secret

发表于 2021-01-16 分类于 Challenge， 2019， 安洵杯， Misc
Challenge | 2019 | 安洵杯 | Misc | secret

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/6911

题目考点

- *内存取证*

解题思路

内存取证，直接上volatility
`volatility -f mem.dump imageinfo`

看进程

`volatility -f mem.dump --profile=Win7SP1x64 pslist`

看cmd历史

`volatility -f mem.dump --profile=Win7SP1x64 cmdscan`

得到 `flag.ccx_password_is_same_with_Administrator`

从桌面导出文件flag.ccx

`volatility -f mem.dump --profile=Win7SP1x64 dumpfiles -Q 0x000000003e435890 -D ./`

hashdump得到Administrator的哈希

`volatility -f mem.dump --profile=Win7SP1x64 hashdump`

得到
`Administrator:500:6377a2fdb0151e35b75e0c8d76954a50:0d546438b1f4c396753b4fc8c8565d5b:::`

cmd5解密得到`ABCabc123`

然后在进程中或者桌面看到有一个Cncrypt的应用，百度下载该应用然后用ABCabc123解密挂载，得到flag

Flag

```
1 flag{now_you_see_my_secret}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/安洵杯/Misc/cKvU3hYvLofgUvthcG5wQN.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # Misc # 2019 # 安洵杯
吹着贝斯扫二维码
Attack