

实验吧安全杂项WP(九)

原创

Neil-Yale 于 2017-03-23 13:15:06 发布 2767 收藏 1

文章标签: [github](#) [安全](#) [CTF](#) [wp](#)

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/yalecaltech/article/details/65442340>

版权

1.XDCTF misc100 (<http://www.shiyanbar.com/ctf/1761>)

下载来是两张图片

根据提示百度得知这是个开源项目

于是去github扒下来然后编译

具体的用法 -help即可

我这里直接用csdn上下的已编译好的工具

将图片和工具放在相同路径下, cmd打开

名称	修改日期	类型	大小
bflib.dll	2015/10/2 15:41	应用程序扩展	11 KB
bflib.dll.mdb	2015/10/2 15:38	Microsoft Acces...	4 KB
bftools.exe	2015/10/2 15:38	应用程序	9 KB
bftools.exe.mdb	2015/10/2 15:37	Microsoft Acces...	3 KB
ManyConsole.dll	2015/10/2 15:41	应用程序扩展	22 KB
NDesk.Options.dll	2015/10/2 15:41	应用程序扩展	22 KB
org.png	2015/10/13 14:15	PNG 文件	30 KB
--out.png	2017/3/23 10:18	PNG 文件	1 KB
zzzzzyu.png	2015/10/13 14:15	PNG 文件	26 KB

```
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation. 保留所有权利。

C:\Users\hasee>cd Desktop
C:\Users\hasee\Desktop>cd bftools
C:\Users\hasee\Desktop\bftools>bftools.exe decode braincopter zzzzzzyu.png --output --out.png
C:\Users\hasee\Desktop\bftools>bftools.exe run --out.png
XDCTF {ji910-dad9jq0-iopuno}  □□□□□□
C:\Users\hasee\Desktop\bftools>
```

得到flag

3.XDCTF misc200 (<http://www.shiyanbar.com/ctf/writeup/1635>)

题目提示明文攻击

什么是明文攻击呢？

在所有密码分析中，均假设攻击者知道正在使用的密码体制，该假设称为Kerckhoff假设。而已知明文攻击也假设攻击者能够获取部分明文和相应密文，如截取信息前段，通过该类型攻击获取加密方式，从而便于破解后段密文。

在这个题目中意思是让我们通过一部分有明文和密文对应的文件，来得到key，从而解密

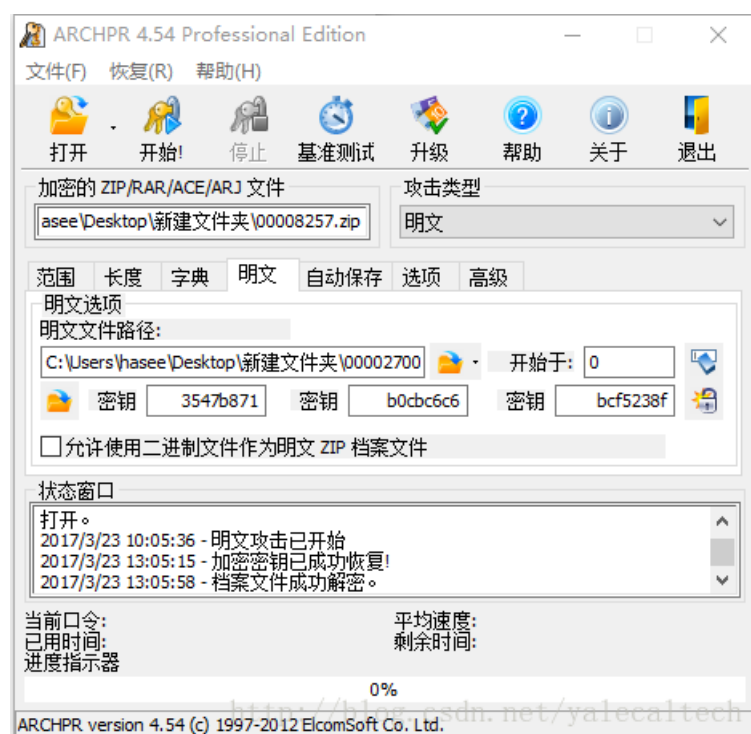
这里我们注意到



两个readme.txt的CRC相同，所以这应该就是相应的明文和密文

2700是可以解压的，将解压出的readme.txt压缩成readme.zip,作为明文去破解

使用ARCHPR



得到所示的三个密钥就可以解密了

解压后的文件夹中的flag.txt就是flag