2021陇剑杯网络安全大赛wp-内存取证（详细题解）

原创

偷一个月亮 于 2021-09-15 14:28:11 发布 1393 收藏 1

分类专栏： 2021陇剑杯网络安全大赛 CTF 文章标签： 网络安全

本文链接：https://blog.csdn.net/yiqiushi4748/article/details/120307882

2021陇剑杯网络安全大赛 同时被 2 个专栏收录

8 篇文章 46 订阅

订阅专栏

CTF

43 篇文章 5 订阅

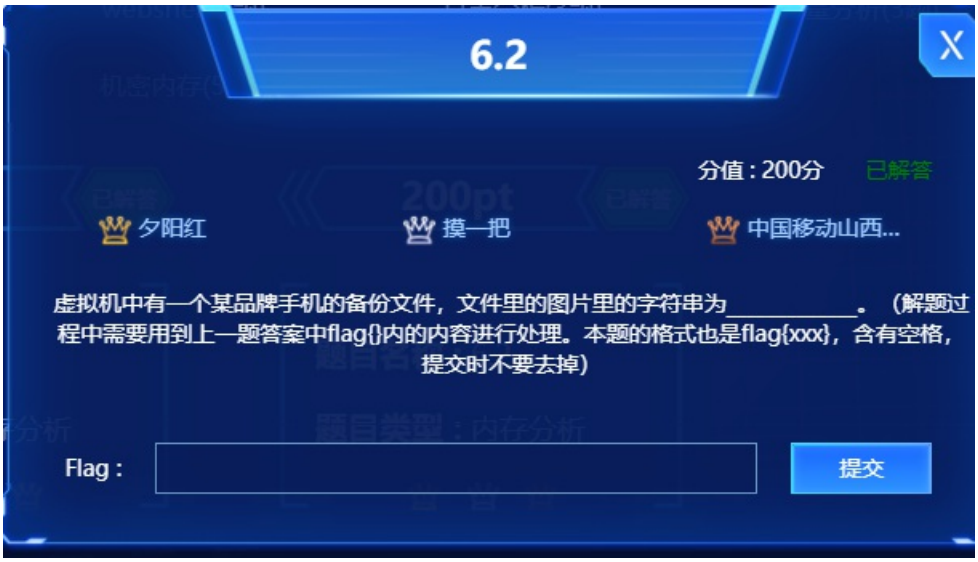
订阅专栏

6.1

使用volatility对内存进行分析，配合mimikatz插件跑密码

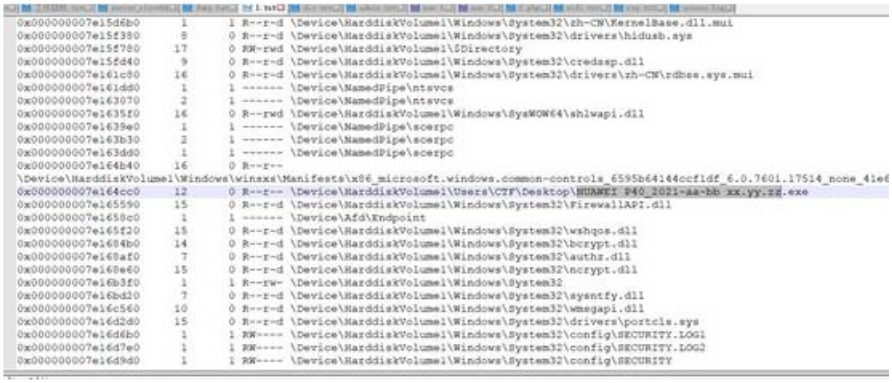
```
root@m3rser:~/桌面# volatility -f Target.vmem --profile=Win7SP1x64 mimikatz
Volatility Foundation Volatility Framework 2.6
Module   User             Domain           Password
-------- ---------------- ---------------- ------------------------------------
wdigest  CTF              WIN-QUN5RVOOF27  flag{W31C0M3 T0 THiS 34SY F0R3NSiCX}
wdigest  WIN-QUN5RVOOF27$ WORKGROUP
root@m3rser:~/桌面#
```

6.2



根据提示，使用filescan命令在内存中查找文件，发现华为备份文件

HUAWEI P40_2021xxxxxx，搜索后发现多个相关文件，最后发现HUAWEI P40_2021-aa-bb xx.yy.zz.exe 为一自解压文件，解压后即为备份



找到解密工具kobackupdec，根据上一步提示，根据提示将空格替换为_，解密成功

flag{TH4NK Y0U FOR DECRYPTING MY DATA}