攻防世界 Misc高手进阶区 2分题 再见李华

原创

思源湖的鱼 于 2020-10-28 10:32:19 发布 1102 收藏

分类专栏： ctf 文章标签： 攻防世界 ctf misc 网络安全

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109314033

前言

继续ctf的旅程

攻防世界Misc高手进阶区的2分题

本篇是再见李华的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

下下来一个jpg文件

扔进stegsolve

没有发现

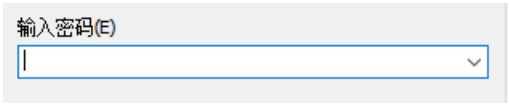
扔进ps

没有发现

扔进winhex
发现文件包含

```
00019136  FF 00 B6 6B FE 14 9F 65  B6 52 71 6F 0F 5F EE 0A  ÿ ¶kþ Ÿe¶Rqo _î
00019152  3E A9 E6 1E DF C8 F2 2B  5F 15 47 28 53 E7 6E 95  >©æ ßÈò+_ G(Sçn•
00019168  B8 7D 9F 2E 58 0E A4 7F  0F 1C E2 AB 5D F8 99 2E  ¸}Ÿ.X ¤  â«]ø™.
00019184  95 63 82 34 96 49 3E 45  25 C2 A1 EE 46 73 DB 9F  •c‚4–I>E%Â¡îFsÛŸ
00019200  C0 57 B4 08 20 C9 3E 44  59 FF 00 70 52 43 6D 6E  ÀW´  É>DYÿ pRCmn
00019216  BF 72 DE 24 E7 F8 50 0A  7F 54 F3 17 B7 F2 38 DF  ¿rÞ$çøP  Tó ·ò8ß
00019232  86 F6 D6 B0 43 A9 B5 B0  2E 0C A8 8F 39 52 16 46  †öÖ°C©µ°. ¨ 9R F
00019248  00 92 14 9E A1 77 63 34  57 74 00 03 00 62 8A EB  ' ž¡wc4Wt  bŠë
00019264  84 2D 14 8C 5B BB B9 FF  D9 50 4B 03 04 14 00 01  „- Œ[»¹ÿÙPK
00019280  08 08 00 ED A1 0B 49 05  02 71 1B 25 00 00 00 1A     í¡ I  q %
00019296  00 00 00 07 00 00 00 6B  65 79 2E 74 78 74 1F B8        key.txt ¸
00019312  6D CB A3 14 44 0A 7B 05  9B B6 EA 30 C9 9E 7C C2  mË£ D { ›¶ê0Éž|Â
00019328  AF B2 CF 43 47 6A 85 68  0B 8A 76 FB D5 C7 F2 EF  ¯²ÏCGj…h ŠvûÕÇòï
00019344  99 45 98 50 4B 01 02 3F  00 14 00 01 08 08 00 ED  ™E˜PK  ?       í
00019360  A1 0B 49 05 02 71 1B 25  00 00 00 1A 00 00 00 07  ¡ I  q %
00019376  00 24 00 00 00 00 00 00  00 20 00 00 00 00 00 00   $
00019392  00 6B 65 79 2E 74 78 74  0A 00 20 00 00 00 00 00   key.txt
00019408  01 00 18 00 B2 8D 26 0A  CA F3 D1 01 B2 8D 26 0A      ² & ÊóÑ ² &
00019424  CA F3 D1 01 A1 97 97 00  AC F3 D1 01 50 4B 05 06  ÊóÑ ¡-- ¬óÑ PK
00019440  00 00 00 00 01 00 01 00  59 00 00 00 4A 00 00 00          Y   J
00019456  00 00
```


改后缀
解压



需要密码

大概是原图片的md5？
先爆破试试

失败

回头看眼提示

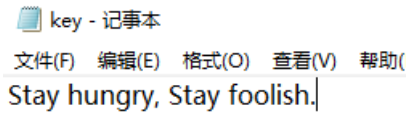
```
假如你是李华（LiHua），收到乔帮主一封密信，没有任何特殊字符，请输入密码，不少于1000个字。同学，记得署名哦～
```

这里的1000如果作为二进制，就是8
所以密码不小于8位
然后可能最后是LiHua
那就用AZPR爆破

Total passwords	12,850,617
Total time	875ms
Average speed (passwords per second)	14,686,419
Password for this file	15CCLiHua
Password in HEX	31 35 43 43 4c 69 48 75 61

得到密码

解压
得到key.txt



得到flag

结语

提示有点点绕
没想明白md5是咋回事儿