# 2022 SMUCTF 永远都对-rui WriteUp



<u>瑞瑞z</u> ● 于 2022-04-20 17:01:57 发布 ● 1006 全 收藏 分类专栏: CTF 文章标签: web安全 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/m0\_45373799/article/details/124256901 版权



CTF 专栏收录该内容

3 篇文章 0 订阅 订阅专栏

## Misc

签到

直接输入flag。

#### emoji

把emoji和key复制到 emoji-aes 解密得到flag

(key 就是 SMUCTF)



## **SMUGIFQR**

题目附件给了一个gif的二维码,分别扫出每一个二维码组合即可得到flag。

# 冰墩墩的汉信码

#### 把冰墩墩图片放到StegSolve里得到汉信码



#### 扫码即可得到flag

	中國电信圖 <sup>18</sup> ,111 奈, 6 <sup>0</sup> 答义 96% <b>—</b> 11 00:22
	< ○ 扫描结果
	2022 <b>\$\$</b> 4 <b>\$</b> \$13 <b>\$</b> \$009
Ē	
L	原始信息
	Dear SMUCTFers, congratulations on getting the flag : flag[Have.YOu.ever.Heard.Of.HanXinMa]
ř.	
Ł	条码知识
	汉信码是由中国物品编码中心研制开发、是我国第一个
	制定了国家标准的自主知识产权的二维码、具有知识产
	权免费、汉字编码能力强、抗污损、抗畸变、信息容量
	大等特点,2007年8月23日,国家标准化管理委员会发布
	了GB/T 21049《汉信码》国家标准、和其他二锥码相比、
	汉信码更适合汉字信息的表示,真支持GB 18030中规定的
	160万个汉字信息字符,具有高度的汉字表达能力和汉字
	正确效干,共可很强的介绍能力、把访快和叫支能力。 支持加密技术。

listentomusic

#### 拨号音用DTMF2NUM解出后得到压缩包密码

C:\Windows\Syste	m32\cmd.exe					
C:\Users\ZJR\Down	hloads\DTMF2NUM>dtmf2num.exe pass.wav	Z				
DTMF2NUM 0.1c by Luigi Auriemma e-mail: aluigi@autistici.org web: aluigi.org						
<pre>- open pass.wav wave size format tag channels: samples/sec: avg/bytes/sec: block align: bits: samples: bias adjust: volume peaks:</pre>	56000 1 8000 16000 2 16 28000 0 -32768 32767					
- MF numbers:	7745					
└─ DTMF numbers:	1933056020					
C:\Users\ZJR\Downloads\DTMF2NUM>CSDN @瑞瑞z						

打开压缩包后发现里面还有一首歌,先用了Audacity查看频谱图没有得到线索,我又用了SilentEye打开,得到 了一个百度网盘的链接



链接里又是一段音频,发现这是慢扫描SSTV,在kali中用QSSTV接收得到flag



#### High-level\_SMUpdf

题目给了一个加密的压缩包,里面有两个pdf

首先尝试密码爆破,其中一个pdf成功破解,发现是一篇文档,将其转成excel,得到flag.pdf的密码。打开flag.pdf 里面是一个ppt并没有flag。这里想到应该是pdf隐写,用wbStego4.3open解密一下,得到flag。

	0-1					Ð
查看	应用程序工具			~ 🕐	图像	视频 公
₹″r <sup>wbS</sup> <b>"<u>Re</u></b>	itego4.3open ady, Stead	y, Go!	×	搜索"wbStego4.3ope		
	tep 6	Current settings: Manipulated file: flag.pdf		335 КВ 27 КВ 26 КВ 944 КВ		
		Result: /123456.txt One	e m	tion Decoding process finis	×	
	Help	no encryption Select "Continue" to begin with the selected proces		ОК		,得到 新 eqo4
Ele	Settings	<< <u>B</u> ack	ntinue >>		-	
					CSDN	1 @玗耑玗耑z

flag{0urSMUPDF}

#### 病毒文件恢复

题目描述:

三明学院网络安全协会内部出现了勒索病毒,并且各位的重要工程文件都被黑客锁住,请各位SMUCTFers解锁被勒索病 毒锁住的文件。

查看附件后发现该病毒为---= GANDCRAB V5.1 =--- ,找到对应的解密工具BDGandCrabDecryptTool进行 解密,即可得到flag

	Bitdefender Decryption Utility for GandCrab V1,V4,V5.		- ×		
	Get the best ransomware protection Bitdefender 2019 intercepts any kind of ransomware attack	BUY NOW	Bitdefender *		
	Please enter the necessary information to start Scan entire system Backup files		r. f		
PI	Select the encrypted folder [FULL SYSTEM]				
		START TOOL	ADVANCED OPTIONS		BDGandGra bDecryptTo okexe
ext	ortion		ٽ ~		SDN @瑞瑞z xtortion"
^	名称 ^	修改日期	类型	大小	
	📄 flag.txt	2022/4/15 19:43	文本文档	1 KI	3
	NXGSZAGBX-DECRYPT.txt	2020/12/13 20:28	文本文档	csBN	3 @盱耑盱耑z

# 内存取证

下载附件得到 WIN.raw文件,文件居然有512M。首先打开010Editor看一下,并没有发现文件头,直接在010里 搜索文本" flag{ ",得到flag。

119	)2:	6AA0h:	67	65	64	69	74	2E	65	78	65	2C	2D	33	30	39	00	00	gedit.exe,-309	
119	92:	6AB0h:	2E	00	31	00	00	00	00	00	F9	70	8B	35	53	00	00	90	1ùp<5S	
119	)2:	6AC0h:	44	69	61	67	6E	6F	73	74	69	63	2E	52	65	73	6D	6F	Diagnostic.Resmo	
119	)2:	6AD0h:	6E	2E	43	6F	6E	66	69	67	00	00	63	00	75	00	6D	00	n.Configc.u.m.	
119	)2:	6AE0h:	65	00	6E	00	74	00	00	00	FC	70	8B	35	53	00	00	88	e.n.tüp<5S^	
119	92:	6AF0h:	66	6C	61	67	7B	62	30	39	32	34	63	65	33	32	64	61	flag{b0924ce32da	
119	)2:	6B00h:	64	62	65	65	36	63	34	65	63	65	63	31	37	64	66	33	dbee6c4ecec17df3	
119	92:	6B10h:	37	62	64	34	64	7D	00	00	E3	70	8B	35	53	00	00	90	7bd4d}ãp<5S	
119	92:	6B20h:	63	ЗA	5C	77	69	6E	64	6F	77	73	5C	73	79	73	74	65	c:\windows\syste	
119	92:	6B30h:	6D	33	32	5C	6D	73	70	61	69	6E	74	2E	65	78	65	00	m32\mspaint.exe.	
119	92:	6B40h:	2E	00	31	00	00	00	00	00	E6	70	8B	35	53	00	00	80	1æp∢5S€	
119	)2:	6B50h:	FF	FF	74	65	72	6E	65	74	20	45	78	70	6C	6F	72	65	ÿÿternet Explore	
119	92:	6B60h:	72	20	28	36	34	20	E4	BD	8D	29	00	B7	00	00	00	00	r (64 ä½.).∙	
119	92:	6B70h:	74	75	70	00	00	00	00	00	E5	70	8B	35	53	00	00	88	<u>tup</u> åp‹5S^	
119	92:	6B80h:	66	6C	61	67	7B	62	30	39	32	34	63	65	33	32	64	61	<pre>flag{b0924ce32da</pre>	
119	92:	6B90h:	64	62	65	65	36	63	34	65	63	65	63	31	37	64	66	33	dbee6c4ecec17df3	
119	)2:	6BA0h:	37	62	64	34	64	7D	00	00	E8	70	8B	35	53	00	00	90	7bd4d}èp<5S	
119	92:	6BB0h:	D0	21	C5	02	00	00	00	00	D0	21	C5	02	00	00	00	00	Ð!ÅÐ!Å	
119	92:	6BC0h:	70	0E	3C	03	00	00	00	00	A0	2B	28	F3	FE	07	00	00	p.< +(óþ	
119	92:	6BD0h:	00	69	70	00	31	00	00	00	EF	70	8B	35	53	00	00	90	.ip.1ïp‹5S	
119	92:	6BE0h:	68	E0	BC	02	00	00	00	00	40	0F	C5	02	00	00	00	00	hà¼@.A	
110	17・	GRENH.		55	່າງ		nn	<u></u>	<u></u>	nn	01		<b>^</b>	00	ີ່	61	۴C	۶C	·"	
׳	重找	\$ 文本: ^	fla	g{		<u>^``</u>	^	全	部(A	)	选项	ኳ(P)		66 6	C 61	67	7B			
查抄	梲结	课																		
	Γ	地址		值	i															
	Е	, 找到 2 个	'fla	g{'.																
	1	1926AF0	h f	flag{																
	1	1926B80ł	n f	flag{																CSDN @瑞瑞z
	l																			

### smuimg

这个题只给出了一张jpg的图片,看似没有任何线索,在010Editor中打开后发现别有洞天。

居然在文本栏中发现了PK,504B0304这不是zip的文件头吗。原来这张图片背后隐藏了一个压缩包。

A070h:	44	40	44	44	04	44	40	44	44	04	44	40	44	44	04	44	D@DD.D@DD.D@DD.D
A080h:	40	44	44	04	44	40	44	44	04	44	40	44	44	04	44	41	@DD . D@DD . D@DD . DA
A090h:	FF	D9	50	4B	03	04	14	00	00	00	80	00	53	00	3B	54	ÿÙ <mark>PK</mark> S.;T
A0A0h:	B7	55	3C	40	0B	95	00	00	30	BB	00	00	10	00	00	00	·U<@.•0»
A0B0h:	6F	75	74	67	75	65	73	73	66	6C	61	67	2E	6A	70	67	outguessflag.jpg
A0C0h:	EC	5B	05	54	94	5F	16	FF	E8	90	16	FC	D3	20	8C	32	ì[.Τ″ÿèüÓ Œ2
A0D0h:	30	82	4A	77	88	03	0C	8A	94	30	34	22	D2	82	D2	25	0,Jw <sup>^</sup> Š"(如何)的爱垢垢Z

分离图片与压缩包后,将其解压缩,又得到了一张图片与一个加密的压缩包。显而易见这个压缩包的密码肯定 在这张图片里。既然图片的名字叫outguessflag.jpg,那就试试outguess隐写吧。在kali里打开outguess,别忘了 压缩包注释里还有一行SMUCTF,那这个应该就是key。



成功得到密码。

打开压缩包后里面还是一张图片和一个压缩包,这次图片的名字叫F5flag.jpg,那就用F5-steganography-master。压缩包同样的注释,所以key还是SMUCTF。



成功得到下一个密码

这一次图片叫JPHSflag.jpg,那就用Jphswin来看看。

<ul> <li>flag.txt - 记事本</li> <li>文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)</li> </ul>	
flag{Have_Y0u_Seen_smuimg_steganography}	
JPHS for WIndows - Freeware version BETA test rev 0.5 -	×
Exit Open jpeg Hide Seek Save jpeg Save jpeg as Pass phrase C Help About	Options
	_
Input jpeg Director C:\Users\ZJR\Downloads\smuimg (6)\flag\flag\flag Filename JPHSflag.jpg	
Filesiz 41 Kb Width 763 pixel Height 750 pixel	
Approximate max / Kb recommended 4 Kb	
Hidden Director C:\Users\ZJR\Downloads\smuimg (6)\flag\flag\flag Filename flag.txt	
Filesiz 1 Kb	
Saved jpeg	
Director Filename	
Filesiz Kb	
This jpeg file already contains a hidden file	
	CSDN @瑞瑞z
ag!!	<b>从</b> 切得

# WEB

# Readflag

	10 1		
	ыт. 1		
	.ALC		"
法输入Linux会会来得到flag			
Hallin / revenue 4 Velamina			
		CSDN @	瑞瑞z

要求输入Linux命令,那首先想到flag应该是一个文件形式储存的,先 ls / 一下看看都有什么



XFF

$\leftrightarrow$ $\rightarrow$ C $\triangle$	▲ 不安全   175.178.102.149:7002
🔗 腾讯云 - 产业智变	🕉 百度搜索资源平台 🔾 360站长平台-站点 <mark>人</mark> 控制台 - 最
110.83.243.2错误!	你的IP不在访问列表之内!

CSDN @瑞瑞z

查一下robots.txt



打开burp抓包,伪造ip为1.1.1.1,成功得到flag。

#### linkup



出题人说这是一道游戏题,那不如直接把这个简单的连连看玩通关试试。试了几次都没完成,45秒倒计时太快了。打开burp抓包,不允许数据包返回服务器,这次随便倒计时都不怕了。

游戏通关,成功得到flag



#### Hello

打开链接,只有一句WELCOME来欢迎我,查看一下源码,发现还有一个upload.php。

打开upload页面

file:选择文件 未选择任何文件

请上传jpg gif png 格式的文件, 文件大小不能超过100KB

CSDN @瑞瑞z

先来个一句话木马,伪装成jpg,看看目录下都有什么文件。



进入返回的保存路径



bin boot dev etc flaaaaag home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var flag{c18ae73dddde113b0458caee4007a309} CSDN @瑞瑞z



## REVERSE

合金弹头

由GameMaker制作,W/A/S/D控制方向,U/I开火

又是一道游戏题,玩了几关还挺有意思。

这个题关键词之处就在于GameMaker。先用gm8decompiler解包得到.gmk文件,再用gamemaker打开,在背景 图中找到flag。

.\gm8decompiler.exe "hjdt.exe"

