高校战“疫”网络安全分享赛-MISC-ez_mem&usb writeup

原创

me晴天 于 2020-03-10 23:05:59 发布 430 收藏 1
分类专栏： CTF

MISC-ez_mem&usb

binwalk发现两个压缩包，提取后但无法打开。

```
root@kali:~/桌面# binwalk c.pcap

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Libpcap capture file, little-endian, version
2.4, Ethernet, snaplen: 262144
3816          0xEE8           Zip archive data, at least v2.0 to extract, c
ompressed size: 40719149, uncompressed size: 134217728, name: data.vmem
42753990      0x28C5FC6       End of Zip archive, footer length: 22
42754861      0x28C632D       gzip compressed data, from Unix, last modifie
d: 1970-01-01 00:00:00 (null date)
42756440      0x28C6958       HTML document header
42756657      0x28C6A31       HTML document footer
42763051      0x28C832B       XML document, version: "1.0"
42764384      0x28C8860       XML document, version: "1.0"
42765522      0x28C8CD2       XML document, version: "1.0"
42767039      0x28C92BF       XML document, version: "1.0"
42769842      0x28C9DB2       Unix path: /var/www/html/upload
42774115      0x28CAE63       XML document, version: "1.0"
42775574      0x28CB416       XML document, version: "1.0"
42776712      0x28CB888       XML document, version: "1.0"
42779016      0x28CC188       Zip archive data, at least v2.0 to extract, c
ompressed size: 40719149, uncompressed size: 134217728, name: data.vmem
85572647      0x519BC27       End of Zip archive, footer length: 22
85573214      0x519BE5E       gzip compressed data, from Unix, last modifie
d: 1970-01-01 00:00:00 (null date)
85574791      0x519C487       HTML document header
```


使用Wireshark提取，得到一个镜像文件“data.vmem“

使用volatility进行分析

```
volatility -f data.vmem imageinfo
```

```
root@kali:~/桌面# volatility -f data.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2
x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/桌面/data.vmem)
                      PAE type : PAE
                           DTB : 0x b18000L
                          KDBG : 0x80546ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2020-02-24 07:56:47 UTC+0000
     Image local date and time : 2020-02-24 15:56:47 +0800
root@kali:~/桌面#
```



```
volatility -f data.vmem --profile=WinXPSP2x86 pslist
```

找到两个关键进程

```
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
                Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ --------------
-------------- ------------------------------
0x80ea2660 System                    4      0     52      231 ------      0

0xff57fc28 smss.exe                372      4      3       19 ------      0 2020-02-23 13:1
7:13 UTC+0000
0xff432020 csrss.exe               464    372     12      317      0      0 2020-02-23 13:1
7:13 UTC+0000
0xff435020 winlogon.exe            492    372     20      501      0      0 2020-02-23 13:1
7:13 UTC+0000
0xff445020 services.exe            668    492     16      253      0      0 2020-02-23 13:1
7:14 UTC+0000
0xff46b020 lsass.exe               680    492     19      309      0      0 2020-02-23 13:1
7:14 UTC+0000
0xff510bf0 vmacthlp.exe            836    668      1       25      0      0 2020-02-23 13:1
7:14 UTC+0000
0xff493568 svchost.exe             848    668     14      189      0      0 2020-02-23 13:1
7:14 UTC+0000
0xff491a78 svchost.exe             932    668     11      230      0      0 2020-02-23 13:1
7:14 UTC+0000
0xff416b10 svchost.exe            1024    668     44      939      0      0 2020-02-23 13:1
7:14 UTC+0000
0x80dac020 svchost.exe            1072    668      4       57      0      0 2020-02-23 13:1
7:14 UTC+0000
0xff4ca4e0 svchost.exe            1132    668      7      118      0      0 2020-02-23 13:1
7:14 UTC+0000
0xff30d020 explorer.exe           1476   1400     13      481      0      0 2020-02-23 13:1
7:15 UTC+0000
0xff51d468 spoolsv.exe            1568    668     10      120      0      0 2020-02-23 13:1
7:15 UTC+0000
0xff5793d8 VGAuthService.e        1932    668      2       60      0      0 2020-02-23 13:1
7:33 UTC+0000
0xff576da0 vmtoolsd.exe           2008    668      7      265      0      0 2020-02-23 13:1
7:40 UTC+0000
0xff4afda0 wmiprvse.exe            540    848     13      242      0      0 2020-02-23 13:1
7:41 UTC+0000
0xff486da0 vmtoolsd.exe            588   1476      6      229      0      0 2020-02-23 13:1
7:41 UTC+0000
0xff47dda0 ctfmon.exe              596   1476      1       71      0      0 2020-02-23 13:1
7:41 UTC+0000
0xff5b57b8 cmd.exe                1396   1476      1       61      0      0 2020-02-23 13:2
4:09 UTC+0000
0xff4583c0 conime.exe              544   1396      1       38      0      0 2020-02-23 13:2
4:09 UTC+0000
root@kali:~/桌面#
```


查看iehistory

```
root@kali:~/桌面# volatility -f data.vmem --profile=WinXPSP2x86 iehistory
Volatility Foundation Volatility Framework 2.6
root@kali:~/桌面#
```

没有信息的，查看cmd

> volatility -f data.vmem --profile=WinXPSP2x86 cmdscan

```
root@kali:~/桌面# volatility -f data.vmem --profile=WinXPSP2x86 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: csrss.exe Pid: 464
CommandHistory: 0x556bb8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x504
Cmd #0 @ 0x3609a0: passwd:weak_auth_top100
Cmd #1 @ 0x5576d0: start wireshark
Cmd #13 @ 0x9f009f: ??
Cmd #41 @ 0x9f003f: ?\?????????
root@kali:~/桌面#
```


发现passwd

> weak_auth_top100

使用editbox查看输入框内容

> volatility -f data.vmem --profile=WinXPSP2x86 editbox

```
root@kali:~/桌面# volatility -f data.vmem --profile=WinXPSP2x86 editbox
Volatility Foundation Volatility Framework 2.6
******************************
Wnd Context       : 0\WinSta0\Default
Process ID        : 1476
ImageFileName     : explorer.exe
IsWow64           : No
atom_class        : 6.0.2600.5512!Edit
value-of WndExtra : 0x133618
nChars            : 39
selStart          : 0
selEnd            : 39
isPwdControl      : False
undoPos           : 0
undoLen           : 0
address-of undoBuf: 0x0
undoBuf           :
------------------------
C:\Documents and Settings\Administrator
root@kali:~/桌面#
```


访问的地址是C:\Documents and Settings\Administrator

猜测到需要提取的文件内容地址

filescan插件搜索文件，grep过滤包含Administrator的地址

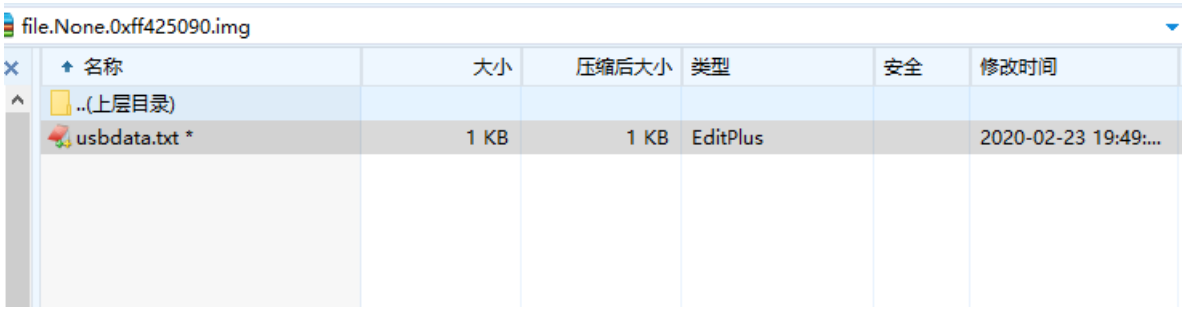
> volatility -f data.vmem --profile=WinXPSP2x86 filescan | grep "Administrator"

```
0x0000000000ae1f90      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\NetHood
0x0000000001062380      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单
0x000000000106d7b8      2      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单\desktop.ini
0x000000000107a2e8      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单
0x000000000107a7b0      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单\程序\附件\娱乐\
desktop.ini
0x000000000107fb48      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\Application Data\Microsoft\I
nternet Explorer\Quick Launch
0x000000000107fc90      2      1 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\History\Histo
ry.IE5\index.dat
0x0000000001081a20      4      1 RW---- \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
0x00000000010e7ae0      1      1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator
0x00000000010eb270      2      1 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Cookies\index.dat
0x00000000010f2408      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面
0x00000000011109f8      1      0 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\History\Histo
ry.IE5\MSHist012020022320200224\index.dat
0x00000000011114d80      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application D
ata\Microsoft\CD Burning
0x00000000011481c0      2      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\Favorites\Desktop.ini
0x000000000114a0e0      1      1 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Temporary Int
ernet Files\Content.IE5\index.dat
0x000000000114b638      1      1 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Cookies\index.dat
0x000000000114b710      1      1 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\History\Histo
ry.IE5\index.dat
0x0000000001155f90      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\flag.img
0x0000000001161c30      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\Desktop
0x0000000001167d60      2      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\My Documents\desktop.ini
0x000000000516dca8      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单\程序\启动\deskt
op.ini
0x0000000005172568      1      1 RW---- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application D
ata\Microsoft\Windows\UsrClass.dat.LOG
0x0000000005172a90      4      1 RW---- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application D
ata\Microsoft\Windows\UsrClass.dat
0x0000000005c5a028      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator
0x0000000005c5ed18      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\Recent
0x0000000005c60f90      2      1 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Temporary Int
ernet Files\Content.IE5\index.dat
0x0000000005e05828      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单\程序\附件\辅助
工具\desktop.ini
0x0000000005e53158      1      1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator
0x0000000006dbfab0      1      1 RW---- \Device\HarddiskVolume1\Documents and Settings\Administrator\ntuser.dat.LOG
```


发现关键文件flag.img,提取出来

```
volatility -f data.vmem --profile=WinXPSP2x86 dumpfiles -Q 0x0000000001155f90 --dump-dir=./
```

得到文件file.None.0xff425090.dat，修改后缀为img



使用之前得到的passwd解密

得到usb流量

使用脚本进行提取

```
mappings={0x04:"A",0x05:"B",0x06:"C",0x07:"D",0x08:"E",0x09:"F",0x0A:"G",0x0B:"H",0x0C:"I",0x0D:"J",0x0E:"K

nums=[]

keys=open('usbdata.txt')

forlineinkeys:

ifline[0]!='0'orline[1]!='0'orline[3]!='0'orline[4]!='0'orline[9]!='0'orline[10]!='0'orline[12]!='0'orline[

continue

nums.append(int(line[6:8],16))

keys.close()

output=""

forninnums:

ifn==0:

continue

ifninmappings:

output+=mappings[n]

else:

output+='[unknown]'

print'output:\n'+output
```

得到flag