BUUCTF misc 面具下的flag

原创

Warning 于 2019-10-02 20:02:30 发布 4161 收藏 2
分类专栏： 杂项 文章标签： vmdk

给了一个.jpg的图片，用winhex打开后发现文件的结尾并不是FF D9

```
AD 40 12 A8 A8 46 C2 C7  3F 85 11 4F FF D9 50 4B  瓗.?'虑??.O  PK
03 04 14 00 00 00 08 00  6C 87 42 49 56 A1 A2 02  ........l?BIV???
A7 58 02 00 00 00 30 00  09 00 00 00 66 6C 61 67    ....0.....flag
2E 76 6D 64 6B EC DA 7D  88 0C 71 1C C7 F1 DF 9D  .vmdk?趧??q.邱?K
E7 F1 EC 70 45 31 ED 15  45 CE ED DE 93 A3 23 77  珩藹E1?.E?磙揑#w
EB F1 F2 D0 9D EE 8A C2  EC CE EC DE B8 B5 73 ED  腾蛐.?婷煳燹傅s?
AE F3 54 5C 14 45 51 14  45 51 14 45 51 14 45 51    T\.EQ.EQ.EQ.EQ
```

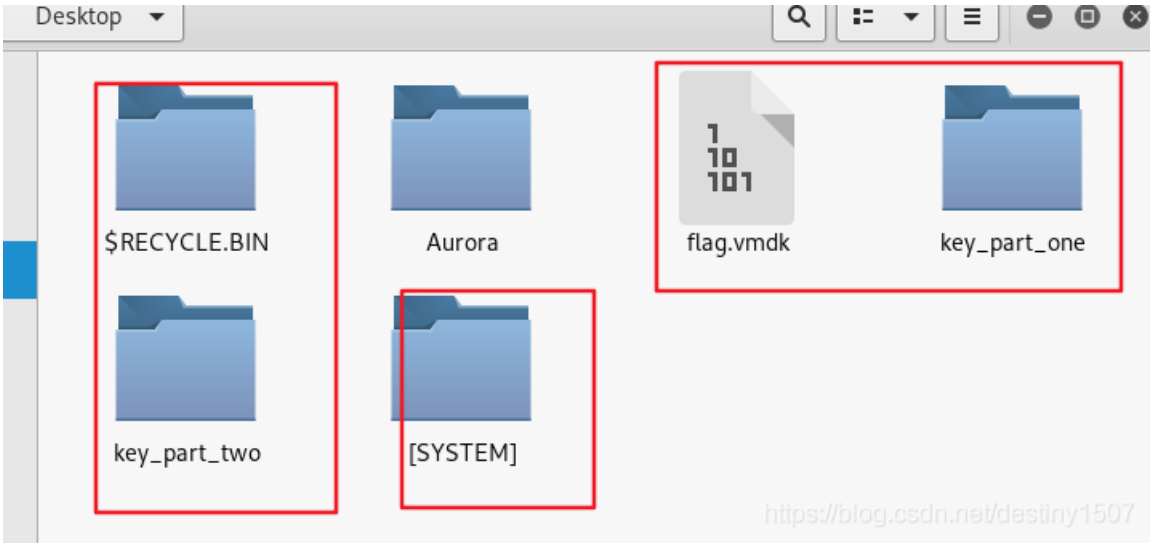
紧接着后面是50 4B 03 04，是.zip文件的文件头，有伪加密，修改后成功解压，得到一个flag.vmdk虚拟机磁盘文件。

然后……我以为是内存取证题目呢（菜

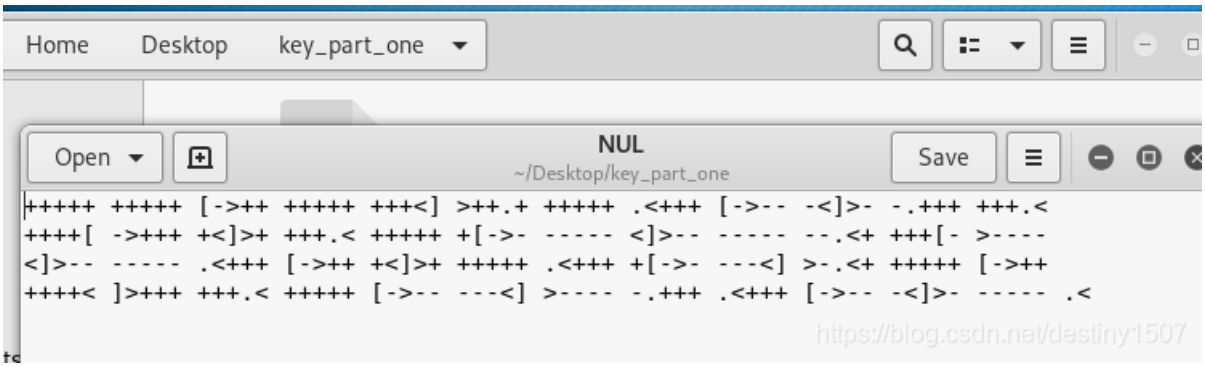
然后用volatility分析了半天连个操作系统信息都分析不出来（泪

后来百度了题解（颓

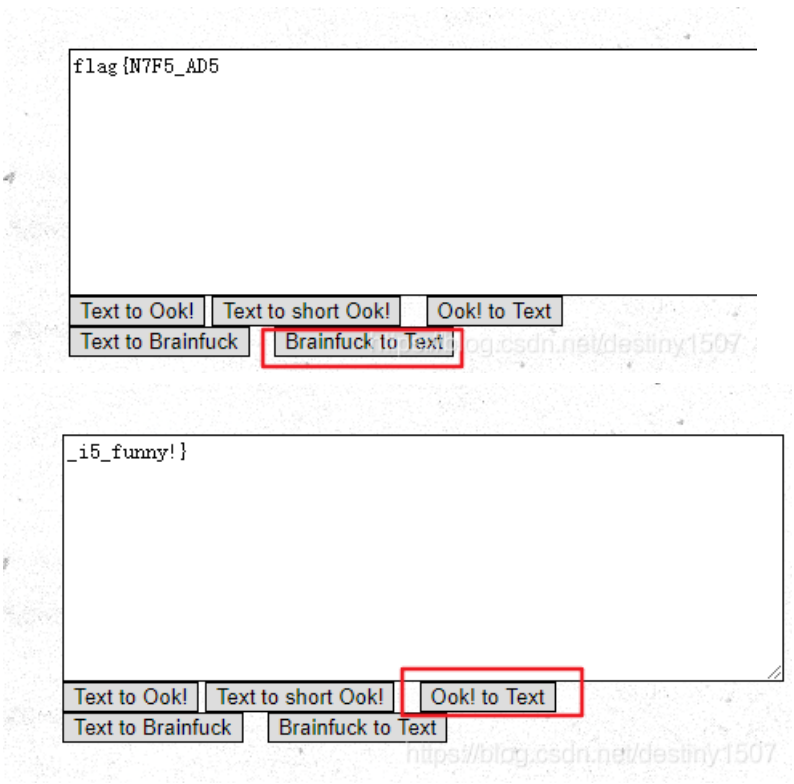
用7z解压缩后得到了很多个文件夹，



其中key_part_one和key_part_two中含有Ook!与Brainfuck加密得到的文本，解密后将得到的字符串前拼接起来就得到了flag:


Home
Desktop
key_part_one
Open
NUL
~/Desktop/key_part_one
Save
+++++ +++++ [->++ +++++ +++<] >++.+ +++++ .<+++ [->-- -<]>- -.+++ +++.<
++++[->+++ +<]>+ +++.< +++++ +[->- ----- <]>-- ----- --.<+ +++[- >----
<]>-- ----- .<+++ [->++ +<]>+ +++++ .<+++ +[->- ---<] >-.<+ +++++ [->++
++++<]>+++ +++.< +++++ [->-- ---<] >---- -.+++ .<+++ [->-- -<]>- ----- .<


Open
where_is_flag_part_two.txt:flag_part_two_is_here.txt
~/Desktop/key_part_two
Save
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook?
Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook!
Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook.
Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook?
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook! Ook.
Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook!
Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook?
Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook! Ook. Ook?
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook.
Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook!
Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!


flag{N7F5_AD5
Text to Ook!
Text to short Ook!
Ook! to Text
Text to Brainfuck
Brainfuck to Text
_i5_funny!}
Text to Ook!
Text to short Ook!
Ook! to Text
Text to Brainfuck
Brainfuck to Text

但是我并不知道为什么.vmdk文件为什么可以用7z解压缩，难道.vmdk文件就是用7z的压缩算法生成的？我没有找到讲解的资料……先挖个坑吧。