


内存取证常见例题思路方法–volatility (没有最全 只有更全)

原创路baby已于 2023-02-24 17:00:21 修改阅读量2.9k收藏34点赞数7

分类专栏：内存取证文章标签：服务器网络安全内存取证volatility

内存取证 专栏收录该内容

19 订阅4 篇文章

目录


- 1.从内存文件中获取到用户hacker 的密码并且破解密码，将破解后的密码作为 Flag值提交;
 - 2.获取当前系统的主机名，将主机名作为Flag值提交;
 - 3.获取当前系统浏览器搜索过的关键词，作为Flag提交;
 - 4.获取当前内存文件的 ip地址
 - 5.当前系统中存在的挖矿进程，请获取指向的矿池地址，将矿池的IP地址作为. Flag值提交(局域网ip);.
 - 6.恶意进程在系统中注册了服务，请将服务名以 Flag{服务名}形式提交。
 - 7.请将内存文件中的剪贴板内容作为flag 值提交;
 - 8.从内存文件中获取记事本的内容，并将该内容作为flag值提交;
 - 9.从内存文件中获取截图的内容，并将该内容作为flag值提交;
 - 10.从内存文件中获取黑客进入系统后下载的图片，将图片中的内容作为 Flag值提交。
 - 11.查看被删除的文件里的内容
 - 12.最后一次更新时间，运行过的次数为 Flag值提交。
 - 13.将最后一次cmd的命令当作flag
- 加油各位(´ω`)y 期待与君再相逢

决定出一期内存取证常见题型的文章，利于诸君平时做题 文章也会持续更新

如果需要详细的安装教程和插件使用请查看以下文章

内存取证-volatility工具的使用 （史上更全教程，更全命令）_路baby的博客-CSDN博客

内存取证-volatility工具的使用 （史上更全教程，更全命令）安装步骤 命令解析 工具插件分析 例题讲解

 https://blog.csdn.net/m0_68012373/article/details/127419463

1.从内存文件中获取到用户hacker 的密码并且破解密码，将破解后的密码作为 Flag值提交;

先获取内存文件的profile，使用imageinfo 插件即可

volatility -f xxx.vmem imageinfo

使用 "SAM\Domains\Account\Users\Names"查看用户（这一步可有可无）

volatility -f xxx.vmem --profile=[操作系统] printkey -K "SAM\Domains\Account\Users\Names"

破密码

volatility -f xxx.vmem --profile=[操作系统] hashdump(hashcat或者john 去破解)

volatility -f xxx.vmem --profile=[操作系统] mimikatz

volatility -f xxx.vmem --profile=[操作系统] lsadump

2.获取当前系统的主机名，将主机名作为Flag值提交;


volatility -f xxx.vmem --profile=[操作系统] printkey -K "ControlSet001\Control\ComputerName\ComputerName"

volatility -f xxx.vmem --profile=[操作系统] envvars(查看环境变量)

3.获取当前系统浏览器搜索过的关键词，作为Flag提交;

volatility -f xxx.vmem --profile=[操作系统] iehistory

4.获取当前内存文件的 ip地址

路baby

关注

7



34



9



```
volatility -f xxx.vmem --profile=[操作系统] netscan
```

```
volatility -f xxx.vmem --profile=[操作系统] connscan
```

```
volatility -f xxx.vmem --profile=[操作系统] connections
```

5.当前系统中存在的挖矿进程, 请获取指向的矿池地址, 将矿池的IP地址作为. Flag值提交(局域网ip);

```
volatility -f xxx.vmem --profile=[操作系统] netscan(找唯一一个已建立的 ESTABLISHED)
```

6.恶意进程在系统中注册了服务, 请将服务名以 Flag{服务名}形式提交。

```
volatility -f xxx.vmem --profile=[操作系统] pslist -p [子进程号]
```

(子进程好上一题可知)

得到父进程

然后在通过svcsan可以查询服务名称, 根据父进程找到对应服务名

```
volatility -f xxx.vmem --profile=[操作系统] svcsan
```

7.请将内存文件中的剪贴板内容作为flag 值提交;

```
volatility -f xxx.vmem --profile=[操作系统] clipboard
```

8.从内存文件中获取记事本的内容, 并将该内容作为flag值提交;

```
volatility -f xxx.vmem --profile=[操作系统] editbox
```

```
volatility -f xxx.vmem --profile=[操作系统] notepad
```

9.从内存文件中获取截图的内容, 并将该内容作为flag值提交;

```
volatility -f xxx.vmem --profile=0S screenshot --dump-dir=.
```

10.从内存文件中获取黑客进入系统后下载的图片, 将图片中的内容作为 Flag值提交。

```
volatility -f xxx.vmem --profile=[操作系统] filesan | grep -E "png|jpg|gif|bmp|zip|rar|7z|pdf|txt|doc"
```

11.查看被删除的文件里的内容

```
volatility -f xxx.vmem --profile=[操作系统] mftparser
```

12.最后一次更新时间, 运行过的次数为 Flag值提交。

```
volatility -f xxx.vmem --profile=[操作系统] userassist
```

13.将最后一次cmd的命令当作flag

```
volatility -f xxx.vmem --profile=[操作系统] cmdscan
```

加油各位(̀ω´)y 期待与君再相逢💗

内存取证入门第二题

hacker_zrq的

题目链接。链接: https://pan.baidu.com/s/1byt9mF_IOBrXY_NYtlgNQ--来自百度网盘超级会员V2的分享。

中科磐云 内存取证.zip

磐云内存取证题目 2021中职 网络安全 试题4

9 条评论



南炼

热评

博主最后一次更新时间算做保存镜像时间吗

OtterCTF 内存取证_ctf内存取证

最近小小的学习了一下内存取证,装环境搞了整整一天,非常麻烦,在阅读相关资料时偶然看到了一篇WriteUp,是关于OtterCTF2018的十三道内存取证题目,用的全部是同一个

CTF 内存取证 USB流量分析

题目附件地址 目录 Baby_forensic 知识点: 内存取证工具volatility 的使用: 取证方法建议 Keyboard scan code: 解题过程: 1. Kali中解压文件 2. pslist查看进程 3. 通过cmdsc

Volatility工具——内存取证的解题思路步骤 最新
内存取证的实战题目。



路baby

关注

👍 7



★ 34



💬 9

