

BUUCTF 面具下的flag writeup

原创

碧羽o(*^▽^*)づ回雪 于 2021-10-15 12:47:59 发布 78 收藏

分类专栏: [CTF writeup](#) 文章标签: [python](#)

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/zhangzhaolin12/article/details/120780770>

版权



[CTF writeup](#) 专栏收录该内容

16 篇文章 0 订阅

订阅专栏

下载后是一张图, 010打开后后面是压缩包。直接分离出来, 解压时发现需要密码, 但是暂时找不到密码提示, 那就在010里搜索504b, 查看每一个后面是否有14 00, 这个后面就是加密的标识, 发现其他都是00 00, 就一个09 00, 显然就是伪加密了(如果都是09 00, 可能就不是伪加密了, 但这是可能, 就算都是09 00也可能是伪加密), 手工改成00 00。

```
00 00 00 00 00 00 00 00 00 00 00 90 F1 07 50 4B
01 02 3F 00 14 00 09 00 08 00 6C 87 42 49 56 A1
A2 02 A7 58 02 00 00 00 30 00 09 00 24 00 00 00
00 00 00 00 20 00 00 00 00 00 00 00 66 6C 61 67
2E 76 6D 64 6B 0A 00 20 00 00 00 00 00 01 00 18
```

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 90 F1 07 50 4B
01 02 3F 00 14 00 00 00 08 00 6C 87 42 49 56 A1
A2 02 A7 58 02 00 00 00 30 00 09 00 24 00 00 00
00 00 00 00 20 00 00 00 00 00 00 00 66 6C 61 67
```

解压后是一个wmware的虚拟磁盘文件。

名称	修改日期	类型	大小
flag.vmdk	2016/10/2 16:59	VMware 虚拟磁盘文件	3,072 KB

这个可以再kali里解压。

```
(root@kali) [~/桌面]
# 7z x flag.vmdk -o./

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
7zip Version 16.02 (locale=zh_CN.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (906EA),ASM,AES-NI)

Scanning the drive for archives:
1 file, 3145728 bytes (3072 KiB)

Extracting archive: flag.vmdk
```

解压后, flag分在了两个文件里, key_part_one和key_part_two,这两个是两种加密, 可以说是两种编码 (brainfack和ook) 在 [在线解密工具](#)。

这里还有一个brainfack的离线工具。

链接: <https://pan.baidu.com/s/1Qyh3CXRIIsYhAZ8CXg7P2w>

提取码: 4mnt

但是ook的离线工具我没有, 这里发一个求助, 希望有ook解密工具或者解密脚本的小伙伴能分享给我一份, 我这里也有

不少工具，大家需要的话我也可以分享给大家。

```
1 ++++++ ++++++ [→++ ++++++ ++<] >+., ++++++ .<+++ [→ — <] > — .,+++ +++.<
2 +++++[ →+++ +<]>+ +++.< ++++++ +[→ — <]> — — .<+ +++[- > —
3 <]> — — .<+++ [→++ +<]>+ ++++++ .<+++ +[→ — <] >.<+ ++++++ [→++
4 +++++< ]>+++ +++.< ++++++ [→ — <] > — — .,+++ .<+++ [→ — <]> — — .<
```

CSDN @几味^少年

```
1 0ok. 0ok.
2 0ok. 0ok. 0ok. 0ok! 0ok? 0ok! 0ok! 0ok. 0ok? 0ok. 0ok. 0ok. 0ok. 0ok.
3 0ok. 0ok? 0ok. 0ok?
4 0ok! 0ok. 0ok? 0ok. 0ok.
5 0ok. 0ok.
6 0ok. 0ok! 0ok. 0ok? 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok! 0ok? 0ok! 0ok!
7 0ok. 0ok? 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok? 0ok. 0ok? 0ok! 0ok. 0ok?
8 0ok. 0ok! 0ok. 0ok? 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok.
9 0ok. 0ok. 0ok. 0ok. 0ok! 0ok? 0ok! 0ok! 0ok. 0ok? 0ok! 0ok! 0ok! 0ok!
10 0ok! 0ok! 0ok! 0ok! 0ok! 0ok! 0ok! 0ok! 0ok! 0ok? 0ok. 0ok? 0ok! 0ok. 0ok?
11 0ok! 0ok! 0ok! 0ok! 0ok! 0ok! 0ok! 0ok. 0ok? 0ok. 0ok. 0ok. 0ok. 0ok.
12 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok! 0ok? 0ok! 0ok! 0ok. 0ok? 0ok. 0ok.
13 0ok. 0ok? 0ok. 0ok? 0ok! 0ok.
14 0ok? 0ok. 0ok! 0ok.
15 0ok. 0ok!
16 0ok. 0ok? 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok! 0ok? 0ok! 0ok! 0ok. 0ok?
17 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok? 0ok. 0ok? 0ok! 0ok. 0ok? 0ok. 0ok.
18 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok! 0ok! 0ok! 0ok! 0ok!
19 0ok! 0ok. 0ok! 0ok. 0ok?
20 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok. 0ok! 0ok? 0ok! 0ok! 0ok. 0ok? 0ok. 0ok.
21 0ok. 0ok. 0ok. 0ok. 0ok? 0ok. 0ok? 0ok! 0ok. 0ok? 0ok. 0ok. 0ok. 0ok!
```

CSDN @几味^少年