WMCTF2021 WP misc



 <u>是Mumuzi</u>
 于 2021-08-31 00:08:12 发布
 917 % 收藏 2

 分类专栏:
 <u>笔记</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/120000111</u>

版权



笔记 专栏收录该内容

23 篇文章 6 订阅 订阅专栏 唉因为太菜本来不想写的(其实是因为都只能做一半导致太水了不好写)

复现了一下取证还是写一下吧

Checkin

ctrl+c ctrl+v enter

你画我猜

画!都可以画!



WMCTF{x1aoma0_wants_a_girlfriend}

我画你猜

猜!都可以猜!

 费 我圖你猜 	 × ● 上网号航 - 经快上网 从这里开始 ☆ 182.92.232.152:5000 	+	₹ (č. ×	S▼ 大象驾驶证走红	Q 🚗	ت ر ۲۰ × ۱	- E	∍ × . =
			, ,			0	Ŭ	Ĺ
我画你猜					相关游戏		à	- 1
00:0-	-51 WMCTF(L1near_has_double_girlfriends) WMC	WMCTF{L1near_has_double_girlfriends} TF{L1near_has_double_girlfriends}	WMCTF{L1near_has_double_girlfriends}		tiette	你回我猜想	18K)	1
	Z	3		56/58/80 🔎	位画我猜	我画你猜	<u>— 笔变</u> 道	I.
							/5 65*	
						CSI	DN @是M	umuz <mark>i</mark> .

WMCTF{L1near_has_double_girlfriends}

LOGO

LOGO!都可以LOGO!



为了要把图给画下来,当然是重定向啦

nc 118.190.157.196 10001 > 1.txt

打开之后发现每次都是5个参数 例如[48;2;23;21;24m 并发现前面两个都不变,因此推断出RGB为后三个参数,即(23,21,24) 因此就可以写一个脚本,将其画下来。 但是画下来之后发现,图片被拉宽了。并且有明显的LSB隐写,但是就是找不到flag 于是准备将值打印出来



发现一个问题,每两行的值都是一样的,再结合nc上面输出的是正方形,由此可推断,原图是256256,而并非256512 于是每隔一个画图,最后查看LSB发现flag 一把梭脚本:

```
from PIL import Image
pic = Image.new('RGB',(256,256))
f = open('1.txt','r').readlines()
for i in range(len(f)):
   f[i] = f[i].split('[')
        f[i][j] = f[i][j].split(';')
for i in range(256):
       pic.putpixel((j-1,i),(int(f[i][j*2][2]),int(f[i][j*2][3]),int(f[i][j*2][4][:-3])))
pic.save('WM.png')
pic1 = Image.open("WM.png")
w = pic1.size[0]
flag =
for i in range(w):
   g = pic.getpixel((i,0))
   R,G,B = bin(g[0])[2:].zfill(8),bin(g[1])[2:].zfill(8),bin(g[2])[2:].zfill(8)
   li = [R,G,B]
        flag += color[7]
tmp = ''
for k in range(len(flag)):
    tmp += flag[k]
    if len(tmp) == 8:
        print(chr(int(tmp,2)),end='')
```

```
m<mark>umuziakali:~/桌面$</mark> python3 LOGO.py
WMCTF{dba5d43b6c0035d8559437ed34f2f8fb}'²Éï¶G¾Þ¶KmZâR$[bI $¶ÛbIØI;v
```

WMCTF{dba5d43b6c0035d8559437ed34f2f8fb}

Questionnaire

WMCTF{s33_u_in_2022}

Flag Thief (复现!)
WP写的真的很详细了
题!好!考点: 呜呜呜忘干净了

【卑微各群群欺】肘子炫之看守所分炫 2021/7/6 16:22:54

V3geD4g 2021/7/6 16:00:37 https://www.freebuf.com/articles/ web/279561.html 好像又是一个出题思路



@V3geD4g 确定 【卑微各群群欺】肘子炫之看守所分炫 2021/7/6 16:22:56 确实 CSDN @是Mumuzi

https://www.freebuf.com/articles/web/279561.html(可恶居然押中题) 有关此类取证可能碰到的知识点(tokeii): https://blog.csdn.net/u010418732/article/details/120009187 根据提示,可以猜测是RDP,于是去仿真查看日志管理器-安全,id 4624d的日志,但是啥都没翻到。然后中间阿巴阿巴做了一堆事情啥也没找到惹。 好! 复现就只知道是关于上面那个链接,然后就可以做完惹 路径%USERPROFILE%\AppData\Loca\Microsoft\Terminal Server Client\Cache 用FTK挂载打开

AccessData FTK Imager 4.3.0.18						
文件(<u>F</u>)	查看(<u>V</u>)	模式(<u>M</u>)	帮助(<u>H</u>)			



Dia alla	

_

Add Image			
Image			
E:\BaiduNetdiskD	ownload\evidence\evidence.E01		
Mount Type:	Physical & Logical \sim		
Drive Letter:	P: ~	随便选一个	
Mount Method:	Block Device / Writable 可与 ~		
Write Cache Fold	ler:		
E:\BaiduNetdiskD	ownload\evidence		
		Mount	
		CSDN @是Mumu	zi

毕地磁盘 (Y:) 》 用户 》 WMCTF 》 AppData 》 Local 》 Microsoft 》 Terminal Server Client 》 Cache

🔲 bcache24.bmc	2021/8/17 18:50	BMC 文件	0 KB
🚭 Cache0000.bin	2021/8/17 18:51	BIN 文件	32,471 KB
🚭 Cache0001.bin	2021/8/17 17:37	BIN 文件	53,994 KB
😱 Cache0002.bin	2021/8/17 17:39	BIN 文件	CSDN @ Z4 243 KB 但是Mumuzi

这三个bin, 弄出来。

你跟着那个链接,一个个去弄,那肯定不现实,那好,那咱就去百度



5eCuri7yPaSsW0rd@__WMCTF

好!那VeraCrypt的东西在哪。当然是用取证大师来找了

_					-			
	1	edbres00002.jrs	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Users\WMCTF\AppData\Loca	524.288
\checkmark	2	5ebe2294ecd	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Users\WMCTF\AppData\Loca	157,286,400
	3	startscreen.vid	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Program Files\WindowsApps\	2,457,600
	4	📄 edbres00001.jrs	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Users\Administrater\AppDat	524,288
	5	edbres00002.jrs	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Users\Administrater\AppDat	524,288
	6	📄 V010001A.log	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Users\WMCTF\AppData\Loca	524,288
	7	📄 V01res00001.jrs	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Users\Administrater\AppData	524,288
	8	📄 V01res00002.jrs	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Users\Administrater\AppData	524,288
	9	USSres00001.jrs	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Users\Administrater\AppData	3,145,728
	10	USSres00002.jrs	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Users\Administrater\AppData	3,145,728
	11	edbres00002.jrs	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Users\Administrater\AppData	524,288
	12	edbres00001.jrs	疑似TrueCrypt加密文件	AES/Twofish/Serp	打开保护	暂不支持	分区4_本地磁盘[D]:\Users\Administrater\AppData	524,288
							65	DN @ÆMUINUZI

这个很大,我忍一下,直接导出,然后解密。顺便把FTK关了

驱动器 <mark>(&D)</mark>	Method	分区	Image				
PhysicalDrive3	Block Device/Wri	Image	E:\BaiduNetdiskDownload\evidence\evidence.E01				
V:	Block Device/Wri	Basic data part	E:\BaiduNetdiskDownload\evidence\evidence.E01				
W:	Block Device/Wri	EFI system par	E:\BaiduNetdiskDownload\evidence\evidence.E01				
X:	Block Device/Wri	Microsoft reser	E:\BaiduNetdiskDownload\evidence\evidence.E01				
Y:	Block Device/Wri	Basic data part	E:\BaiduNetdiskDownload\evidence\evidence.E01				
<			>				
Unmount CSDN @是Mumuz							

记得unmount!

1 :	學吃板	组织	新建	打井
	← → ~ ↑ 🔷 > 此电脑 > 本地磁	结盘 (R:)		
M:	文档 * ^ 名称	^	修改日期	类型
0: P:	Nox-di	sk2.vmdk	2021/8/17 15:16	360压缩
■ Q: ■ R:\5ebe2294ecd0e0f08eab7690d2a6 149 MB AES 常規 ■ S: 	 到回收站 ★ ■ BaiduNetdiskD 			
创建加密卷(C) 加密卷属性(X) 撞線	<pre>evidence LSB-steganogra</pre>			
加密卷	📙 ubuntu - 副本			
D:\取证大师专业版(V6.1.80018)\FMP\Case\Case01-20210829- > 选择:	 OneDrive 			
✓从不保留历史记录(R) 加密卷工具(T) 选择:	🍮 WPS网盘			
	🕒 最近			
卸载(D) 自动加载设备(A) 全部卸载(S)	★ 星标		CSDN @#	륃Mumuzi

啊,是nox-disk, 搜一下,是夜神模拟器,于是可以去下载一个 (做完了表示,直接diskgenius恢复文件然后去找到通讯录就可以了) 导入一开,妈的还有密码,绝了。



点我,一定要看

diskgenius挂载(想用winhex也行的)

DiskGenius V5.1.1.696 专业版 文件 磁盘 分区 工具 查看 帮助

	Н	保存分区表(F8)		in (
促左1		备份分区表(F2)		
I7K15-		还原分区表(F3)		IRRIJI E TERU
1				-SSD(C·)
磁盘		清除保留扇区(E)	ĥ	FS
		转换分区表类型为GUID格式(P)	-	SGB
」接口	ø	转换分区表类型为MBR格式(B)	1	N439739 容重
.		动态磁盘转换为基本磁盘(D)	200	刘览文件 扇
		指定磁盘参数(G)		
E		查看S.M.A.R.T.信息(S)	E	M_DRV(0)
	*	坏道检测与修复(Y)	(1	L)
		复位坏扇区记录	0	ws-SSD(C:)
		(注) (15)		DDV(4)
			ľ	_DKV(4)
Œ				14 T U
		新建虚拟磁盘文件(N)	• 5	5型:
. E	G	打开虚拟磁盘文件(V)		
		关闭虚拟磁盘文件(C)	- [
		虚拟磁盘格式转换	:	
		重新加载当前磁盘(Ctrl_L)	-12	寻:
		安全単出磁盘①	1	
		更改设备状态	+	
		TRIM优化	護	号:
	-	入 †	に水フ	七小:
		12(3)	PFP・@元	EMumuzi

分	区表问题报告		>	<			
磁盘 VD0:nox-disk2.vmdk(63GB)存在下列分区表问题:							
	分区	错误说明	更正方法				
	主分区(2)	警告: 警告:没有活动分区 错误: 终止位置参数溢出	修正参数 重新建立				
说明: 更正时仅调整分区表参数,不执行"重建分区或重新格式化"操作。请在更正完其它错误后手动执行 这些操作。							
		更正	取消 CSDN @是Mumuz	zi			

☐ DiskGenius V5.1.1.696 专业版 文件 磁盘 公区 工具 音赛 契助							- 🗆 X
(保存更改 搜索分区 恢复文件 快速分区 新建分区	ART 開除分区 ART	Geni	US Part	All-In-O ition Manag	ne Solution For ement & Data Reco	very	
「 《 》 磁盘 3 接口・ATA 刑号-VMMare Virtual Disk 容별・52.8G8/642	665WB) 社而教・130570 祥头教・16 英道院区制	1-63	主分区 EXT4 62.50	(2) 4 58			
	公交条款 浏览文件 启区编辑	(100)2/04/228	2.10101.020				
□ ● 至 主分区(2) ▲	→ 2称	大小	立住米刑	届姓	修改时间	命理时间	,
adb		ДŢ	文件关望	10011			
anr	procstats		又任光	arwx	2021-06-29 11:01:26	2021-06-29 11:01:26	
app	sensor_service		又针头	drwx	2021-06-29 11:01:28	2021-06-29 11:01:28	
app-asec			又什类	drwx	2021-06-17 15:13:05	2021-06-29 11:01:29	
app-epiteneral			文件天	drawrawr-y	2021-08-17 15:13:06	2021-06-29 11:01:20	
	2901314	0.8	2801314 立件		2021-08-17 15:15:20	2021-00-23 11:01:20	
	bEdd25dfcb22ae522edab14f11ba7422	08	bEdd2Edfdb	1.00	2021-08-17 15:15:27	2021-08-17 14:18:10	
- bootchart	build prop	2 7/8	D500550105	1 W	2021-00-17 15:12:05	2021-08-17 15:12:05	
🗄 🔂 cache	build prop64	0.242	prop 文件 prop 64 文件	- w	2021-00-17 15:12:05	2021-08-17 15:13:05	
⊕ 🔁 dalvik-cache	battervetate bin	3.3KD	propor 文件 bin 文件	- w	2021-08-17 15:13:03	2021-08-17 15:15:05	
🗄 - 🚞 data	bacter ystats.bin	2.360	bill 文다 xml 文件	- W	2021-08-17 15:15:05	2021-06-17 15:15:05	
	device policies yml	227.8	メルシート		2021-05-05 19:57:57	2021-00-29 11:01:32	
🕀 🔁 local		2276	XIII XII+	- w	2021-08-17 14:44:17	2021-06-17 14:44:17	
lost+found	framework atlas config	110 8	videocD .da	-1 W	2021-06-20 11:01:20	2021-06-29 11:01:20	
🕀 🛄 media	astekeeper password key	0.8	coning 文件	-1 W	2021-06-29 11:01:29	2021-06-29 11:01:29	
mediadrm	gatekeeper pattern key	59.0	ey 文件	-1 W	2021-08-17 14:44:17	2021-06-17 14:16:46	
I misc	Jack-tetrim	0.0	key 文IH 文/H	-1 W	2021-06-20 11:01:29	2021-06-20 11:01:28	
ter in the second seco	last hander tut	260 8	XI+ Taut File	-r w	2021-06-29 11:01:26	2021-06-29 11:01:20	
misc_de		4 OVP	OO Messag	- W	2021-06-20 11:01:29	2021-06-20 11:01:29	
	locksettings.db	22 OKB	QQ Hessag		2021-00-23 11:01:28	2021-06-29 11:01:28	
	ledwettings.db-snin	144 OKB	db-wal 文件	- W	2021-08-17 13:13:04	2021-06-29 11:01:28	
		177. SKD	ub-wai 옷(+	- W	2021-00-17 14:44:17	2021-00-29 11:01:20	
	og-nies.xmi	/18	xmi 文件 立件	-rw	2021-08-17 15:13:06	2021-08-17 15:13:06	
ss		20.048	XI+	srwx	2021-08-17 15:13:04	2021-06-17 15:15:04	
🖃 🦳 system	actification log db ieuroal	20.0KB	du inurcal	- w- w	2021-00-17 14:17:44	2021-06-29 11:01:31	
.update_2	actification_policy.vml	12.3KD	ub-journal	-1 W	2021-00-17 14:17:44	2021-06-29 11:01:31	
🔂 dropbox	Deckages list	1.7KB	加以什	- W	2021-00-17 15:15:04	2021-08-17 15:13:04	
🗀 heapdump		0.0KD	list 文件	-rw-r	2021-06-17 15:13:03	2021-08-17 15:15:05	
🔁 ifw	pockages.xill	2/3.0KB	が出入け	- w- w-	2021-00-17 10:13:03	2021-00-17 15:15:03	
inputmethod	bertait conice ym	10 8	×1+	- w	2021-00-17 14:37:43	2021-00-17 14:57:45	
install_sessions V	iderrora byt	1148	Taxt File	T W	2021-06-20 11:01:26	2021-06-20 11:01:26	G m
*	i uden or s. tXt	048	rextrile	- WXIWXI	2021-06-29 11:01:26	2021-00-29 11:01:26	
計法							CSDN @最好umuzi

3.根据device_policies.xml文件中,我们可以得到该解锁图案的长度为9.

device_policies 1949.xml - 记事本	-]	×	
文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H)					
<pre> <?xml version='1.0' encoding='utf-8' standalone='yes' ?</pre></pre>	?>			^	
<policies setup-complete="true"></policies>					
<active-password length="9" quality="65536" th="" uppercase<=""><th>se="0" lowercase="0"</th><th>letter</th><th>s="0</th><th></th><th></th></active-password>	se="0" lowercase="0"	letter	s="0		
	🔆 电子取证及可信应	周协论	训中心	ι,	
	C	SDN (0是Ⅳ	lum	ızi
I device policies.xml - 记争不			_		×
xml version='1.0' encoding='utf-8' standalone='yes' ? <policies setup-complete="true"> <active-password (="" length="9" quality="65536" uppercase="0"> </active-password></policies>	owercase="0" letters="()" num	neric=	"9"	
		CSD	N @是	Mun	nuzi

芽,咱也是9
然后跑他的脚本,具体看那篇博客,记得最后加一个print password
f1 = open('password123.txt', 'r')
lines = f1.readlines()

CSDN @是Mumuzi

然后。。。跑了我一个多小时 不过是有其他方法的捏,但是复现玩玩捏,就懒得去搞其他方法捏,比如hashcat捏。



183492765

~





∩OX 夜神模拟器1 7.0.1.5		☑ 2 1		~
			5:34	к 7 К 3
☆ 🖌 ።	J	11011 912 0 手机		
	•	BS7nX1uw+KmS4LSXIK3LIntByEturqY4qjGI/ yj3Di8aps4K+DR9hCzndjUD7w54 住宅	•	
	简介	格		
	昵称 Flag			
弗莱格 Fu Laige	姓名 Fu La	拼音 ige		I D J
			CSDN @是Mum	uzi ⁱ .



BS7nX1uw + KmS4LSXIK3LIntByEturqY4qjGI/yj3Di8aps4K + DR9hCzndjUD7w54

AES加密模式: ECB v 填充: zeropadding v 数据块: 128位 v 密码: 18349276	5 偏移量: iv偏移量,
待加密、解密的文本: 🖻 🗙	
BS7nX1uw+KmS4LSX1K3LIntByEturqY4qjGI/yj3Di8aps4K+DR9hCzndjUD7w54	
	AES加密 AES解密
AES加密、解密转换结果(base64了): 🖻 🗙 😝	
wmctf{dc4fc81e0aedc4692a7e312ce503e3ef}	CSDN @是Mumuzi
	CDD14 GAEIMUITULI

wmctf{dc4fc81e0aedc4692a7e312ce503e3ef}