第二届"祥云杯"网络安全大赛暨吉林省第四届大学生网络安全 大赛 WriteUp 2021年祥云杯misc

原创

<u>是Mumuzi</u> ① 于 2021-08-23 12:01:48 发布 ② 3039 🏠 收藏 6

分类专栏: <u>ctf</u>

版权声明:本文为博主原创文章,遵循<u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。 本文链接:<u>https://blog.csdn.net/qq_42880719/article/details/119859244</u>



ctf 专栏收录该内容

75 篇文章 28 订阅 订阅专栏 团队汇总WP:n03tack 6web+4misc+4crypto+2re+3pwn

层层取证

层层套娃取证(确信) 给了一个内存和一个虚拟磁盘的取证,先看磁盘,取证大师打开提示存在bitlocker加密 用Passware Kit Forensic 2021 v1 (64-bit)能直接梭出来bitlocker的秘钥 方法是把001解压出来,然后把2.ntfs放进去,再选择有内存镜像,导入这道题的内存镜像,然后等待......

$\bigstar \Leftarrow \Rightarrow$					Tools Hel	p 😳	- 0	×
Recover File P	assword	Files	Passwords Found	Resources	Performance	Attacks	Log	
2.ntfs Folder File Type Complexity MD5: Memory image file: MD5: Password: BitLocker Volume Master Key	E:) BaiduNetdiskDownload Bitlocker Volume — Open Bitlocker Volume — Open SASSS704A9060694FC33 E:) BaiduNetdiskDownload 2058F94CE6F699BSDC14 File-Open No Det IncnZJNDGk6qeyfubO.	d) Forensic_9b2 Password, Nume E468595E5588 d) Forensic_9b2 I851E02CDF33E t found tails	3172e1dba502daa656b8d erical Password, Hardware 3172e1dba502daa656b8d	4234897f) disk_im, acceleration possib 4234897f) memdu	age) Forensic_ima; ile, Instant Memory mp) memdump.m	je attack possib em	le	
(Numerical Password)	y 549714-116633-00644	46-278597-176 AF4E-48E30C09	000-708532-618101-1 8739	31406				
Unprotected	i file: E:) For MD	BaiduNetdiskI ensic_image-de 5: 63C84845E8F	Download) Forensic_9b2 crypted-partition-0.dd 6407D252EA09881D20C8	3172e1dba502daa	1656b8d4234897f) disk_image	>	
PASSWORDS FOUND TIM 1 3 m	E ELAPSED inutes, 56 seconds						+ 0 K/s	57%
🖶 Print 📄 Save Job 🗸				RESUME ATTACKS	SAVE R	EPORT	WERNEN-	110

当然之后也发现内存中也可以找到,但是已经不重要 得到549714-116633-006446-278597-176000-708532-618101-131406

解开发现E盘存在一个流量包

		Э	SIME IMIT
BaiduNetdiskDownload\Forensic_9b23172e1dba502daa656b8d		10	SRECYCLE.BIN
B□□□ 分区1_本地磁盘[C]		11	Secure
⊕□□□ 分区2_本地磁盘[D]		12	Secure+\$SDH
白□□□□ 分区3_本地磁盘[E]		13	Secure-SSDS
⊕ ¤ □ 🕼 \$Extend	Π	14	Secure+\$SII
⊕ □□ 💋 \$RECYCLE.BIN		15	1 \$UpCase
-P (Root directory)		16	SVolume
	П	17	G (Boot directo
-DI System Volume Information		18	(Root directo
⊕□□◎ 签名恢复结果	H	10	
	H	20	「こpcaping pcaping の 手仕立け
	-	20	
		21	MFT Allocati
		22	System Vol
		23	
		24	◎ 签名恢复结果

在udp里面找到一个rar,里面包含了一个flag.docx



然后导出,说压缩包密码是开机密码

									THING PORCE	CONTRACTOR OF
🛃 2.rar - 360)	王绾				文件	操作	IR	帮助	Û	- 🗆 ×
			o	2	C					
添加	解压到	一键解压	删除	压缩包语言	工具					
* 🔳 😑	📕 2.rar - 解包:	大小为 14.0 KB								Q
名称				压缩前	压缩后	与计算	机开机密	码相同		
📕 (上级目录)		📑 sii.2	「密码					×		
			lag.docx 显示密码				*			
			管理密码	确定		取消				
<					>					
大小: 11.5 KB 共	1 个文件 压缩率	81.8%					ogics			

然后去看俺的另一篇博客

Volatility Foundat: Virtual	ion Volatility Fram Physical	Name
0 + ffffan03596410 pfffffan03596410 pfffffan03596510 0 + ffffan035915 0 + ffffan03516 0 + ffffan03516 0 + ffffan03516 0 + ffffan03516 0 + ffffan0355610 0 + ffffan0355610 0 + ffffan0355610 0 + ffffan0355600 0 + fffffan0355600 0 + fffffan0355600 0 + fffffan0355600 0 + ffffan0355600 0 + ffffan03556000	0-800080001218c310 0-800080001218c310 0-800800002138c310 0-800800012121030 0-800800012210010 0-800800012210010 0-800800011121010 0-800800011121010 0-800800011121010 0-800800011121010 0-8008000055771010	\SystemRoot\System32\Config\DEFAULT [no name] VEGGISTRY\MACHINE\SYSTEM VEGGISTRY\MACHINE\HARDWARE \Device\HardWarDiskVolume\HARDWARE \Device\HardWarDiskVolume\HARDWARE \SystemRoot\System32\Config\SACURITY \SystemRoot\System32\Config\SAM Y?\C:\Windows\ServiceProfiles\LocalService\MTUSER.DAT \??\C:\Windows\ServiceProfiles\LocalService\MTUSER.DAT \??\C:\USerS\Administrator\ntuser.dat \??\C:\System Volume Information\Syscache.HWIPS://Di0g.csdn.ned/qc_42880719
2.hashdump: volatility -f raw.rav	wprofile=Win7S	P1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a001390010
2.hashdump: volatility -f raw.rav	wprofile=Win7S	P1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a001390010
2.hashdump: volatility -f raw.ray volatility Foundat Administrator:500: Guest:501:aad3b435	Wprofile=Win7S \$ volatility -f raw. ion Volatility Frame aad3b435b51404eeaad3 b51404eeaad3b435b514	P1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a001390010 rawprofile-Min7591×64 hashdung -y 0+fffff8a000024010 -s 0×fffff8a001390010 work 2.6 84x01351444ee <u>13466ff0016se031073c590700c089c01::</u>

这里提取的是92EFA7F9F2740956D51157F46521F941

录:[^{2]} Spoil_mu],付赛查询剩余条数[73],[充值][退出]					
	卷:	t: 92EFA7F9F	2740956D51157F46	521F941	
	类	2: NTLM			✔ [帮助]
			查询	加照	
	查询结果:				
	xiaoming_handsome				

密码xiaoming_handsome, cmd5解一下就行了(不会有人没开会员吧) 解压之后发现docx还有密码

- 2 - 1	10.00										
文件 主页	共享	売君									~
オ 前 第25月 第1 はまびの	1000 × 10000 × 10000 × 10000 × 10000 × 1000 × 1000 × 1000 × 1000 × 1000 × 100	1943 第1985년 1859日建方式	લ્યોકા સલ્લેકા જેવા સલ્લેકા	e anis ≣esa a	● 10 年日 ● 10 日日 ● 10 日日 ● 10 日日 ● 10 日 ● 10 日	14月日 - 145月 - 編約 編約	副打开・ ☑ 编辑 ▶ 历史记录 打开	 金田道塔 金田取用 金田取用 反向道祥 支邦 			
e +	= > #3	458 > Winds	ows 7 (2) > 用户	> XiaoMing	> #8			~	0	.0 (8%*#B*	
1 文档	**	66	~		你改日期		英型	大小			
副用	*	E flag.txt	t.		2020/8/13	21:19	文本文档	1	KB		
 副初始 2 disk_ima Menin8i 第(約7卷) OneDrive WPS网盘 ● Qui ● Qui ● 和約二次 二葉文化 	yr soldrat Hillion:					🧃 fleg.tx 文:时(F) 6 hint: 你说	1、20年年 18月(5) 松(50) 年电線都不能	善■(*) 帮他(8店真打开,i	H) 不想要	flag ?	
·····································	wt/len≚ 1 个项目	42 宇竹				https:					

实在找不到了的时候, 挂载一下, 发现hint

然后去仿真。。。。。。嗯仿真不出来

照着https://www.freesion.com/article/51701409948/#DDE01_8我也不行

然后就去导出内存,还是看□的博客



从原始数	星星人图象	1 🖬 🕫	20:34 🚭
0	00000		
8			
	10-1-0000-11 seeings1-01-0	Related Benefit 1 In the Advances was a second benefit to a second	
Â	222		
a			
100	10.0		
	图像类型(I):	KB Alpha	:
10	位形(约:		435182 1
	克度(w):	Stor	1
<u> </u>	高度(=0);		7 1
	0.6		
	色质类型(约):	R, G, 10(目前)	:
	(1845);		1
	色板文件(6);	DD	
Ŧ	WEIB1H0	https://blog.csdn.net/cg4zee	149

可以自己去操作放大看,偏移294435180,宽510 结合用户名,得到xiaoming1314,解压成功 得到flag

```
flag{9ca871b668f2-b668-097c-cbm8-9op404c891e2}
```

当然对于赛后复盘,其实Passware Kit能直接把xiaoming的开机密码梭出来,如果看内存的图像知道了是在便笺上但是看不清,可以直接取证的时候将C:\Users\帐户文件夹\AppData\Roaming\Microsoft\StickyNotes\StickyNotes.snt打开,然后再找到里面的 密码。顺带还发现,其实不用解bitlocker也能找到含有rar的流量包,在XiaoMing\AppData\Local\Temp下。总之这种内存取证解 法挺多的,自己喜欢用啥方法就用啥方法。

鸣雏恋

改zip解压,在_rels下发现key和love,key是妥妥的零宽

佩恩:凭你这点力量,为什么要战斗?		佩恩:凭你这点力量,为什么要战斗?
雅田: 说到取到, 另住置制, 这就在我的念道。		非回:说到收到,另往直刑,这就走我可愿道.
	加密 >	
龍 藏文字: 清除 (长度: 26)	# \$62182	
Because] Like naruto best	a literation	

解压之后是两张图,其实这里可以不用解压直接读CRC,可惜写的脚本有点问题,为了不浪费时间还是解压了(其实是解压途中 写的zip读CRC脚本写的有问题就还是用读图片了) 然后写个脚本,2进制的ASCII

```
from PIL import Image
from tqdm import tqdm
path = 'C:\\Users\\mumuzi\\AppData\\Local\\Temp\\噶維态_2dad763070b79f50c4635a906359909a\\噶维态\\_rels\\love\\ou
t\\'
flag = ''
for i in tqdm(range(129488)):
    img = Image.open(path:str(i)+'.png')
    s = img.getpixel((1010))
    if(str(s) == '1'):
        flag += '0'
    elif(str(s) == '3'):
        flag += '1'
    else:
        print('wrong!')
        exit()
s = ''
for i in flag:
    s =-i
    if len(s)==8:
        rflag += chr(int(s,2))
        s =''
print(rflag)
```

得到base64的png图,图片最下面就是flag



flag{57dd74fb21bb1aee50f19421bf836f23}

考古

最后的xor我是真的服气这一来怎么直接想得到太浪费时间了 先imageinfo,发现是XP,然后pslist列出表,发现cmd正在运行,cmdscan看一下cmd



然后Filescan |grep "Oneclickcleanup.exe",然后dumpfiles -Q 0x00000000017bcbc0 -D / 一共是得到一个dat和一个iso,dat直接拖IDA32 发现是两个异或,第一个异或是存放地址,第二个异或是异或的数据

```
__main();
for ( i = 0; i <= 44; ++i )
   _data_start_[i] ^= key[i % 10];
for ( j = 0; j < (int)size; ++j )
   data[j] ^= key[j % 10];
for ( k = 0; k <= 9; ++k )
   puts("Hacked by 1cePack!!!!!!");
v4 = fopen(_data_start_, "wb+");
fwrite(data, size, 1u, v4);
return 0; dps://blog.csdn.ne/qg_42880719
```

key是this_a_key,data就是数据,把data导出,写个脚本

flag = ''
#flags = [0x37,0x52,0x35,0x37,0x30,0x02,0x2A,0x06,0x00,0x17,0x00,0x1B,0x49,0x12,0x31,0x05,0x7F,0x38,0x00,0x0D,0x
00,0x01,0x07,0x14,0x2C,0x3D,0x1E,0x07,0x09,0x59,0x21,0x1B,0x0C,0x01,0x2C,0x3D,0x0B,0x0E,0x08,0x09,0x18,0x09,0x1D
,0x16,0x2C]
flags = [0xA4,0xA7,0x78,0x93,0xFE,0xD0,0x45,.....中间略,0x79,0x74,0x68,0x69,0x73,0x5F,0x61]
for i in range(len(flags)):
 flag += str(hex(flags[i] ^ ord(s[i%10])))[2:].zfill(2)
print(flag)
f = open('ffff.dot','wb')
f.write(flag.encode())

得到的ffff.dot用notepad++打开,将16进制转ascii 为什么要保存为.dot,因为我在复现我知道是dot我乐意 然后WPS打开发现提示版本过低,用office打开



然后就瞎试,比如看16进制,从200h-1800h和1800h到最后是一样的,两者相比较什么的,都试过了,没出继续看内存文件。 最后。。。想着可打印ascii的词频和异或,结果异或出了



因为长度只有31位,爆破一下0-f,竟然不对,然后想着一共出现了两次,再去试试,还是不对。麻了 因为是dot文档,又想着zip解压直接看源文件,然后再来异或

👚 🗐 😑 📕 ffff.zip - 解包	;大小为 3.0 KB
名称 (上级目录)	
ObjectPool [] [1]CompObj [] [5]SummaryInformation	当前文件: WordDocument
WordDocument	解压速度: 0 KB/s 已用时间: 00:00



???我可去你的吧居然还有一段 最终得到flag

flag{8bedfdbb-ba42-43d1-858c-c2a5-5012d309}

麻了,太打脑壳了,别问,问就是4:07交的

Spoil_mu 2021/8/22 4:07:16 考古13解了

ChieftainsSecret

首先给了一个文档和一张图片,文档就是题目描述,图片的话是一个古时候的电话 搜了一下是怎么用的

https://haokan.baidu.com/v?pd=wisenatural&vid=15222023905414500076

Jpg图片后面还有rar,foremost提取出来,发现是一堆TLE5501生成的数据,搜了一下他是一个角度的传感器,给了 sinP,cosP,sinN,cosN

本着不会做就乱试+搜公式的原则,发现想要计算出角度,就得找到tan,于是萌生了sinP/cosP,sinN/cosN,(sinP-sinN)/(cosP-cosN)的想法,想知道角度,就再加上一个ATAN函数,除出来是弧度,就再乘以一个57.3°

顺便看了油管的视频,研究了一下四个值的变换

https://www.youtube.com/watch?v=y68ldqZs4PM

最后在看第三个想法的时候恍然大悟,搞出来也正好是11个峰



上图的意思就是ATAN((sinP-sinN)/(cosP-cosN))*57.3,然后因为ATAN的范围是-90°~90°,所以才会出现到90°的时候马上反转成 负的,然后负的又接着变为正的,总之,第一个90°之后,后面的值要加180.第2个90°之后,后面加270,妈的简直找惨了。 得到的数字大概为210 210 280 230 160 260 190 90 140 160 210

然后去下载一个量角器(PicPickPortable),发现2正好是90°,所以我直接就排除1了,然后一个个去量,下图举个例



所以flag为flag{77085962457}

Rev_Dizzy

一串简单的数学计算,首先是IDA F5,挺慢的,多等等,如果提示要逆的太大了,就自己百度一下,改一下

H & & & & & A	to the O	2-2-2-1X -00	No debugger	1 1 2 3 P P						
Library function Regular function	Instruction	Duta memplored Int	ernal symbol E Lusin	a function	-					-
Unicipiente D e		Vier-a C Costrings C	EPseudocode-C U	ng Preudocoder b	LE Presidocode-A LI	No. Bes View-1 []	A structures U	IL BARS ()	The Deports L1	E Espirits U
ction name	. 5055	v13 - 24;								
wb_401000	5858	v14 = -14;								
ub_401010	5853	v15 = -110;								
ub_401020	 Sesi 	v16 = 0x80;								
ub_401050	 5051 5051 	v17 = -30;								
ub_401080	 5460 5460 	v10 = 56;								
ub_401090	5052	v20 = -78;								
ub_4010D0	5053	v21 = 103;								
ub_4010FD	5054	<pre>v22 = 119;</pre>								
ub_401110	5063	v23 = 15;								
ub_401130	 5001 5001 	V24 = -10; v25 = 13:								
main	 Saci 	v26 = -74;								
ub_434230	5061	v27 = -191								
ub_434330	5070	v28 = 28;								
ub_434570	5871	v23 = 101;								
ub_4345A0	• 5072	v30 = -118;								
ub_434580	 587 	v32 - 831								
ub_434630	5875	v33 = -90;								
ub_434680	5878	v34 = 102;								
ub_434830	5877	for (j = 0; j < 32)	M *((unsignedin	t8 ")&v6 + j) == (un	signedints)byte_	43841C[j]; ++j)				
td:_Fac_node:Fac_node(void)	• 5071									
td: Fac tidy reg t:- Fac tidy reg t(void)	5075	1 () == 52)	-h:							
td: Facet Register(std: Facet base *)	588	else	. /.							
security_check_cookie(x)	 5002 	puts("You don;t fi	nd it");							
ub 434916	9 5083	puts(byte_436166);								
oft 434924	₩ 8 5884	return 0;								
	> 0 5083	2								
11 of 114		00033565 main:5054 (4)	14165)							
ntput.										1
SAI: call analysis failed										
SAL: call analysis failed									1	6
SA1: call analysis failed										(70.
SA1: call analysis failed										_
balled similars find										

给了运算、给了最后比较的值,逆一下就行了,将所有复制出来,只留下运算的部分,然后写个脚本

```
s = [0x27, 0x3C, 0xE3, 0xFC, 46,65,7,94,98,-49,-24,-14,-110,128,-30,54,-76,-78,103,119,15,-10,
13,-74,-19,28,101,-118,7,83,-90,102]
f = open('1.txt','n').readlines()
for i in range(len(f)):
    if(i != len(f)-1):
        f[i] = f[i][:-2]
    else:
        f[i] = f[i][:-1]
    f1 = [']'l=n(f)
for i in range(len(f)):
    f1[i] = f[len(f)-1-i]
for i in range(len(f1)):
    tmp = f1[i].replace('byte_43841C', 's')
    if('+=' in tmp):
        tmp = tmp.replace('+=','-=')
    elif('==' in tmp):
        tmp = tmp.replace('+=','+=')
    else:
        pass
    exec(tmp)
for i in range(len(s)):
    print(chr(s[i]%256),end='')
```

flag{Try_R3vers1ng_W1th_ScR!pt!}

shuffle_code的话提一下,后面就数织(补一句:我单推沃玛,沃玛8月13的视频就用了数织所以才知道这是数织的。见:沃玛的 生活/第六期)来反推二维码。然后行数据是对的,但是每行所处的顺序错了,可以根据二维码的固定位置来反推出数织,然后会 出现中间一部分无法确定的情况,用脚本爆破然后去try扫描二维码即可。

那有可能没有听懂是什么意思,这里再说明白一点。

就是首先把数织给的数,放到数织里面去解,会解出一张看起来毫无关系的图。但是你仔细看就会发现,行的数据是正确的,意 思是二维码已经在图上了,但是这29行,被打乱了。

然后就需要根据二维码的性质,把开头的几行,最后的几行给手动恢复一下,中间的十几行,只需要上下移动即可,但是并不知 道正确的图是哪样的,所以需要写脚本来爆破,然后每爆一张,就自动扫描一张,能扫出来的图就是flag。