

BUU-MISC-[ACTF新生赛2020]明文攻击

原创

TzZzEZ-web 于 2021-05-27 19:04:19 发布 717 收藏 1

分类专栏: [BUU-MISC](#)

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_24033605/article/details/117332963

版权



[BUU-MISC 专栏收录该内容](#)

45 篇文章 1 订阅

订阅专栏

[ACTF新生赛2020]明文攻击

得到一张图片和一个加密的压缩包。

binwalk分析一下图片。

```
(root@kali)~[~/桌面]
# binwalk woo.jpg

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
16733       0x415D      End of Zip archive, footer length: 22
```

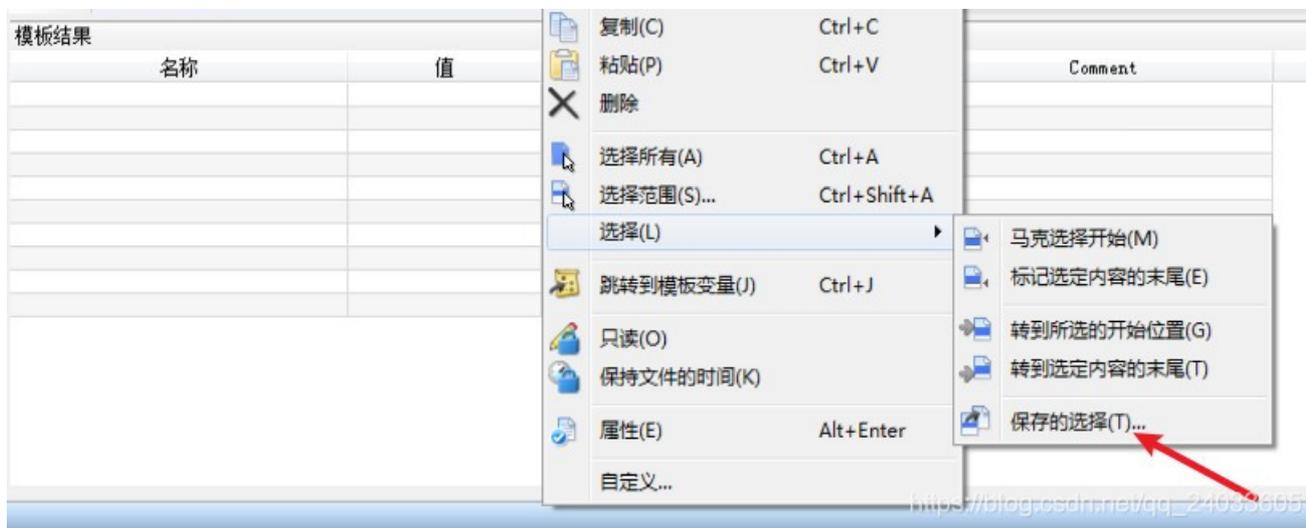
发现图片是以zip文件结尾, 但是分解不出来。

查看16进制码。

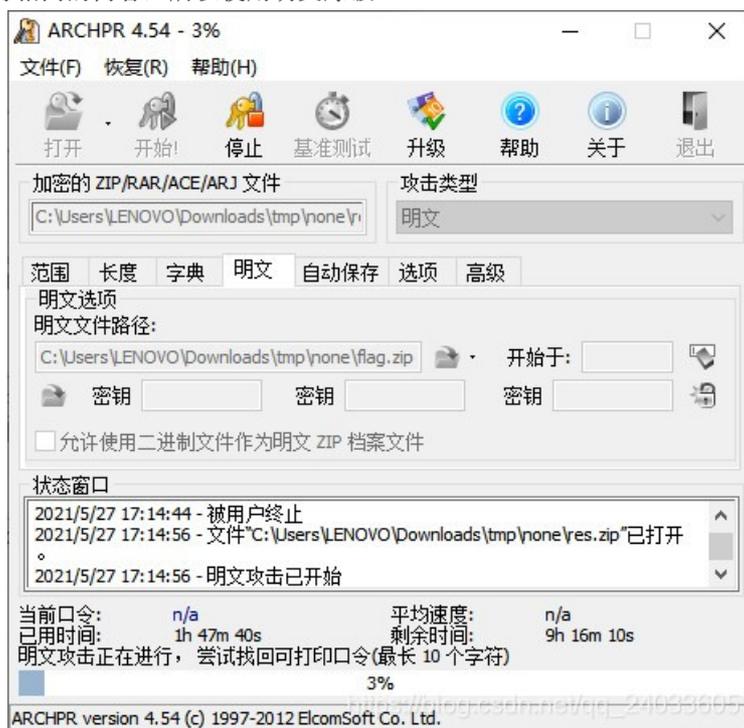
补充zip文件头, 并以zip格式保存。

```
32 32 32 32 32 32 32 32 32 32 32 32 32 50 4B 03 04 222222222222PK..
14 00 00 00 08 00 CB A2 82 4F D8 30 C5 B0 11 00 .....Ëc,O00Å°..
00 00 11 00 00 00 08 00 00 00 66 6C 61 67 2E 74 .....flag.t
78 74 2B C9 C8 2C 56 00 A2 92 8C 54 85 B4 9C C4 xt+ËË,V.c'ËT...'œÅ
74 3D 00 50 4B 01 02 14 00 14 00 00 00 08 00 CB t=.PK.....Ë
A2 82 4F D8 30 C5 B0 11 00 00 00 11 00 00 00 08 c,O00Å°.....
00 24 00 00 00 00 00 00 00 20 00 00 00 00 00 00 .$.
00 66 6C 61 67 2E 74 78 74 0A 00 20 00 00 00 00 .flag.txt..
00 01 00 18 00 01 02 2B 25 0B A9 D5 01 1D 7B 6F .....+Ë.ËÖ..{o
54 0B A9 D5 01 79 58 D8 1C 0B A9 D5 01 50 4B 05 T.ËÖ.yXË..eÖ.PK.
06 00 00 00 00 01 00 01 00 5A 00 00 00 37 00 00 .....Z...7...
00 00 00
```

```
启动 woo.jpg*
编辑为: 十六进制(0) 运行脚本 运行模板
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
4090h: 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
40A0h: 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
40B0h: 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
40C0h: 32 32 32 32 32 32 32 32 32 32 32 32 50 4B 03 04 222222222222PK..
40D0h: 14 00 00 00 08 00 CB A2 82 4F D8 30 C5 B0 11 00 .....Ëc,O00Å°..
40E0h: 00 00 11 00 00 00 08 00 00 00 66 6C 61 67 2E 74 .....flag.t
40F0h: 78 74 2B C9 C8 2C 56 00 A2 92 8C 54 85 B4 9C C4 xt+ËË,V.c'ËT...'œÅ
4100h: 74 3D 00 50 4B 01 02 14 00 14 00 00 00 08 00 CB t=.PK.....Ë
4110h: A2 82 4F D8 30 C5 B0 11 00 00 00 11 00 00 00 08 c,O00Å°.....
4120h: 00 24 00 00 00 00 00 00 00 20 00 00 00 00 00 00 .$.
4130h: 00 66 6C 61 67 2E 74 78 74 0A 00 20 00 00 00 00 .flag.txt..
4140h: 00 01 00 18 00 01 02 2B 25 0B A9 D5 01 1D 7B 6F .....+Ë.ËÖ..{o
4150h: 54 0B A9 D5 01 79 58 D8 1C 0B A9 D5 01 50 4B 05 T.ËÖ.yXË..eÖ.PK.
4160h: 06 00 00 00 00 01 00 01 00 5A 00 00 00 37 00 00 .....Z...7...
4170h: 00 00 00
```



得到flag.txt，和加密压缩包中有相同的内容，所以使用明文爆破。



常规爆破即可。

flag{3te9_nbb_ahh8}