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

本文链接：https://blog.csdn.net/yalecaltech/article/details/65442340

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

下载来是两张图片

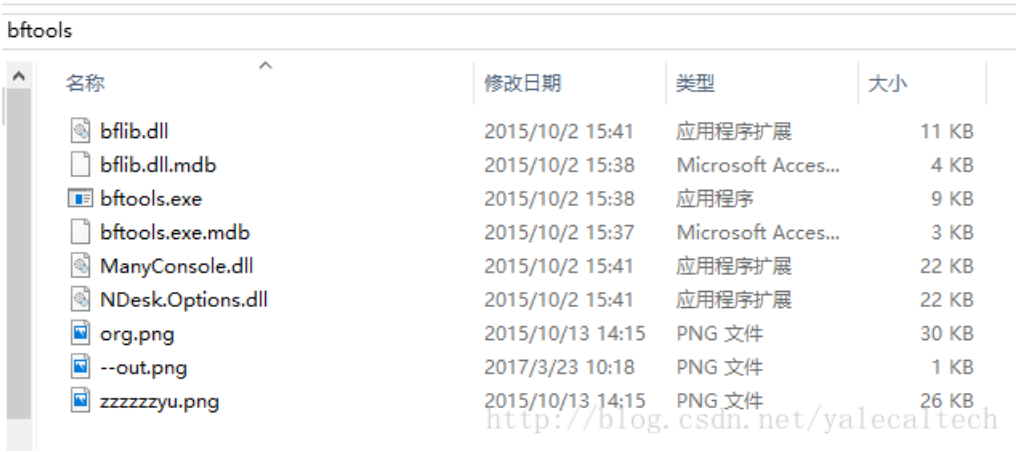
根据提示百度得知这是个开源项目

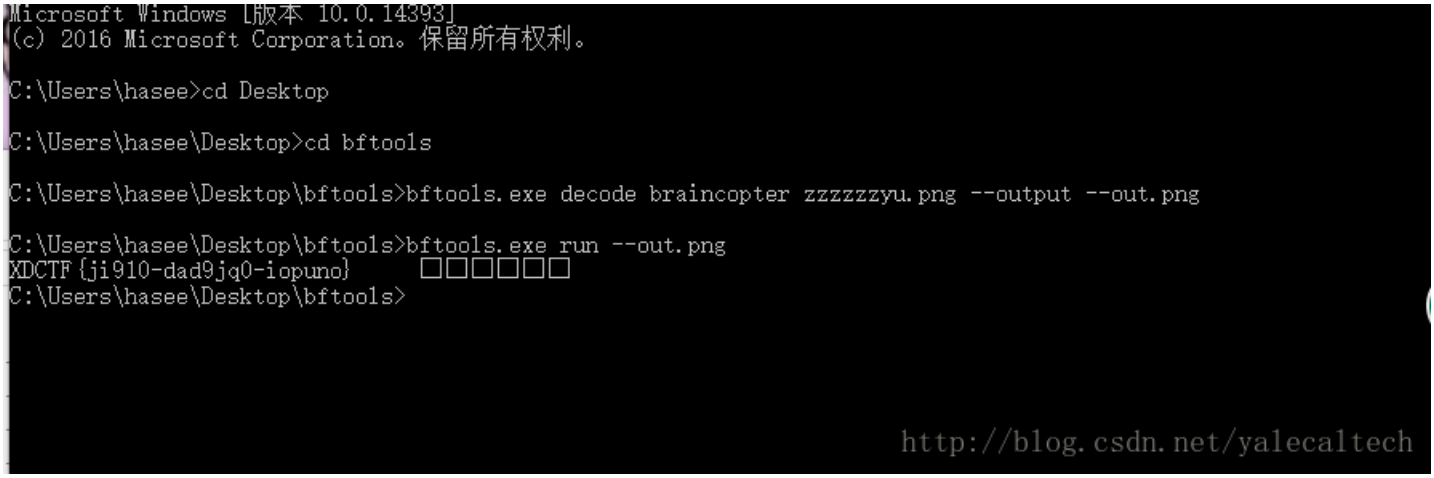
于是去github扒下来然后编译

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





得到flag

2.女神（http://www.shiyanbar.com/ctf/724）
解压后打开是个txt,目测是base64编码
思路当然就是解码，得到

PNG开头，那就是图片了
得到图片后直接百度识图就行
这里我直接跑python

```
>>> open('nvshen.png','wb').write(open('nvshen.txt','rb').read().decode('base64'))
...

>>>
```

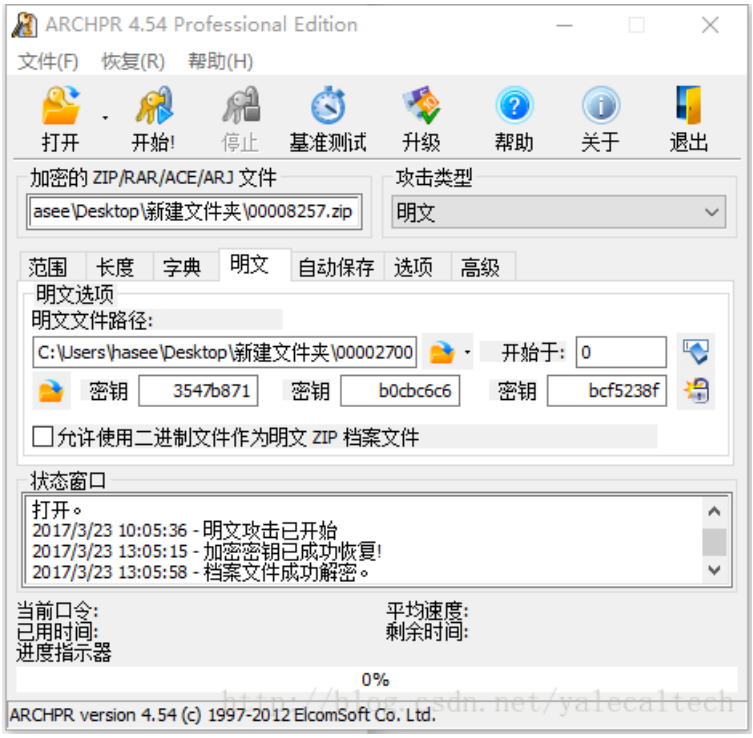

得到

识图即可

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