mbp 封神台靶场 七（笔记）

原创

qq_43558415 于 2020-02-09 22:15:59 发布 528 收藏 1

分类专栏： 封神台靶场

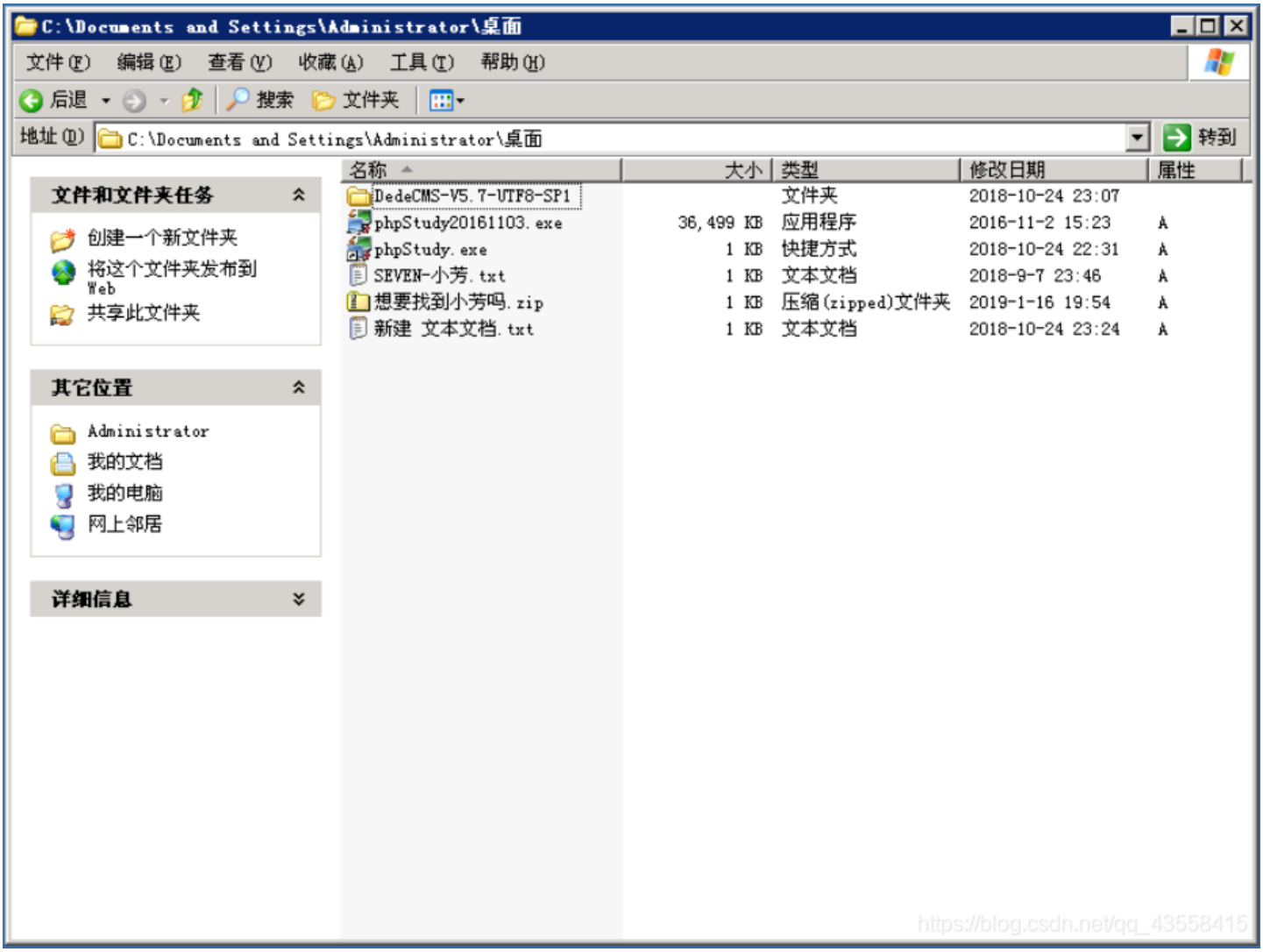
本文链接：https://blog.csdn.net/qq_43558415/article/details/104241345

封神台靶场 专栏收录该内容

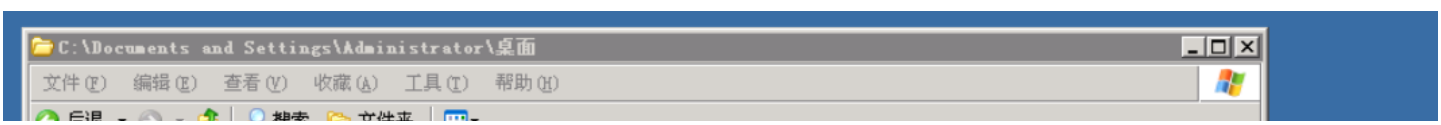
7 篇文章 4 订阅

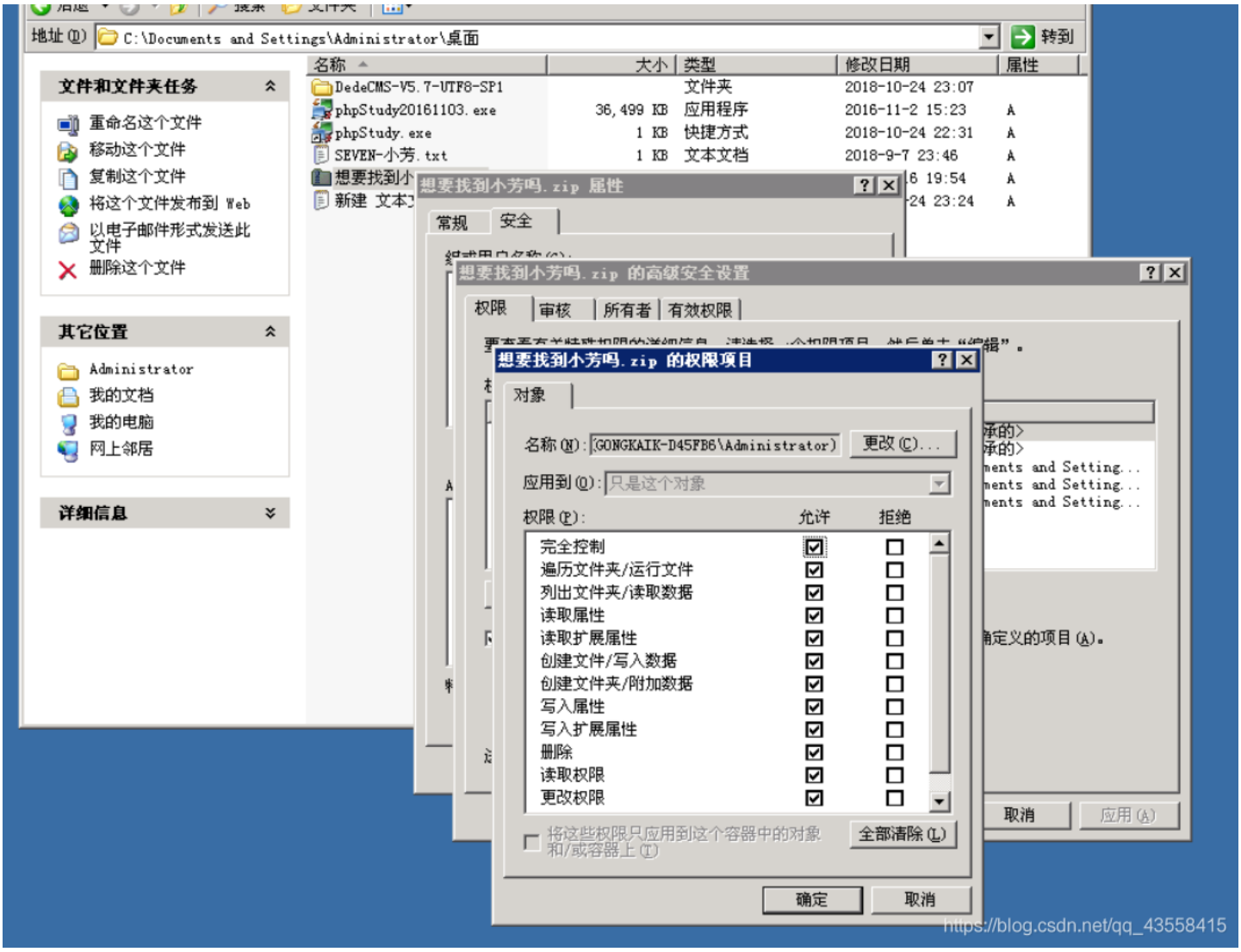
订阅专栏

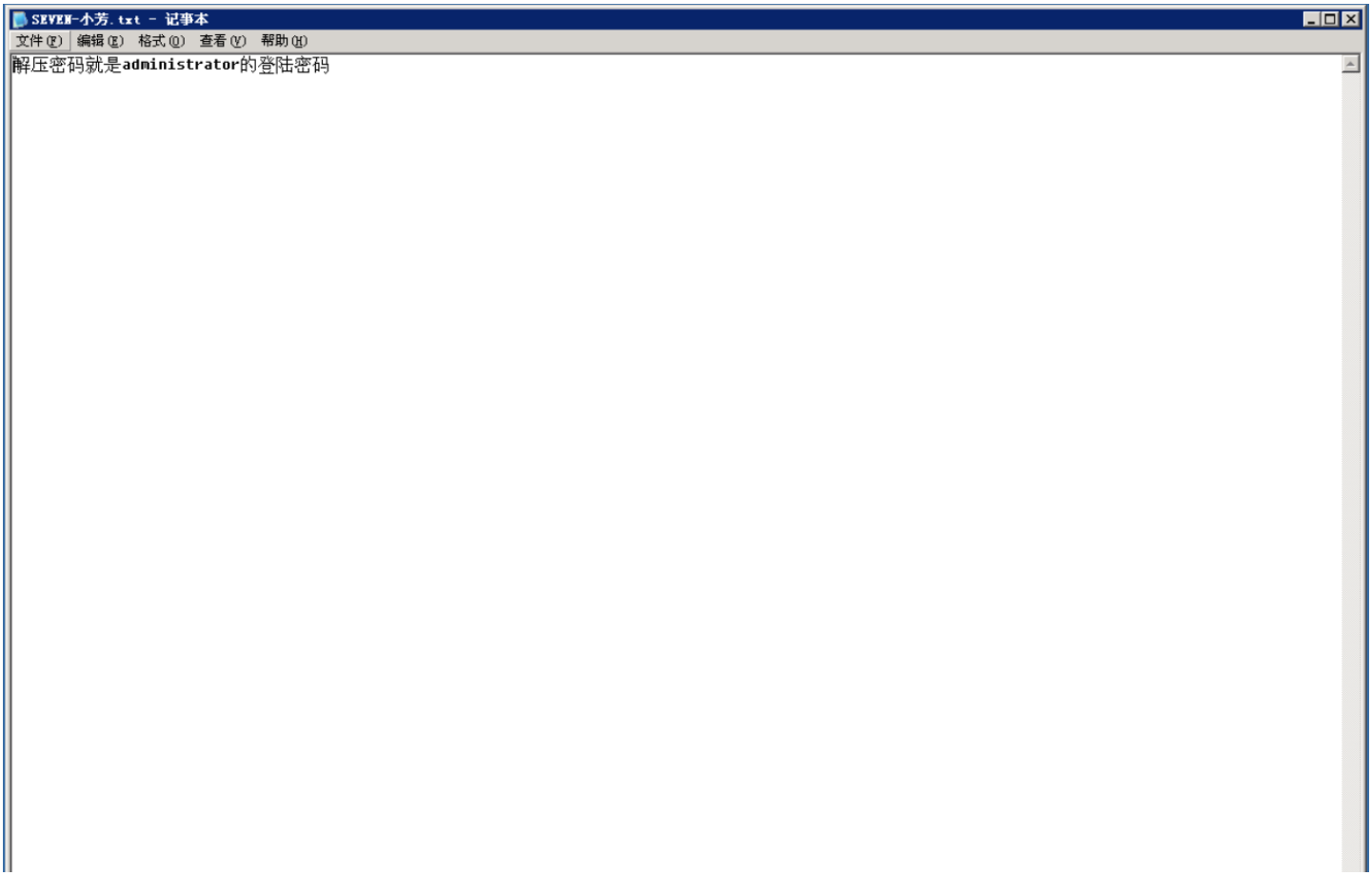
打开链接，还是在上一关的基础上进行操作，接上打开C盘发现有线索。两个关于小芳的文件都打不开。

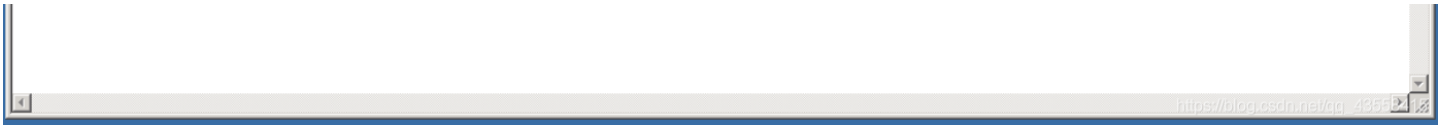


于是首先zip文件和txt文件启用了ACL，需要进行更改，右键找到属性》安全〉高级，把完全控制从拒绝改成允许。txt文本说解压密码就是Administrator的登录密码。

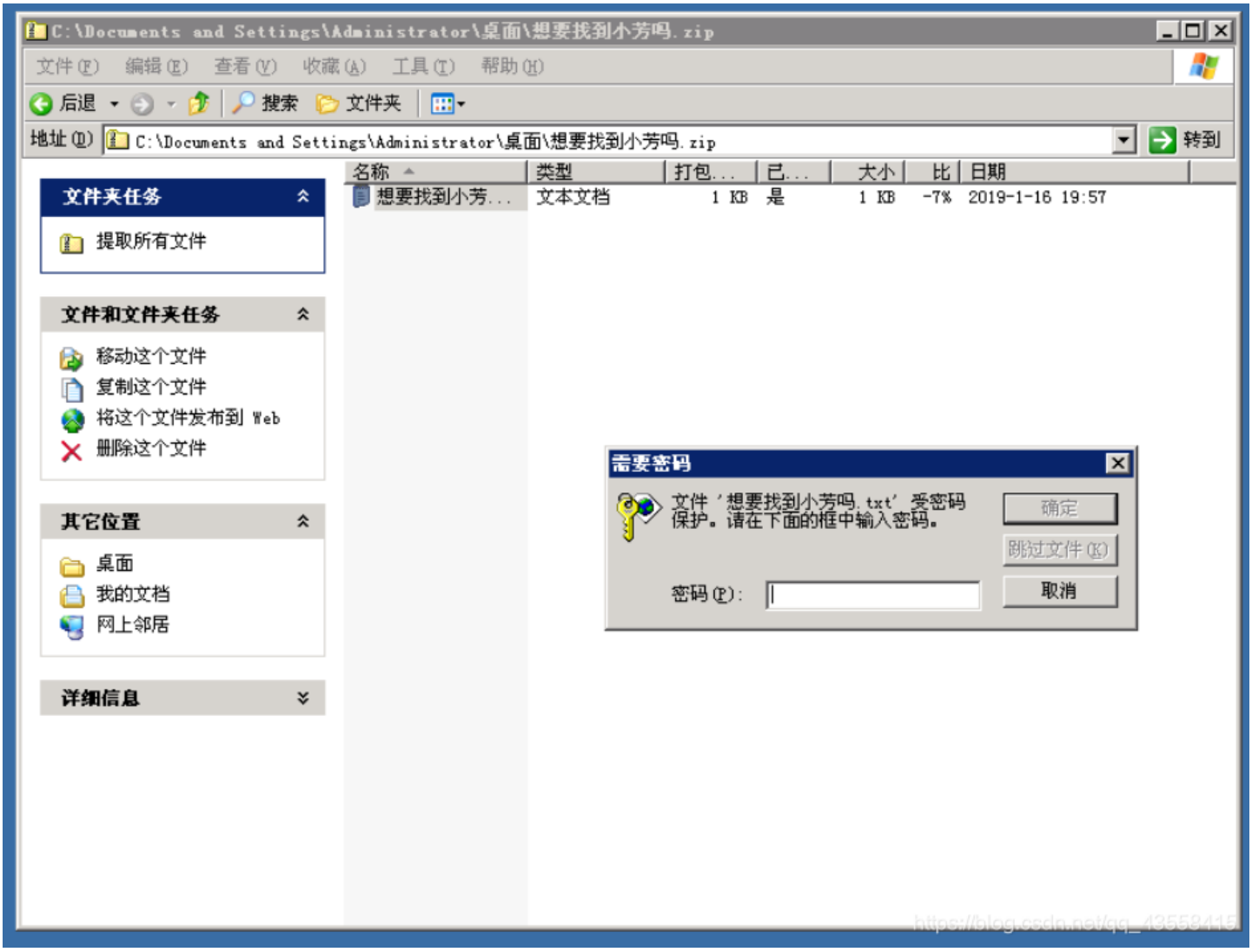



地址(D) C:\Documents and Settings\Administrator\桌面
转到
文件和文件夹任务
重命名这个文件
移动这个文件
复制这个文件
将这个文件发布到 Web
以电子邮件形式发送此文件
删除这个文件
其它位置
Administrator
我的文档
我的电脑
网上邻居
详细信息
名称
大小
类型
修改日期
属性
DedeCMS-V5.7-UTF8-SP1
文件夹
2018-10-24 23:07
phpStudy20161103.exe
36,499 KB
应用程序
2016-11-2 15:23
A
phpStudy.exe
1 KB
快捷方式
2018-10-24 22:31
A
SEVEN-小芳.txt
1 KB
文本文档
2018-9-7 23:46
A
想要找到小芳吗.zip 属性
常规
安全
想要找到小芳吗.zip 的高级安全设置
权限
审核
所有者
有效权限
想要找到小芳吗.zip 的权限项目
对象
名称(N): GONGKAIK-D45FB6\Administrator)
更改(C)...
应用到(O): 只是这个对象
权限(P):
允许
拒绝
完全控制
遍历文件夹/运行文件
列出文件夹/读取数据
读取属性
读取扩展属性
创建文件/写入数据
创建文件夹/附加数据
写入属性
写入扩展属性
删除
读取权限
更改权限
将这些权限只应用到这个容器中的对象和/或容器上(T)
全部清除(L)
确定
取消
应用(A)
https://blog.csdn.net/qq_43558415

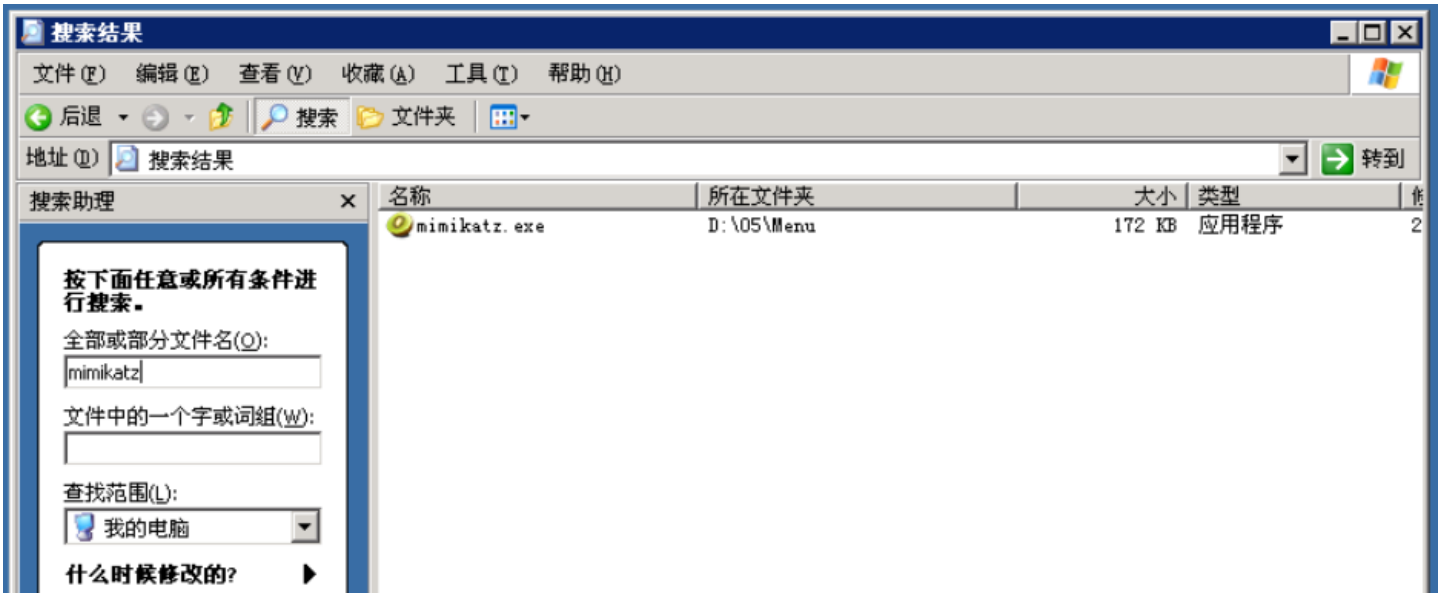

SEVEN-小芳.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
解压密码就是administrator的登陆密码

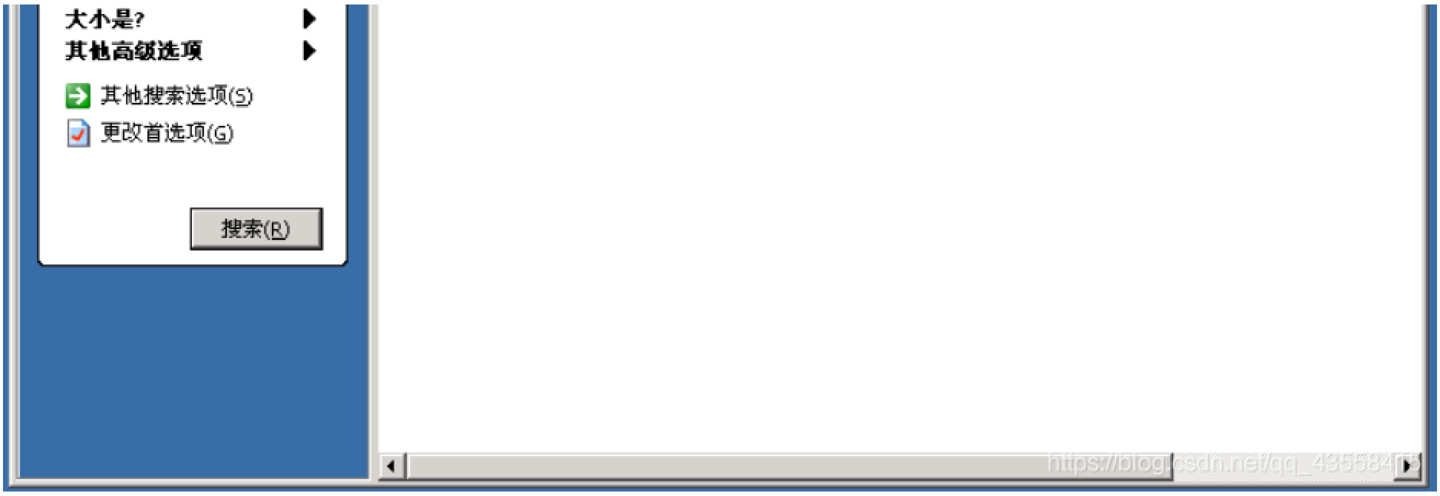


打开文件，发现还需要密码。

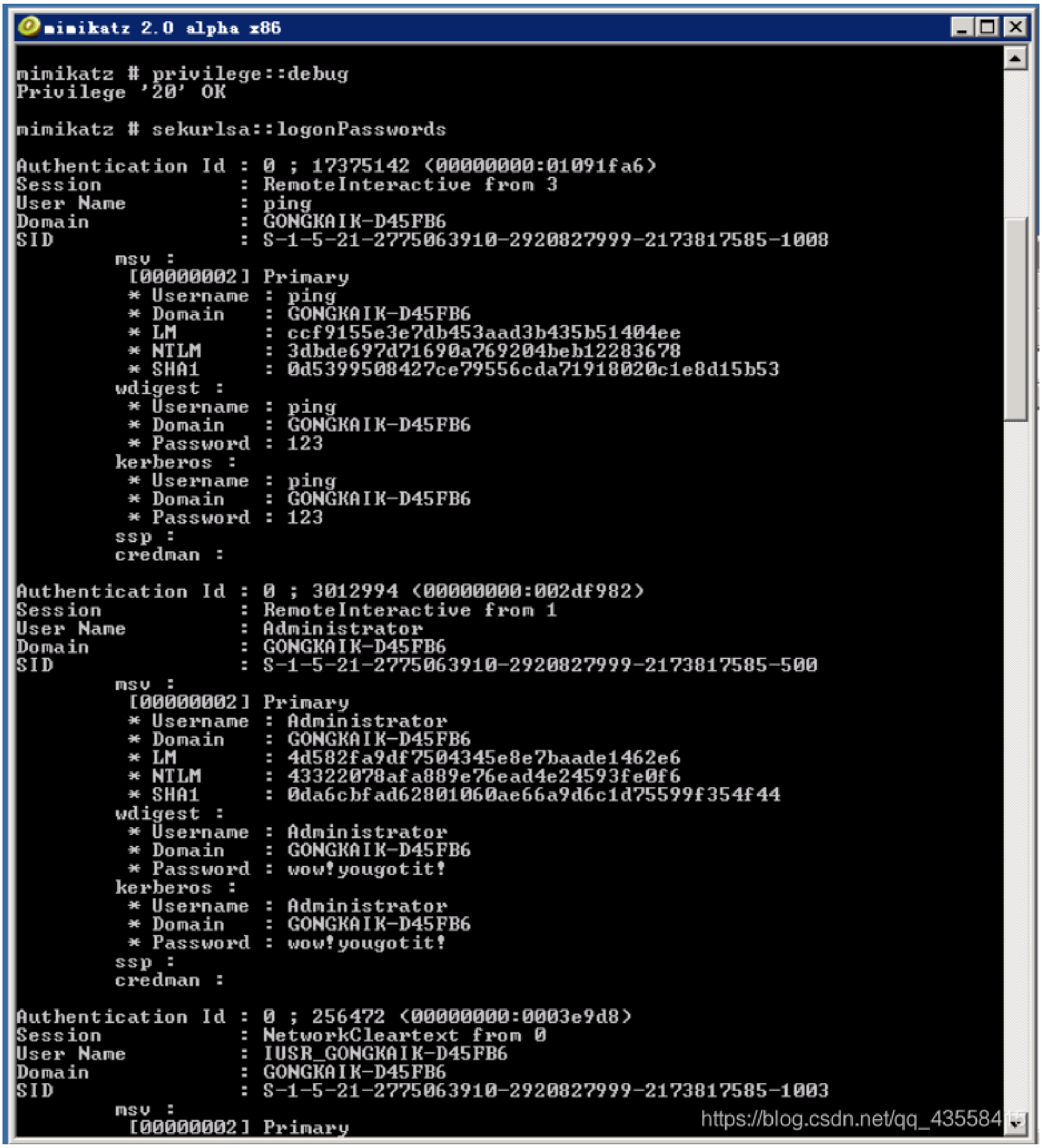


这需要使用mimikatz工具，在参考中是选择通过上传方式来使用该软件，我考虑到这工具可能服务器上就存在，于是在服务器中搜索，结果真的找到了。



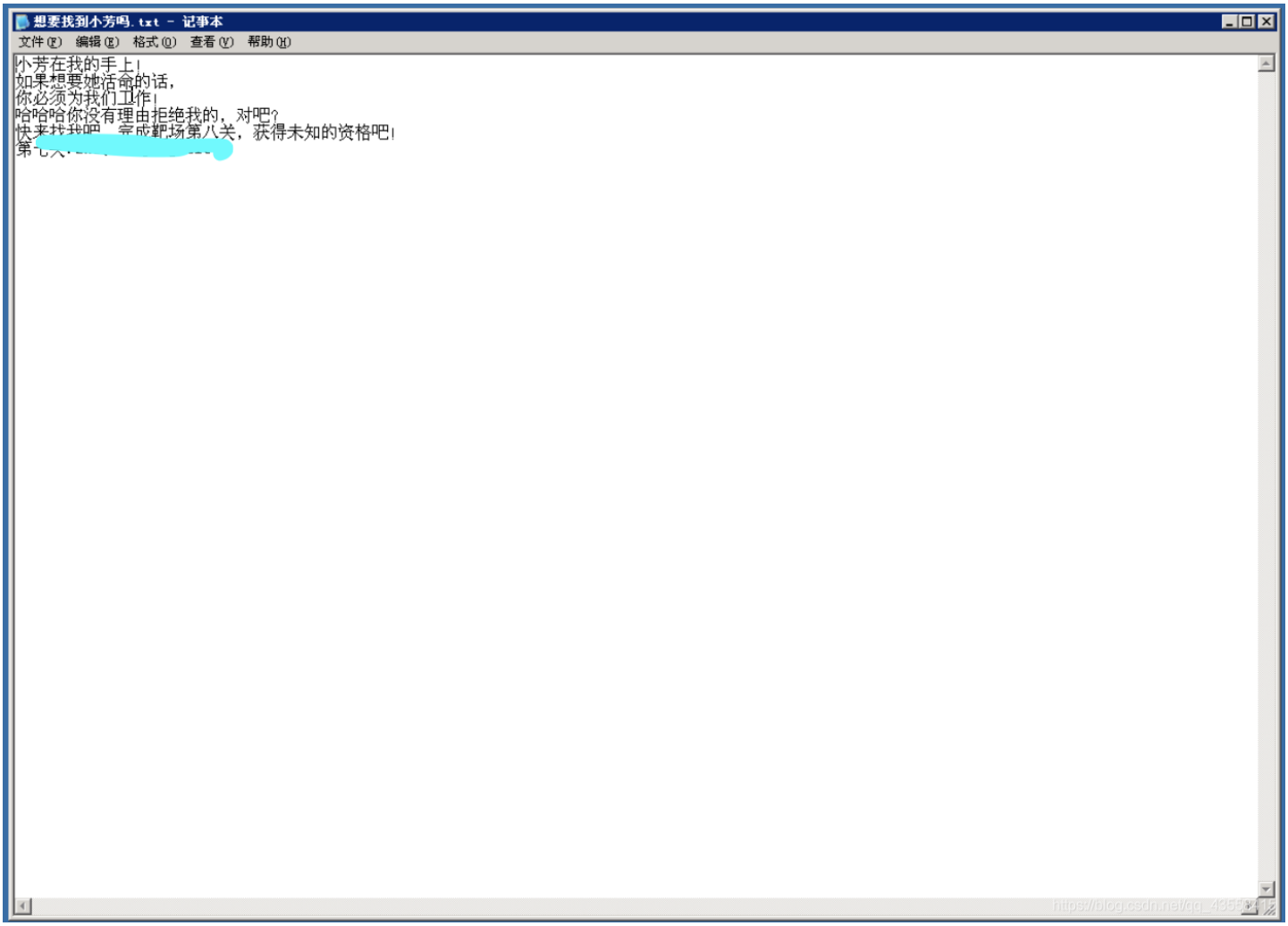


找到该工具后点开输入`privilege::debug`提升权限
`sekurlsa::logonPasswords` 获取密码



找到password,

填写进入zip文件，拿到flag。



总结：好好学习。