EzMemory

发表于 2021-01-04 分类于 Challenge， 2019， 湖湘杯， Misc
Challenge | 2019 | 湖湘杯 | Misc | EzMemory

点击此处获得更好的阅读体验

题目考点

- *内存取证*

解题思路

解法一

这个题目直接解压后对目标文件mem.raw进行二进制搜索就可以搜到flag，具体的操作如下：

PS: 一个strings命令秒掉两个misc，emmm

```
~/Downloads/hxb2019
➜ strings mem.raw| grep flag{
flag{wiND0w5_M3m0RY_F0R3n5IC5}.lnk
flag{wiND0w5_M3m0RY_F0R3n5IC5}.txt
flag{wiND0w5_M3m0RY_F0R3n5IC5}.txt
flag{wiND0w5_M3m0RY_F0R3n5IC5}.lnk
flag{wiND0w5_M3m0RY_F0R3n5IC5}.lnk
notepad  "flag{wiND0w5_M3m0RY_F0R3n5IC5}.txt"
```

解法二

拿到一个mem.raw，上volatility

```
volatility -f mem.raw imageinfo
```

获取镜像系统信息--profile=Win7SP1x64指定操作系统

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

列出所有进程，发现有一个cmd进程

查看命令行上的操作发现flag

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

FLAG

```
flag{wiND0w5_M3m0RY_F0R3n5IC5}
```


 # Challenge # Misc # 2019 # 湖湘杯
argument
ezre