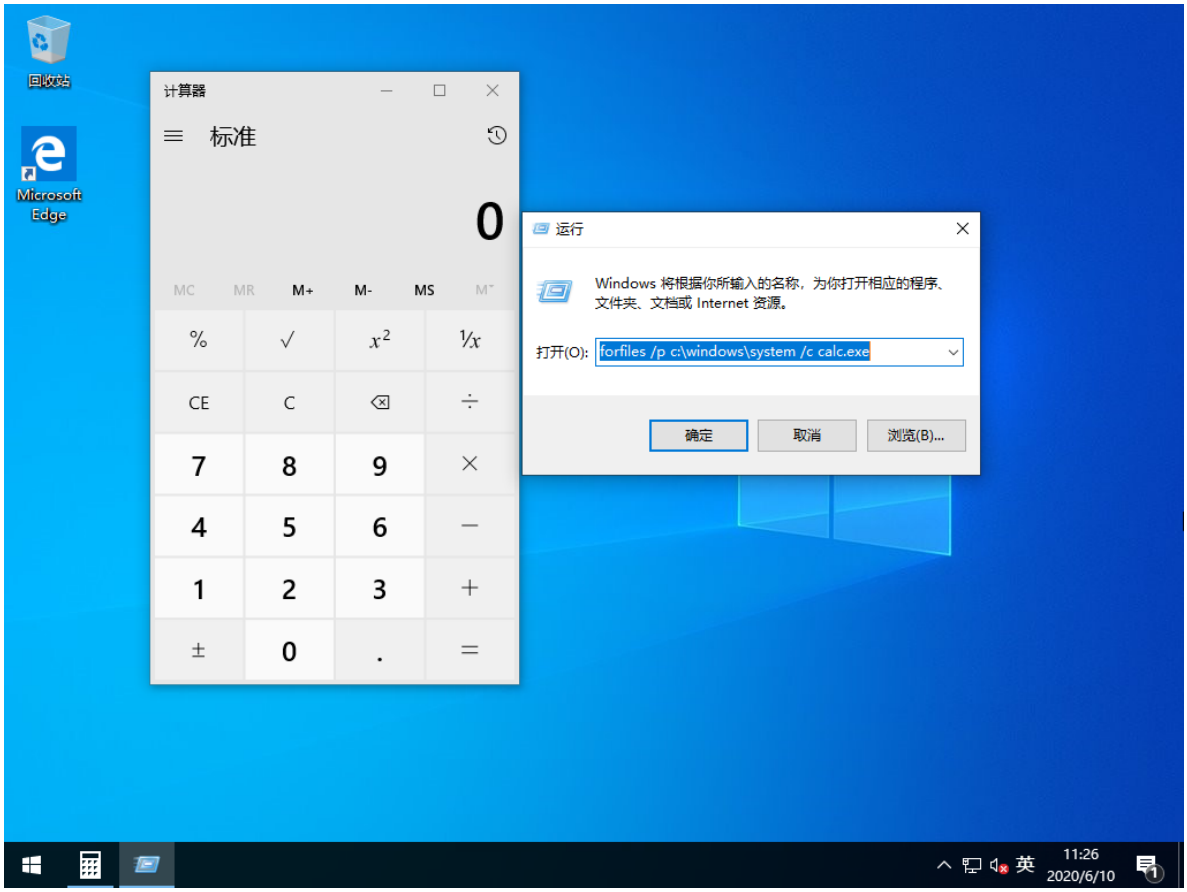
当然window10系统下你们是可以使用powershell代替，但是如果是win7系统呢?

当然有些杀毒软件也会禁用cmd命令，这时候就用得到我们的白名单去绕过，白名单：forfiles命令

在百度上搜索forfiles对它的操作是这样的：

> **forfiles** 命令用来搜索不同盘符指定文件或文件夹, 更新软件或执行批处理程序都非常方便, 其语法为: forfiles /p 要搜索的文件夹或盘符 /m 要搜索的文件类型 /s 递归搜索文件 /c 执行文件命令 **(/c 后面一定要用字符串进行包裹噢)**

为此我们可以使用forfiles /p c:\windows\system\ /c calc.exe去打开计算器，当然你也可以去打开别的文件。

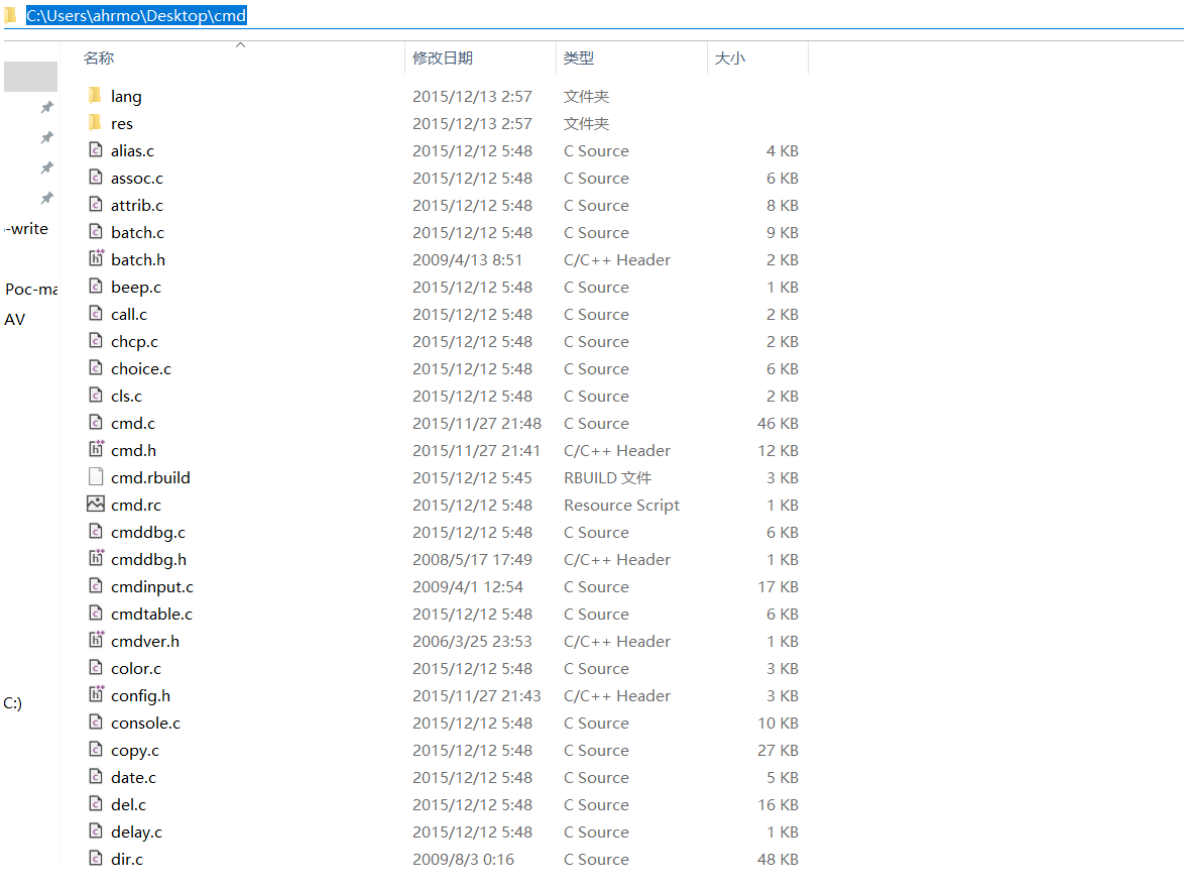


当然你也可以使用forfiles从隐藏在备用数据流中的二进制文件中启动新进程

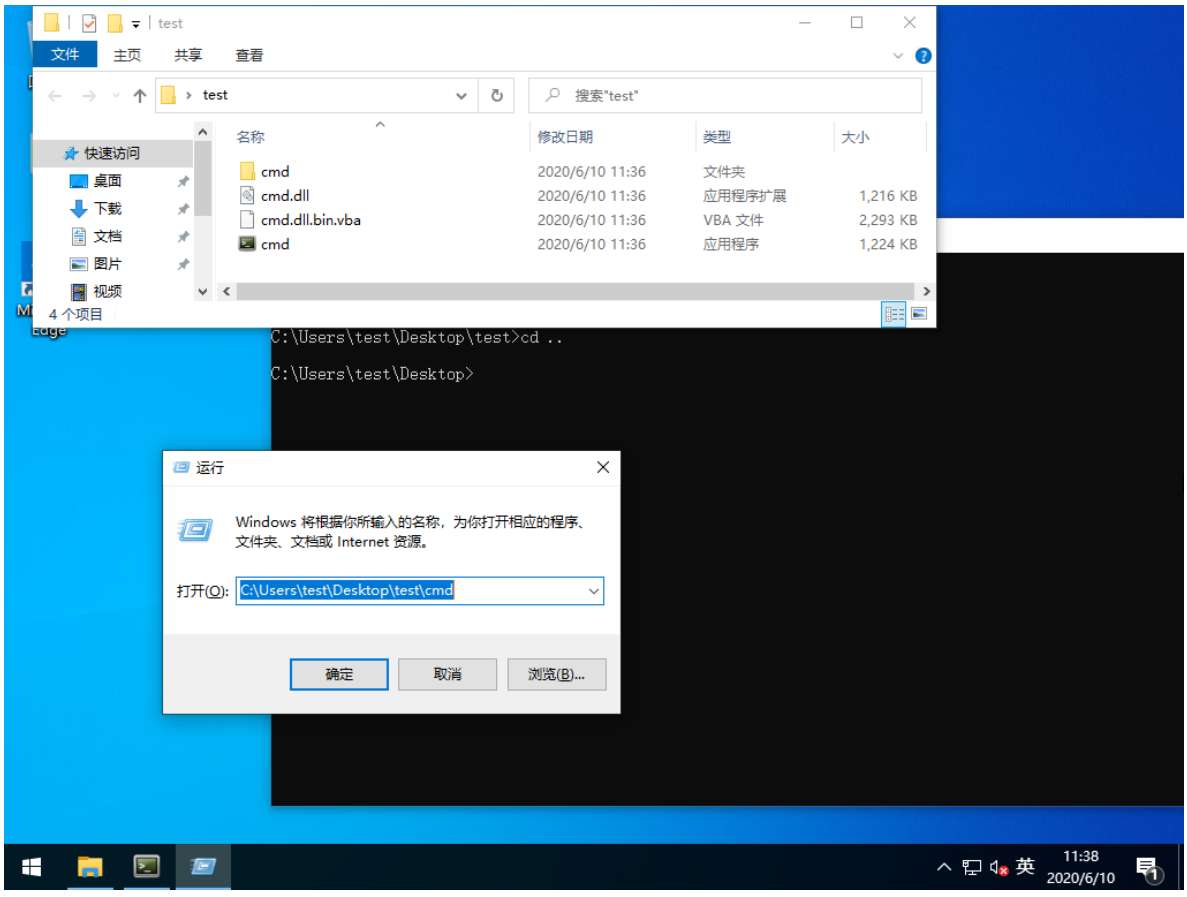
例如：forfiles /p c:\windows\system32 /m notepad.exe /c "c:\folder\normal.dll:evil.exe"

方法二：

当然自己写一个CMD也是可以的：



把自己写好的CMD->打包->解压->然后你懂的



方案-注册表编辑工具被禁用

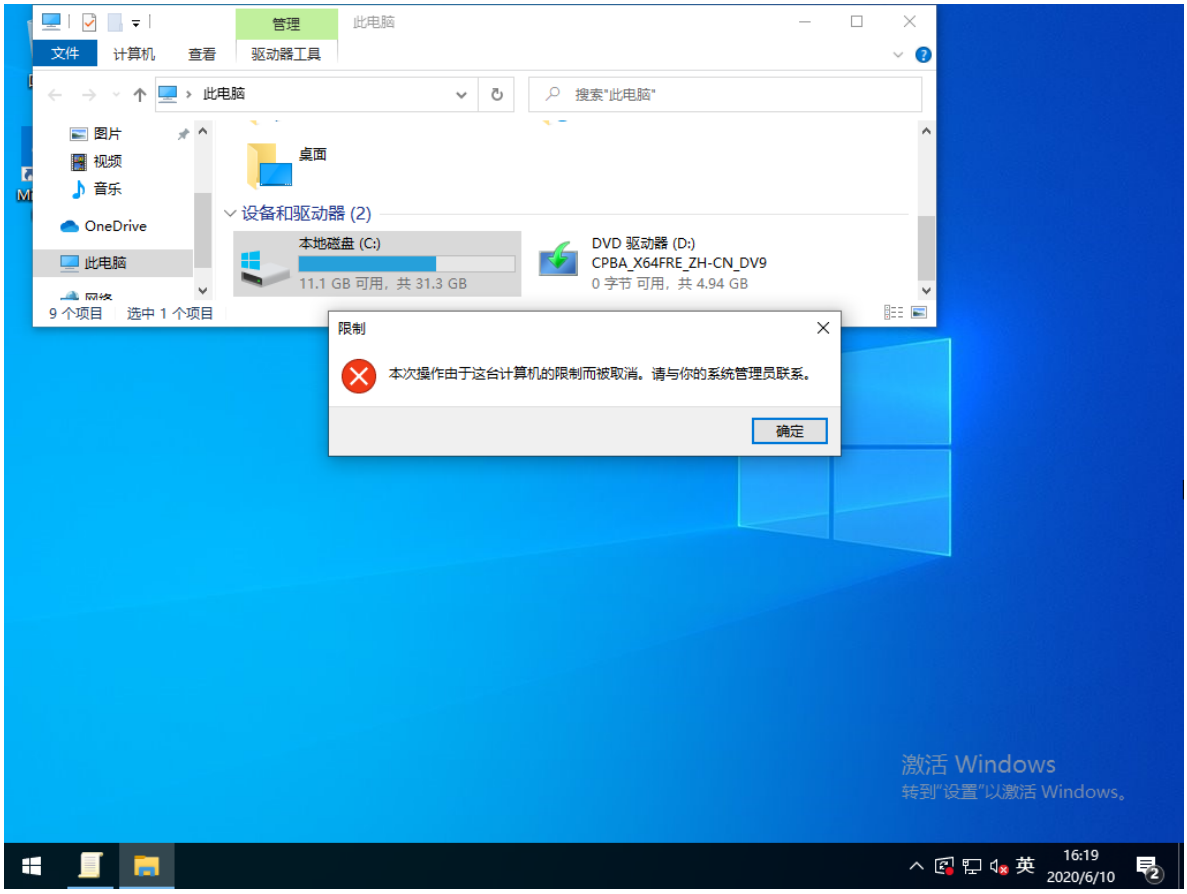
我们可以将以下代码生成.vbs格式:

```
从注册表中读取path变量所需要的
Set objWshShell = WScript.CreateObject("WScript.Shell")
strKeyToRead = objWshShell.RegRead("HKCU\Environment\path")
wscript.echo strKeyToRead
用于使用vbscript写入注册表
Set objWshShell = WScript.CreateObject("WScript.Shell")
myKey = "HKCU\Environment\mysetting"
objWshShell.RegWrite myKey,1,"REG_DWORD"
```

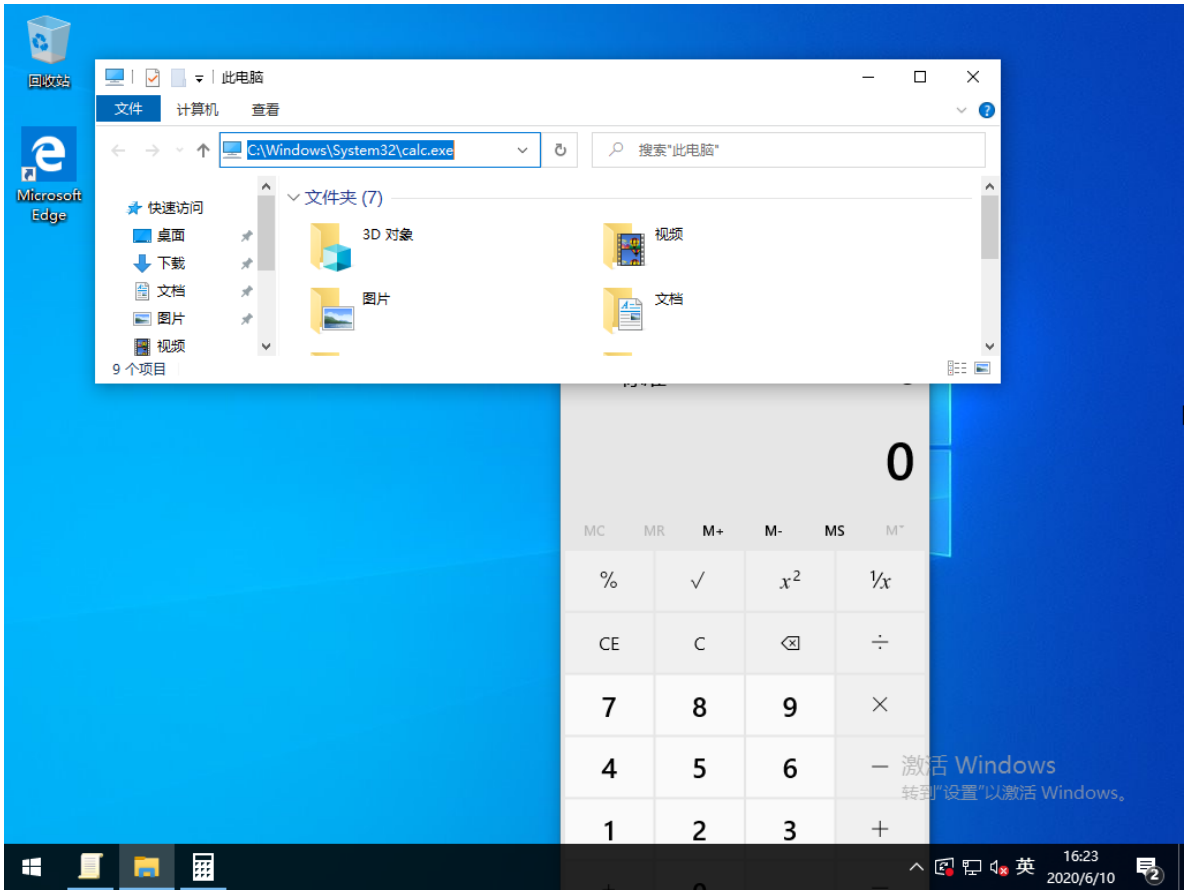
执行后：

```
[HKEY_CURRENT_USER\environment]
"Path"=hex(2):25,00,55,00,53,00,45,00,52,00,50,00,52,00,4f,00,46,00,49,00,4c,\
  00,45,00,25,00,5c,00,41,00,70,00,70,00,44,00,61,00,74,00,61,00,5c,00,4c,00,\
  6f,00,63,00,61,00,6c,00,5c,00,4d,00,69,00,63,00,72,00,6f,00,73,00,6f,00,66,\
  00,74,00,5c,00,57,00,69,00,6e,00,64,00,6f,00,77,00,73,00,41,00,70,00,70,00,\
  73,00,3b,00,00,00
"TEMP"=hex(2):25,00,55,00,53,00,45,00,52,00,50,00,52,00,4f,00,46,00,49,00,4c,\
  00,45,00,25,00,5c,00,41,00,70,00,70,00,44,00,61,00,74,00,61,00,5c,00,4c,00,\
  6f,00,63,00,61,00,6c,00,5c,00,54,00,65,00,6d,00,70,00,00,00
"TMP"=hex(2):25,00,55,00,53,00,45,00,52,00,50,00,52,00,4f,00,46,00,49,00,4c,00,\
  45,00,25,00,5c,00,41,00,70,00,70,00,44,00,61,00,74,00,61,00,5c,00,4c,00,6f,\
  00,63,00,61,00,6c,00,5c,00,54,00,65,00,6d,00,70,00,00,00
"OneDrive"=hex(2):43,00,3a,00,5c,00,55,00,73,00,65,00,72,00,73,00,5c,00,6e,00,\
  6f,00,72,00,6d,00,61,00,6c,00,75,00,73,00,65,00,72,00,5c,00,4f,00,6e,00,65,\
  00,44,00,72,00,69,00,76,00,65,00,00,00
```

阻止访问C盘



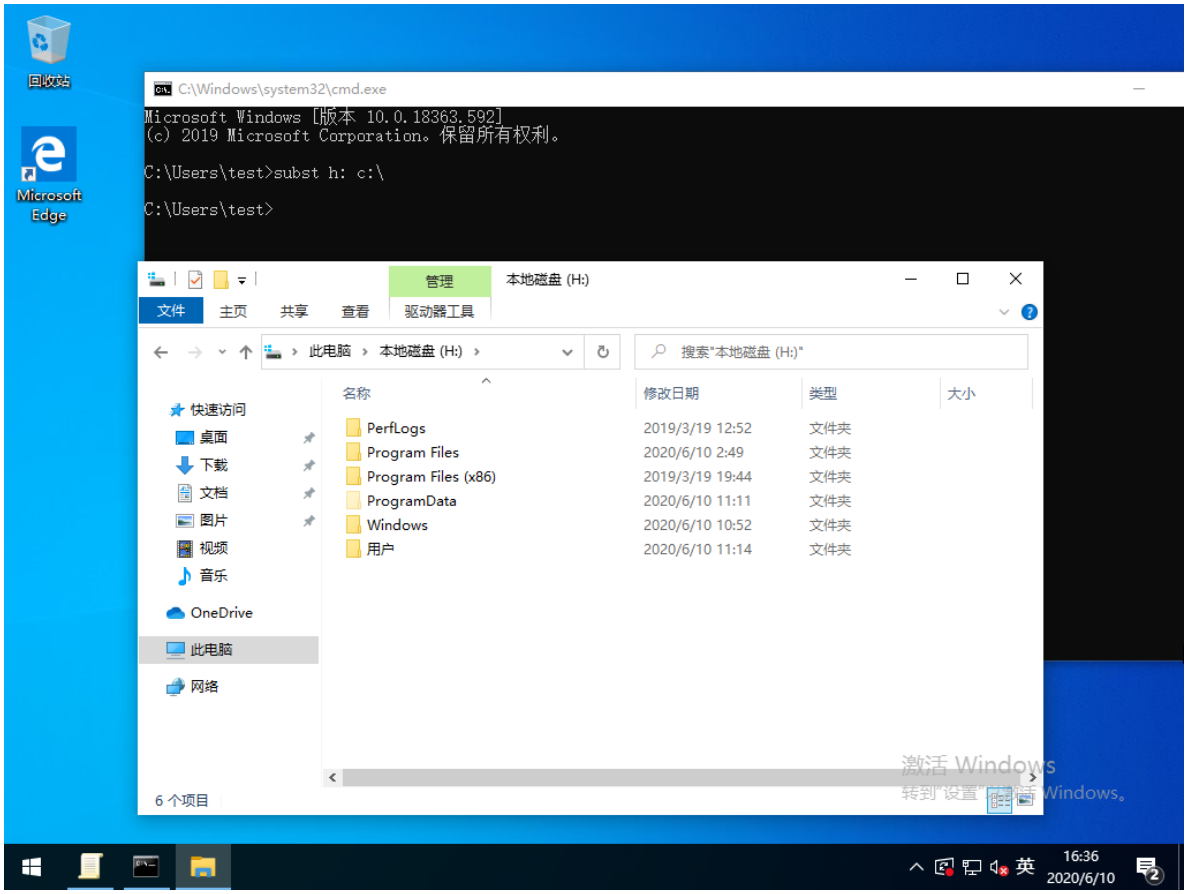
方法一：在资源管理器地址字段中输入完整路径



方法二：在共享文件中使用\ 127.0.0.1 \ c $浏览磁盘

方法三：使用CMD或PowerShell浏览磁盘(不用多说你们都知道)

方法四：执行subst命令来伪造新的驱动器号



技术免责声明

本文仅作技术性研究.请酌情使用,由此引发的一系列后果请自行承担.

By:AhRMo