密码柜

发表于 2021-01-04 分类于 Challenge， 2020， 网鼎杯， 白虎场， Misc
Challenge | 2020 | 网鼎杯 | 白虎场 | Misc | 密码柜

点击此处获得更好的阅读体验

题目考点

- *内存取证*
- *KeePass密钥恢复*
- *Bitlocker密钥恢复*

解题思路

夏风师傅的取证题，十分的硬核和复杂。首先打开一个vmem文件和Database.kdbx文件，kdbx文件使用`KeePass`软件读取，需要一个密码，应该是在win10的vmem中找。于是取证大师一把梭（其实也可以使用volatility，但是十分麻烦，还是取证大师一把梭简单），数据恢复后得到

查找txt有个

打开后是

```
1 密码柜的密码可不能忘了，毕竟那里面存着我最重要的东西
2 而且我走哪都要带着它
3 6s4mxkhvge
```

用这个`KeePass`的密码解密，得到

这也是一种加密，密钥就是main_key，里面有一个Advanced，可以把里面一个something.kge文件导出，密码就是main_key：`XLlArBkn`。导出后再使用`KGB Archiver`对数据进行解压，得到一个BitLocker硬盘，但是没有密钥文件，猜测还是再vmem的win10镜像中，使用`Elcomsoft Password Recovery`对vmem进行提取，得到

导出后双击挂载解压的BitLocker硬盘，然后再用`Elcomsoft Password Recovery`对用刚刚导出的密钥对BitLocker硬盘进行解密

然后就可以得到BitLocker的恢复密钥

```
1 294173-189123-573023-455081-459382-434610-344091-286275
```

输入恢复密钥即可解锁进入硬盘

里面是一个自解压程序，打开这个程序后发现

aux是windows里的一种保留字，强行保存也打不开文件，所以我们对其进行重命名，之后用命令行对其进行cat操作

是一个PNG图片，那就加一个后缀名打开，得到flag

Flag

```
flag{700cf8df-0444-46a4-afd2-22dcce208a67}
```


 # Challenge # 2020 # Misc # 网鼎杯 # 白虎场
逆转思维
boom