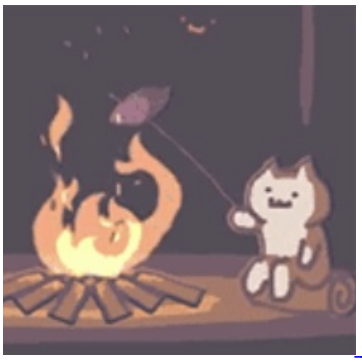
[ctf misc][RCTF2019]disk

原创

shu天 于 2021-08-08 15:01:47 发布 54 收藏

分类专栏： ctf 文章标签： ctf misc



ctf 专栏收录该内容

81 篇文章 4 订阅

订阅专栏

Writeup

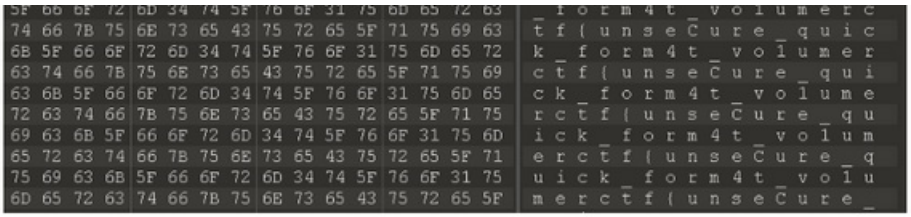
[RCTF2019]disk

> 知识点：
> vmdk虚拟磁盘处理
> 加密容器

[RCTF2019]disk

> 文件：encrypt.vmdk
>
> 题目：An otaku used VeraCrypt to encrypt his favorites.
>
> Password: `rctf`
>
> Flag format: `rctf{a-zA-Z0-9_}`

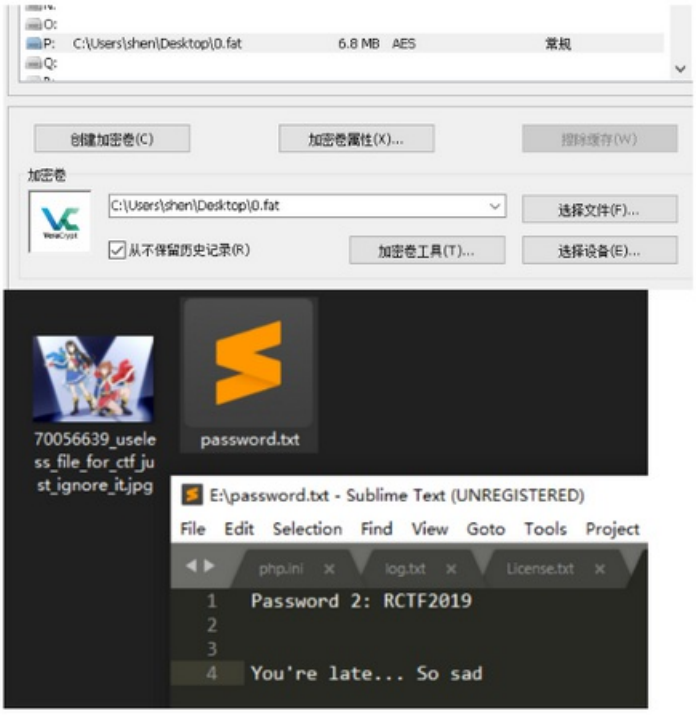
vmdk，尝试winhex和x-ways打开都报错，只能用010查看二进制，发现其中有一部分flag




```
1 rctf{unseCure_quick_form4t_volume
```

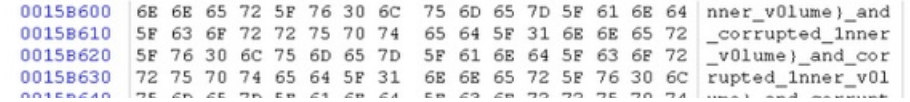
然后知道了vmdk可以用7z解压，得到一个0.fat

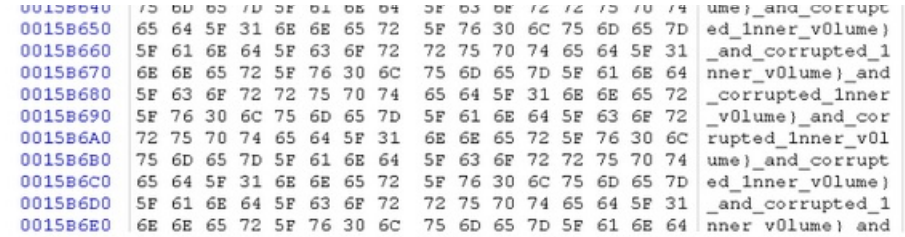
怀疑是个加密容器，利用veracrypt挂起，猜密码是rctf



发现里面有`password.txt`写了密码`Password 2: RCTF2019`，veracrypt在挂载输入密码的时候，不同的密码可以进入不同的文件系统。

新挂起的分区看不到文件系统类型和分区大小，还是只能winhex强行看，得到后半flag





```
0015B640  75 6D 65 7D 5F 61 6E 64  5F 63 6F 72 72 75 70 74  ume}_and_corrupt
0015B650  65 64 5F 31 6E 6E 65 72  5F 76 30 6C 75 6D 65 7D  ed_1nner_v0lume}
0015B660  5F 61 6E 64 5F 63 6F 72  72 75 70 74 65 64 5F 31  _and_corrupted_1
0015B670  6E 6E 65 72 5F 76 30 6C  75 6D 65 7D 5F 61 6E 64  nner_v0lume}_and
0015B680  5F 63 6F 72 72 75 70 74  65 64 5F 31 6E 6E 65 72  _corrupted_1nner
0015B690  5F 76 30 6C 75 6D 65 7D  5F 61 6E 64 5F 63 6F 72  _v0lume}_and_cor
0015B6A0  72 75 70 74 65 64 5F 31  6E 6E 65 72 5F 76 30 6C  rupted_1nner_v0l
0015B6B0  75 6D 65 7D 5F 61 6E 64  5F 63 6F 72 72 75 70 74  ume}_and_corrupt
0015B6C0  65 64 5F 31 6E 6E 65 72  5F 76 30 6C 75 6D 65 7D  ed_1nner_v0lume}
0015B6D0  5F 61 6E 64 5F 63 6F 72  72 75 70 74 65 64 5F 31  _and_corrupted_1
0015B6E0  6E 6E 65 72 5F 76 30 6C  75 6D 65 7D 5F 61 6E 64  nner_v0lume}_and
```

```
_and_corrupted_1nner_v0lume}
```

总结：这鬼东西，根本不能正常思维看，里面的两个文件系统都是坏的可能，只能强行找字符串