

CTF-misc-----buuctf-FLAG

原创

旧日难忘 于 2020-05-24 12:42:52 发布 1671 收藏 4

分类专栏: [ctf MISC](#) 文章标签: [linux](#)

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/weixin_43821278/article/details/106313486

版权



ctf 同时被 2 个专栏收录

11 篇文章 0 订阅

订阅专栏



MISC

1 篇文章 0 订阅

订阅专栏

CTF-MISC

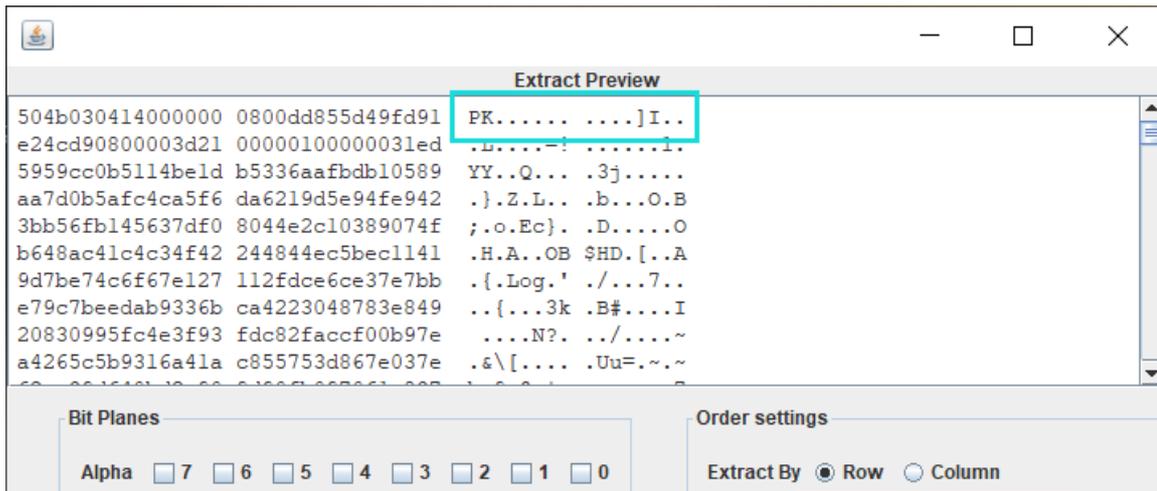
BUUctf misc-> FLAG

最近做 **buuctf-misc**, 在 **FLAG** 卡了很久。因为没有提示, 所以度了一下, 有一个博客, 但是不详细, 故在这再写一下

MISC-图片

1. 右键—属性, 看大小 (可能藏文件), 看备注之类的
2. linux下用 `foremost` 命令分离, windows用一个我忘了名字的exe (可找我要)。看看有没有结果
3. `ultraedit` 查看具体内容, 观察有没有特殊情况; 或者上 `stego`, 然后各种 `analysis` 都试试。
4. gif 可以用 `stego` 帧查看, 然后就是 **LSB** 隐写, `red`, `blue`, `green\0`, 导出 `zip`, `png`, `jpg` 等等, 根据头的标志。
5. 最后不行上 `binwalk` 命令, `png` 图片可以用 `pngcheck` 命令检查。
6. 其他的水平有限, 想不起或者知道了。

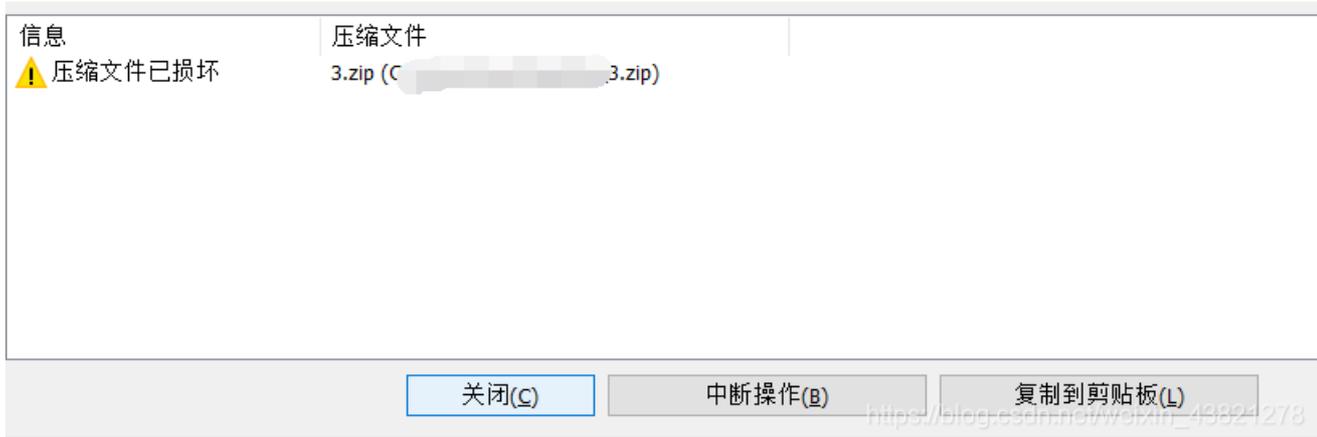
本题的 **LSB** 发现是看博客的,



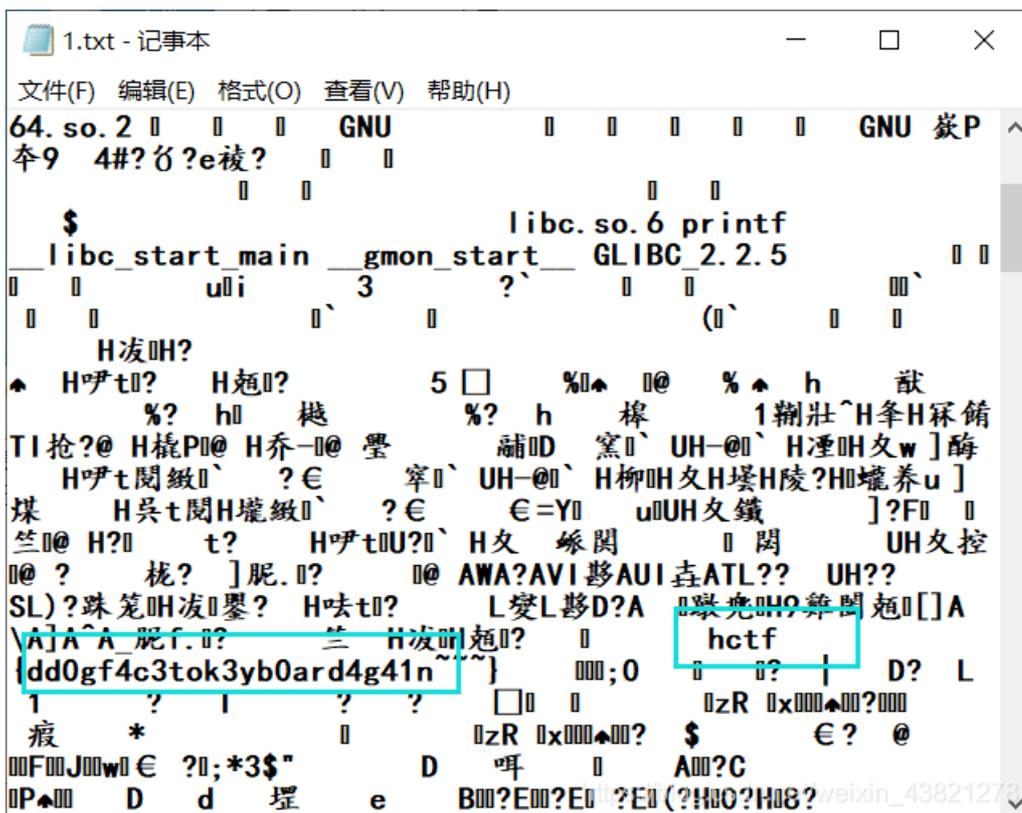


导出为3.zip, 解压却发现

WinRAR:诊断信息



这个时候可以用zip修复软件, http://forspeed.onlinedown.net/down/95222_20170619151215.zip
修复后解压后是个1文件, 无后缀, windows可以改为1.txt看,



linux 可以 grep -a '{*}' 1

```
root@louis:~/home/1# grep -a '{*}' 1
LF
8@ 8@ > @@ @ p @ 8 @ @@ @ @ ? ? 8 E
D 0 8 P 鸚 ? ?@ ?@ 4 4 Q 鸚 T T@ T@ D
R 鸚 ? ? /lib64/ld-linux-x86-64.so.2 GNU
GNU 9py#?eD?ebl?
$ ui 3 ?` libc.so.6 printf __libc_start_main __gmon_start__ GLIBC_2.2.5
H? H? y5 y% @ y%
H[] ? y? ,@ UH-@` H,H 鸚H?Hψu]ú HV[]p@` y? =Y uUH 鸚y?]?F
yUH 忘@ ? 鋒y]; @ AWA?AVI[]dTL?? UH?? SL)?鸚取yH? L 鐳[]y;AH9 [ ]A\A]A^A_!f.? 鸚? h
ctf{dd0gf4c3tok3yb0ard4g41n~~~} 0 ?y| D?yL 1y?y? Tyy? ?y? https://blog.csdn.net/weixin_43821278
```