

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43727482/article/details/104786110

版权



[CTF 专栏收录该内容](#)

6 篇文章 1 订阅

订阅专栏

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, compressed 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 modified: 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, compressed 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 modified: 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 : 0xb18000L
          : 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#

```

https://blog.csdn.net/weixin_43727482

```
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	VGAAuthService.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#

https://blog.csdn.net/weixin_43727482

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 @ 0x36092a0: passwd:weak_auth_top100
Cmd #1 @ 0x557600: start wireshark
Cmd #13 @ 0x9f009f: ??
Cmd #41 @ 0x9f003f: ?\????????
root@kali:~/桌面#
```

https://blog.csdn.net/weixin_43727482

发现passwd

```
weak_auth_top100
```

使用editbox查看输入框内容

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

```
Volatility Foundation Volatility Framework 2.6
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#
```

https://blog.csdn.net/weixin_43727482

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

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

```
volatility -f data.vmem --profile=WinXPSP2x86 filesan | grep "Administrator"
```



```

0x000000000ae1f90 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
0x0000000001114d80 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\PrintHood
0x0000000001167d60 2 0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\My Documents\desktop.ini
0x000000000156dca8 1 0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单\程序\启动\deskt
op.ini
0x000000000172568 1 1 RW--- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application D
ata\Microsoft\Windows\UsrClass.dat.LOG
0x000000000172a90 4 1 RW--- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application D
ata\Microsoft\Windows\UsrClass.dat
0x00000000015c5a028 3 1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator
0x00000000015c5ed18 3 1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\Recent
0x00000000015c60f90 2 1 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Temporary Int
ernet Files\Content.IE5\index.dat
0x00000000015e05828 1 0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单\程序\附件\辅助
工具\desktop.ini
0x00000000015e53158 1 1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\ntuser.dat.LOG
0x00000000015e6bfab0 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

file.None.0xff425090.img					
名称	大小	压缩后大小	类型	安全	修改时间
..(上层目录)					
usbdata.txt *	1 KB	1 KB	EditPlus		2020-02-23 19:49:...

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",0x0F:"L",0x10:"M",0x11:"N",0x12:"O",0x13:"P",0x14:"Q",0x15:"R",0x16:"S",0x17:"T",0x18:"U",0x19:"V",0x1A:"W",0x1B:"X",0x1C:"Y",0x1D:"Z",0x1E:"[",0x1F:"\\",0x20:"]",0x21:"^",0x22:"_",0x23:"`",0x24:"{",0x25:"|",0x26:"}",0x27:"~",0x28:" ",0x29:"\t",0x2A:"\n",0x2B:"\r",0x2C:"\f",0x2D:"\b",0x2E:"\a",0x2F:"\e",0x30:"\c",0x31:"\d",0x32:"\e",0x33:"\f",0x34:"\g",0x35:"\h",0x36:"\i",0x37:"\j",0x38:"\k",0x39:"\l",0x3A:"\m",0x3B:"\n",0x3C:"\o",0x3D:"\p",0x3E:"\q",0x3F:"\r",0x40:"\s",0x41:"\t",0x42:"\u",0x43:"\v",0x44:"\w",0x45:"\x",0x46:"\y",0x47:"\z",0x48:"\A",0x49:"\B",0x4A:"\C",0x4B:"\D",0x4C:"\E",0x4D:"\F",0x4E:"\G",0x4F:"\H",0x50:"\I",0x51:"\J",0x52:"\K",0x53:"\L",0x54:"\M",0x55:"\N",0x56:"\O",0x57:"\P",0x58:"\Q",0x59:"\R",0x5A:"\S",0x5B:"\T",0x5C:"\U",0x5D:"\V",0x5E:"\W",0x5F:"\X",0x60:"\Y",0x61:"\Z",0x62:"\[",0x63:"\\",0x64:"\]",0x65:"\^",0x66:"\_",0x67:"`",0x68:"{",0x69:"|",0x6A:"}",0x6B:"~",0x6C:" ",0x6D:"\t",0x6E:"\n",0x6F:"\r",0x70:"\f",0x71:"\b",0x72:"\a",0x73:"\e",0x74:"\c",0x75:"\d",0x76:"\e",0x77:"\f",0x78:"\g",0x79:"\h",0x7A:"\i",0x7B:"\j",0x7C:"\k",0x7D:"\l",0x7E:"\m",0x7F:"\n",0x80:"\o",0x81:"\p",0x82:"\q",0x83:"\r",0x84:"\s",0x85:"\t",0x86:"\u",0x87:"\v",0x88:"\w",0x89:"\x",0x8A:"\y",0x8B:"\z",0x8C:"\A",0x8D:"\B",0x8E:"\C",0x8F:"\D",0x90:"\E",0x91:"\F",0x92:"\G",0x93:"\H",0x94:"\I",0x95:"\J",0x96:"\K",0x97:"\L",0x98:"\M",0x99:"\N",0x9A:"\O",0x9B:"\P",0x9C:"\Q",0x9D:"\R",0x9E:"\S",0x9F:"\T",0xA0:"\U",0xA1:"\V",0xA2:"\W",0xA3:"\X",0xA4:"\Y",0xA5:"\Z",0xA6:"\[",0xA7:"\\",0xA8:"\]",0xA9:"\^",0xAA:"\_",0xAB:"`",0xAC:"{",0xAD:"|",0xAE:"}",0xAF:"~",0xB0:" ",0xB1:"\t",0xB2:"\n",0xB3:"\r",0xB4:"\f",0xB5:"\b",0xB6:"\a",0xB7:"\e",0xB8:"\c",0xB9:"\d",0xBA:"\e",0xBB:"\f",0xBC:"\g",0xBD:"\h",0xBE:"\i",0xBF:"\j",0xC0:"\k",0xC1:"\l",0xC2:"\m",0xC3:"\n",0xC4:"\o",0xC5:"\p",0xC6:"\q",0xC7:"\r",0xC8:"\s",0xC9:"\t",0xCA:"\u",0xCB:"\v",0xCC:"\w",0xCD:"\x",0xCE:"\y",0xCF:"\z",0xD0:"\A",0xD1:"\B",0xD2:"\C",0xD3:"\D",0xD4:"\E",0xD5:"\F",0xD6:"\G",0xD7:"\H",0xD8:"\I",0xD9:"\J",0xDA:"\K",0xDB:"\L",0xDC:"\M",0xDD:"\N",0xDE:"\O",0xDF:"\P",0xE0:"\Q",0xE1:"\R",0xE2:"\S",0xE3:"\T",0xE4:"\U",0xE5:"\V",0xE6:"\W",0xE7:"\X",0xE8:"\Y",0xE9:"\Z",0xEA:"\[",0xEB:"\\",0xEC:"\]",0xED:"\^",0xEE:"\_",0xEF:"`",0xF0:"{",0xF1:"|",0xF2:"}",0xF3:"~",0xF4:" ",0xF5:"\t",0xF6:"\n",0xF7:"\r",0xF8:"\f",0xF9:"\b",0xFA:"\a",0xFB:"\e",0xFC:"\c",0xFD:"\d",0xFE:"\e",0xFF:"\f"},

nums=[]

keys=open('usbdata.txt')

for line in keys:

    if line[0]!='\0' or line[1]!='\0' or line[3]!='\0' or line[4]!='\0' or line[9]!='\0' or line[10]!='\0' or line[12]!='\0' or line[13]!='\0' or line[14]!='\0' or line[15]!='\0':

        continue

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

keys.close()

output=""

for n in nums:

    if n==0:

        continue

    if n in mappings:

        output+=mappings[n]

    else:

        output+='[unknown]'

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