记一次明文攻击+盲水印 ctf题目

原创

qq_26317875 于 2018-04-01 13:02:38 发布 10416 收藏 9
分类专栏： writeup 文章标签： ctf writeup
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_26317875/article/details/79776727
版权


writeup 专栏收录该内容
3 篇文章 0 订阅
订阅专栏

题目链接 http://pan.baidu.com/s/1slDhhvf 密码：vroj


open_forum.png


warmup.zip

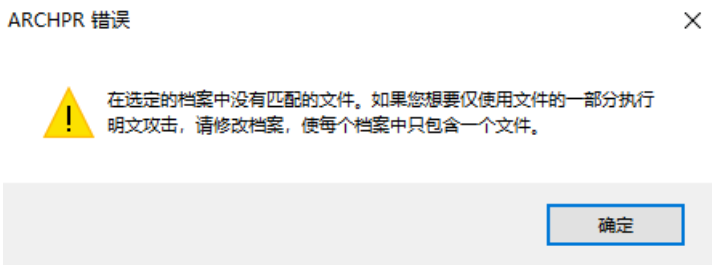
解压出来是这样的

warmup里是这样的

:

fuli2.png *	4.33 MB	4.30 MB	PNG 文件	2017-06-19 17:15:30	02EB038D	ZipCrypto Deflate
fuli.png *	3.69 MB	3.67 MB	PNG 文件	2017-06-19 17:13:54	40056D15	ZipCrypto Deflate
open_forum.png *	41.20 KB	40.55 KB	PNG 文件	2017-07-05 13:03:42	83E22C5E	ZipCrypto Deflate

看着像两个一样的open_forun.png 想到明文攻击，将open_forum.png压缩，然后使用ARCHPR的明文攻击，结果报错了：



在选定的档案中没有匹配的文件。。。

研究了一下，找到了问题所在，原来是因为压缩软件没用对，用winrar重新压缩一次:

这里要选zip。

然后重新明文攻击，成功。

解压出来是这样:

两个图，试试盲水印:

```
C:\Users\li\Desktop\warmup>python27 bwm.py decode fuli.png fuli2.png solved.png
image<fuli.png> + image(encoded)<fuli2.png> -> watermark<solved.png>
```

成功拿到flag:

明文攻击的关键在于压缩软件的使用，其他题目可能会提示使用什么压缩软件进行压缩，需要注意一下。

btw: 盲水印用到的py脚本可以在github上下载,https://github.com/chishaxie/BlindWaterMark,使用时需要安装前置opencv库。

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖