

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

```
1 ~/Downloads/hxb2019
2 → strings mem.raw | grep flag{
3 flag{wiND0w5_M3m0RY_F0R3n5IC5}.lnk
4 flag{wiND0w5_M3m0RY_F0R3n5IC5}.txt
5 flag{wiND0w5_M3m0RY_F0R3n5IC5}.txt
6 flag{wiND0w5_M3m0RY_F0R3n5IC5}.lnk
7 flag{wiND0w5_M3m0RY_F0R3n5IC5}.lnk
8 notepad "flag{wiND0w5_M3m0RY_F0R3n5IC5}.txt"
```

解法二

拿到一个mem.raw，上volatility

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

获取镜像系统信息--profile=Win7SP1x64指定操作系统

□

```
1 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

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

FLAG

```
1 flag{wiND0w5_M3m0RY_F0R3n5IC5}
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2019/湖湘杯/Misc/qQ4E93zWiKqo5Yvn8ocJjn.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](#) [# 湖湘杯](#)
[argument](#)
[ezre](#)