BUUCTF_MISC题解

原创

TYUT_网安小菜鸡 ● 于 2021-05-30 22:12:54 发布 ● 1942 ◆ 收藏 24
分类专栏: BUUCTF 文章标签: 信息安全
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_52885531/article/details/117406720
版权



BUUCTF 专栏收录该内容

1 篇文章 0 订阅 订阅专栏

BUUCTF_MISC题解

第二题

将GIF图片用ps进行逐帧分解,可以得到三张特殊的照片



he11o

gif5.net



直接将三个照片里的内容拼接起来就好

第三题 二维码

下载好附件解压后发现是一个.png文件的二维码

■ QR_code.png 2018/11/6 18:07 PNG 文件	1 KB
--------------------------------------	------

用CQR扫描后得到二维码的结果



.png的文件尾是AE 42 60 82,按理来说在文件尾之后就应该结束,我们却发现png的文件尾后还跟着50 4B 03 04,这是.zip的文件头,说明在该照片下还隐藏着一个.zip文件,到这一步有两种方法:

- 1. 将50 4B 03 04之前的东西全部删掉,之后保存,将文件后缀名改为.zip
- 2. 用Linux中的binwalk将隐藏的.zip文件分离出来。语句: binwalk -e 文件名

然后打开这个.zip文件,解压它,但是!它居然加密了,我们看看是不是伪加密

伪加密这里可以看这个大佬的文章学习 https://blog.csdn.net/qq_26187985/article/details/83654197

禾	输入密码	×	2
•	输入加密文件的密码。		2
			-
	输入密码		
		~	
	□显示密码		
	密码管理器 确定 取消		
l			

再用二进制编辑器打开这个.zip文件

 CA OT CB /F AS 4F SU 4B
 0/ 08 40 S4 4C AE 10 00
 OPK. F4L...

 00 00 0F 00 00 00
 50 4B
 01 02
 1F 00 14 00 09 00
 PK.....

 08 00 8B 50 2F 48 46 34
 4C AF 1D 00 00 00 0F 00
 P/HF4I

发现核心目录区头504B0102四个bytes之后的数为: 09 00,而不是00 00,说明这个.zip文件加密方式是全局真加密,我们只能 去找密码了。可以看见压缩包内的.txt文件名为4numbers,说明密码是四位数字,那我们用kali自带的fcrackzip进行弱口令爆破就 行,语句为: fcrackzip -b -c1 -u -l4 文件名 root@kali2020:~/桌面 # fcrackzip -b -c1 -u -l4 1D7.zip

PASSWORD FOUND!!!!: pw = 7639 root@kali2020:~/桌面#

发现密码是7639

ok, 那就打开它

CTF{vjpw_wnoei}

这样就得到了flag

第四题 N种方法解决

下载附件之后发现是一个.exe文件,结果却发现打不开

此应用无法在你的电脑上运行

若要找到适用于你的电脑的版本,请咨询软件发布者。

那我们就试试拿二进制编辑器打开,看看它是个什么东东

📧 KEY.exe 🛛 🛛



关闭

哇哦,发现这个东西一点都不简单,哪是什么.exe文件,分明就是一个.jpg转成了base64,百度一下怎么办,发现只需要把那一 行丢到浏览器里打开一下就好。



手机扫一下,得到结果KEY{dca57f966e4e4e31fd5b15417da63269}

第五题 大白

这道题题目就给了很大的提示

Challenge	Top 3 Solves	>
	大白	
	1	
	—	
看不到图? 是	- 不是屏幕太小了注意:得到	的flag请包上flag{]
看不到图? 是 建交	- 不是屏幕太小了注意:得到	的flag请包上flag{]
看不到图? 是 是交 🛃 379140b0-c	 不是屏幕太小了注意:得到	的flag请包上flag{]
看不到图? 是 是交 ▲ 379140b0-c Flag	 不是屏幕太小了注意:得到	的 flag 请包上 flag{]

说明照片中是隐含了消息的,只不过不是我们屏幕太小看不见,而是它通过更改照片的尺寸给隐藏起来了

我们继续用二进制打开这个.png文件

 这里有一个知识点

用二进制打开的.png文件的第二行中,前四位表示的是宽度,后四位表示的是长度

我们将其进行修改

将其都修改成00 00 02 A7,再次打开照片就得到了想要的东西



第六题 你竟然赶我走?

这道题比较简单

我们直接拿二进制编辑器打开这个.jpg文件,而在它的最底部就写着flag



第七题 基础破解

Challenge	Top 3 Solves	>
	基础破解	
	1	
含你一个压缩的 匀哈哈哈哈哈哈 劻。。注意:彳	包,你并不能获得什么,因为 合哈。。。不对= =我说了什 得到的 flag 请包上 flag{} 提交	り他是四位数字加密 么了不得的东 を
•		
≥ 5 e46643e-b	_	
≥ 5e46643e-b		Submi

题目给了我们很大的提示:这是一个加密过的.rar文件,并且密码是四位数字。

本来以为和第三题一样用fcrackzip爆破,结果fcrackzip只能爆破.zip文件,那就百度一下吧

上网的过程中经常会碰到下载的rar压缩文件有密码,或者自己很久以前为了安全而加密的重要文件。现在忘记了密码需要暴力解的情况,今天我就专门教大家使用一个非常简单的工具RARPassw ord Unlocker 3.2绿色版,这个软件不用注册,而且是免费的,一分钟就可以学会哦。不过只针对RA R文件格式的密码破解, zip、7z等的格式不支持哦。

🚰 RAR Password Unlocker 3.2 试用 🛛 🚽 🕹 📈 🚽 🚽 🚽								
文件(F) 恢复(R)	帮助(<u>H</u>)							
▶ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	一 停止	? 帮助	① ^{关于}) 购买	[] 退出			
文件名 							打开	
恢复方式 暴力破 破解强加密类型	解 字典 选 文件	顷						
 ● 暴力破解(● 掩蔽暴力破) ● 漳蔽暴力破) ● 字典破解 	尝试所有可能的 解(如掩蔽一些已	密码组合) 2.知密码、符	号)					
日志窗口								
开始时间 状态与结果								
进度								
当前密码: 当前速度:		密码/每秒	þ					

我们选择第二个掩蔽暴力破解,因为我们已经知道密码是四个数字了

恢复方式	暴力破解 字典	选项	
密码长周	# 2	字符集	
最短	4 ▲	_ a - z 20 - 9 _ A -	- Z
最长	4 •	□ 自定义字符集 □ 字首	□字尾

我们这么配置一下,然后让它去跑一下

🔀 RAR Password Unlocl	ker 3.2			-		×
文件(F) 恢复(R) 帮助(F	H)					
17开 开始	 停止 帮助 	① 关于	退出			
文件名						
F:\CTF\BUUCTF\5e46643	e-be69-4c63-86ac-c00	9251 £2287	\基础碳解.rar		〔打开	
恢复方式暴力破解字	:典 选项					
密码长度	字符集					
最短 4 🚔	_a - z 20 -	9 🗌 A -	Z?!@#\$			
最长 4 🖨						
			U FR			
- 日志窗口						
开始时间	 状态与结果					
2021-5-23 22:07:52	开始恢复文件的密码:基	基础破解.r	ar			_
						_
进度						
当前密码: 0498 当前密码: 0498	5 家码/运孙					
	20					

这是跑起来的样子

RAR Pass	word Unic	ocker 3.2	式用				_		\times
と件(E) 恢复	夏(<u>R</u>) 帮助)(<u>H</u>)							
A			\bigcirc		1				
打开	开始	停止	帮助	关于	购买	退出			
文件名									
F:\CTF\BUU	CTF\5e4664	43e-be69-4	c63-86ac-c0	09251£2287	\基础破解.	rar		打开	
								1271	_
恢复方式 纂	暴力破解 :	字典 送	顷						
密码长度	密码已恢	复					×		
最短	该文件的	的密码已恢复	夏成功 ! 你现	见在可以用此	密码来打开	并提取文件。			
最长	点击 "夏	夏制"并以(Ctrl+V)粘贴	到需要解压的	的文件空白线	处打开压缩文件	‡!		
	文件的?	答码是:	2563			Į	制		
日志窗口				确定					
		一些太后结	Ħ						
7千%日中31日3	21.55.01	1030月始	未 文件的家庭,	甘て山て中分子。					
2021-6-23	21:55:01	开始恢复	文件的密码。	基础顿解.r	ar				
2021-5-23	21:58:02	恢复成功	,密码是:2	2563	-				
\		1							
进度									
当前密码:	23	96							
当前速度:	13	5	密码/每秒	少					

然后就跑到了密码: 2563

解压!

打开那个flag.txt



很显然使用base64加密的一段文字,俺们去在线解密一下

请输入要进行 Base64 编码或解码的字符

ZmxhZ3s3MDM1NDMwMGE1MTAwYmE3ODA2ODgwNTY2MWI5M2E1Y30=						
编码 (Encode)	解码 (Decode)	↓交换	(编码快捷键:	Ctrl + Enter)		
Base64 编码或解码的	的结果:					
flag{70354300a5100ba78068805661b93a5c}						

一不小心就得到了flag

第八题 乌镇峰会种图

下载附件之后是一个.jpg文件,观察照片里并没有什么有用的信息,还是老思路,用二进制编辑器打开,看看有没有藏什么信息

06 5C 1	E 8A 38 15 16 C5	DD D8 1F 4A D1 20 1F 9F	. \ 8 J
7A 29 C	2E 5A FB D1 4F 51	1F FF D9 0D 0A <mark>66 6C 61</mark>	z).Z.Qfla
67 7B 3	89 37 33 31 34 65	37 38 36 34 61 38 66 36	g{ 97314e7864a8f 6
32 36 3	32 37 62 32 36 66	33 66 39 39 38 63 33 37	2627b26f3f998c37
66 31 7	D		f 1} ←

事情就是如此的巧妙

第九题 LSB

题目给的信息很清楚LSB,也就是Least Significant Bit(最低有效位)。在大多数PNG问图像中,没个像素都由R、G、B三原色 组成,每种颜色一般用8位数据表示,如果修改其最低位,人眼是不能区分出这种微笑的变化的,因此可以利用没个像素的R、 G、B颜色的分量的最低有效位来隐藏信息,这样每个像素可以携带3位的信息。(摘编自c0d1_CTFer)

既然题目给的信息这么明显,那我们直接就按LSB来处理信息。

处理LSB最常用的软件是Stegsolve,我们打开这个.png文件,我们先一个个查看图像







由着三个图片可以看出来,在这三个通道上是隐藏了信息的,具体分析看看是什么信息

	الله المراجع ا	—		×			
-	Extract Preview						
	89504e470d0ala0a 000000d49484452 .PNGIHDR						
	0000011800000118 08020000008ec/e						
1	db00000542494441 54789ceddd416e23BIDA TxAn#						
	391000416931ffff b2f707c480932e57 9AilW						
	cb1157c3564b5682 8702c9f7d7d7d7dbW.VKV						
-	f837fffdf403c027 1012048404012141 .7'!A						
1	4048101012048404 012141e0cfe167ef @H!Ag.						
-	f77bec39729383e6 c30775788cbbdfca .{.9rux						
re	e5ffe5bbb/bcdff9 9f62458280902020bE						
	2408080902428280 9020202408080902 \$B \$			-			
-	Bit Planes Order settings						
		-					
	Alpha 7 6 5 4 3 2 1 0 Extract By ® Rot	w 🔾 Colur	nn				
50X	Red 7 6 5 4 3 2 1 0 Bit Order • MSE	First 🔾 L	SB First				
100							
	Green ☐ 7 ☐ 6 ☐ 5 ☐ 4 ☐ 3 ☐ 2 ☐ 1 🗹 0 Bit Plane Order						
1	S Blue 7 6 5 4 3 2 1 ≥ 0 ® RGB	GRB					
and the second	C RBG O	BRG					
	Preview Settings	BGR					
	Include Hex Dump In Preview 🖌						
	Preview Save Text Save Bin Cancel						

可以发现是隐藏了一个.png文件在这里,我们点击Save Bin将这个.png文件保存下来看看是什么

结果发现是一个二维码



扫描之后得到了信息

QR Research	- 🗆 X
文件(E) 工具(E) 帮助(H)	
📄 🔛 🔝 🔌 📀	ti 🔘 🖌
I I I I I I I I I I I I I I I I I I I	纠错等级 掩码 H(30%) Auto 版本 尺寸 Auto 4
	^
	~
已解码数据 1:	^
位置:(9.0,9.0)-(270.0,9.0)-(9.0,270.0)-(270.0,270.0) 颜色正常,正像 版本:3 纠错等级:H,掩码:4 内容: cumtctf{1sb_i4_s0_Ea4y}	
J	
	~
解码完成	11.

第十题 文件中的秘密

下载好附件打开后,发现是一个.jpeg格式的文件,还是老样子用二进制编辑器打开

首先我们就注意到了一点

FF D8 FF E0 00 10 4A 46	49 46 00 01 01 01 00 01JFIF
00 01 00 00 FF E1 10 A8	45 78 69 66 00 00 4D 4D Exi f. M
00 2A 00 00 00 08 00 03	87 69 00 04 00 00 00 01 · *

EXIF, 它是在提示我EXIF吗??

屏幕前的小伙伴可能没看过c0d1_CTFer所以这里简单介绍一下

EXIF(可交换图像文件格式)可以用来记录数码照片的属性信息和拍摄数据,EXIF可以被附加在JPEG、TIFF、RIFF等文件中,为其增加有 关数码相机拍摄信息的内容。缩略图或图像处理软件的一些版本信息。

所有我们直接用Windows自带的属性打开查看一下

属性	值		^
说明			
标题			
主题			
分级	$\begin{array}{c} & & \\ & & &$		
标记 🦰			
备注	flag{870c5a72806115cb5439345d8b0143	H	
来源			
作者			
拍摄日期			
程序名称			
获取日期			
版权			
图像 ———		-	
图像 ID			
分辨率	700 x 1167		
宽度	700 像素		
高度	1167 像素		
水平分辨率	1 dpi		
垂直分辨率	1 dpi		
位深度	24		
FT 45			×

芜湖,一切都是如此的妙不可言

第十一题 wireshark

题目提供了很详细的信息: wireshark抓到管理员登陆网站的一段流量包(管理员的密码即是答案)

下载好附件后,我们先用wireshark打开这个数据包

ctrl+f调出搜索框,依次选择分组字节流,宽窄,字符串,然后我们进行查找flag

公如今共达 、	中空	今姪中	flog	
刀垣子巾加一千	风作	子们中	- Tiag	

查找后发现结果的第一个数据包就含有flag,而在flag后紧跟着的就是password,这正好与对应,根据题目的指引,那么 password里的数据就是flag

6	1	69	6C	Зd	66	6c	61	67	26	70	61	73	73	77	6f	72	ail= <mark>flag</mark> &passwor
6	4	3d	66	66	62	37	35	36	37	61	31	64	34	66	34	61	d=ffb756 7a1d4f4a
6	2	64	66	66	64	62	35	34	65	30	32	32	66	38	66	61	bdffdb54 e022f8fa
6	3	64	26	63	61	70	74	63	68	61	3d	42	59	55	47		cd&captc ha=BYUG

第十二题 rar

首先看题目提示的很清楚,四个数字密码,而且附件是.rar我们就直接暴力破解密码

🔏 ARCHPR 4.54 - 87%		- 🗆	\times
文件(F) 恢复(R) 帮助(H)			
口令已成功恢复!	****	,	×
Advanced Archiv	ve Password Recovery 统计	h信息:	
总计口令	8,797		_
总计时间	29s 735ms		
平均速度(口令/秒)	295		
这个文件的口令	8795		6
十六进制口令	38 37 39 35		6
₩ 保存…	×	确定	
□ 空格□ 所有可打印字符	, w 24	用户定义	aB
状态窗口			
\dianli_jbctf_MISC_T10076_201507	707_rar.rar"已打开。		^
2020/10/25 23:04:35 - 口令已成功	×西 5恢复!		
2020/10/25 23:04:35 - '8795' 是这	个文件的一个有效口令		~
当前口令: 8795 已用时间: 29s 口令长度 = 4, 总计: 10,000, 已处理	平均速度: 剩余时间: 聖: 8,797	295 p/s 4s	
	87%		

<mark>8795</mark>

输入密码打开后发现一个.txt文件



得到了flag

第十三题 qr

下载好附件后是一个二维码,扫描之后得到了flag

~

第十四题 zip伪加密

题目告诉我们的信息很少但是已经足够了"zip伪加密"

果不其然,我们在打开附件的时候提示我们输入密码

但由于是伪加密,我们也不需要去爆破密码,我们依旧用二进制编辑器打开它

我们找到核心目录其头50 4B 01 02 后的8个字节

D8 75 32 72 D7 CD 0E D5 0D 8E F2 0C A8 05 00 50 .u2r......P 4B 01 02 1F 00 14 00 01 00 08 00 50 A3 A5 4A 21 K......P..J!

是01 00 说明这个zip是伪加密,我们只需要将其修改成00 00就解除了它的伪加密,就可以直接打开文件了

得到一个.txt文件,里面就是flag

▶1 flag{Adm1N-B2G-kU-SZIP}

第十五题 ningen

下载好附件之后是一个.jpg格式的文件,我们用二进制编辑器打开它,搜索504B0304(这是.zip文件的文件头)

D9 50 4B 03 04 14 00 01 00 00 00 D1 7E 96 45 32 . PK ~ E2 OF BA 58 32 00 00 00 26 00 00 00 0A 00 00 06 . . . X2 . . . & n

结果不小心发现了这个小东西

那我们就把50 4B 03 04之前的东西全部删掉,然后保存,并将文件名修改成.zip

我们将它打开,发现有密码,但是题目告诉了我们这是一个4位数字密码,我们用工具爆破一下

口令已成功恢复!		×
Advanced Are	chive Password Recovery 统计信息:	
总计口令	8,361	
总计时间	10ms	
平均速度(口令/秒)	836,100	
这个文件的口令	8368	- Ca
十六进制口令	38 33 36 38	<u></u>
	✔ 确定	

得到了密码,那就解压,打开,之后的我就不详细说明了哦

第十六题 镜子里的世界

我们下载好附件以后发现是一个.png文件,用二进制打开观察发现是一个纯纯的.png文件没有夹杂其它别的东西



那我们试试用StegSolve打开它,把所有通道都查看一遍之后没发现任何奇怪的地方,那就具体分析分析他的R、G、B通道的最 低有效位,哇哦,一不小心就发现了好东东

.	- 🗆 X
Extract Preview	
4865792049207468 696e6b2077652063 Hey I th ink we of the stafely 616e207772697465 20736166656c7920 an write safely 696e207468697320 66696c6520776974 in this file with stafely 6865757420616e79 6fe652073656569 hout any one sees 6e672069742e2041 6e797761792c2074 ng it. A nyway, the secret key is 3a2073743367305f 7361757275735f77 : st3g0_ saurus v 7233636b7300000 000000000000000000000000000000000000	
00000000000000 000000000000000000000000	· · · · · · · · · · · · · · · · · · ·
Bit Planes	Order settings
Alpha 7 6 5 4 3 2 1 0	Extract By Row Column
Red 7 6 5 4 3 2 1 0	Bit Order () MSB First LSB First
Green 7 6 5 4 3 2 1 0	Bit Plane Order
Blue 7 6 5 4 3 2 1 0	● RGB ○ GRB
Preview Settings Include Hex Dump In Preview 🖌	○ RBG○ BBR○ GBR○ BGR
Preview Save Text Save	Bin Cancel

第十七题 被嗅探的流量

被嗅探的流量,emmmm,很有味道□

用wireshark打开附件,和第十一题的步骤一样,我们在这么多数据包中搜索带有flag字符的

然后第一个包中上传了一个名叫flag的.jpg文件

2	66	6c	61	67	2e	6a	70	ilename= " <mark>flag</mark> .jp
5	6e	74	2d	54	79	70	65	g"••Cont ent-Type
ia	70	65	67	Ød	0a	Ød	0a	∶ image/ jpeg····

我们右键这个数据包,然后追踪它的TCP流,我们在所追踪出的TCP流中再进行查找flag,结果就得到了

第十八题 小明的保险箱

下载好附件之后是一个.jpg文件,但是题目说保险箱有一个四位数的密码,因此我们猜测在这个.jpg文件中肯定还隐藏了其他文件,我们用二进制编辑器打开这个文件。

A0 06 F1 9E DD 69 38 F6 FD 69 F4 50 07 FF D9 52i8..i.P....R 61 72 21 1A 07 00 CF 90 73 00 00 0D 00 00 00 00 ar!....s..... 我们发现FF D9就是.jpg的文件尾就应该结束了,可后面还加了52 61 72 21这正是.rar的文件头吗

说明这里还藏着一个.rar文件,那就很easy了,还是老规矩,我们把.rar文件分离出来(之前说了太多次怎么分了,这里就不加赘述了)

解压时很自然的发现需要密码,这也很正常,毕竟人家早就告诉你有密码了

我们依旧使用爆破工具进行爆破

恢复方式暴	力破解字典	选项
密码长度		字符集
最短	4 🔹	$\Box a = z \swarrow 0 = 9 \Box A = Z \Box = 2?!@#$$
最长	4 🔹	

设置好之后进行爆破

密码已恢复	×
该文件的密码已恢复成功! 你现在可以用此密码来打开并 点击 "复制"并以(Ctrl+V)粘贴到需要解压的文件空白处打	是取文件。 开压缩文件 !
文件的密码是: 7869	复制
确定	

一不小心就得到了密码

第十九题 爱因斯坦

下载好附件后打开发现是一个.jpg文件,用二进制打开,查找.jpg的文件尾FF D9发现在其后面还有一个.zip文件

 3F
 FF
 D9
 50
 4B
 03
 04
 0A
 00
 09
 00
 00
 A5
 2E
 61
 ?...PK
a

 47
 93
 78
 C7
 0D
 33
 00
 00
 27
 00
 00
 08
 00
 1C
 G x...3...'

 47
 93
 78
 C7
 0D
 33
 00
 00
 27
 00
 00
 08
 00
 1C
 G x...3...'

继续解压,发现是有密码的,但是题目没有给任何提示,我们无法确定这个密码的长短,如果直接使用暴力破解的话肯定要花费 很长的时间,所以暴力破解的思路肯定不对

那我们就继续在图片上找找,说不定会有密码

我们用老思路用StegSolve打开图片查看也没有找到任何信息,那我们就查查这个文件的EXIF

果然,在文件的属性中找到这么一句话

属性	值	^
说明 ———		
标题		
主题		
分级	$\begin{array}{c} & \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ $	
标记		
备注	this_is_not_password	
来源		
作者		
拍摄日期		
程序名称		
获取日期		
版权		
图像 ———		
图像 ID		
分辨率	1366 x 768	
宽度	1366 像素	
高度	768 像素	
水平分辨率	96 dpi	
垂直分辨率	96 dpi	
位深度	24	~
FT 40		

这里就很值得怀疑,我们拿去试试是不是密码,结果这还真的就是压缩文件的密码

就得到了flag

第二十题 easycap

下载好附件后发现可以用wireshark打开,打开之后,我们用之前的思路去查询分组字节流中的flag,显示查不到

那就直接追踪数据包的TCP流,结果答案就这么明显的摆在眼前

FLAG: 385b87afc8671dee07550290d16a8071

第二十一题 另外一个世界

打开附件发现是一个.jpg文件,继续用二进制编辑器打开仔细寻找发现里面有两个FF D8 FF,所以有两个.jpg文件,我们将这两个文件进行分离发现什么信息都没有,相反在源文件的基础上,我们直接搜索flag(66 6C 61 67)反而很轻易的看到了flag

2A 0D 0A 66 6C 61 67 ********..fl ag 3A 62 61 73 65 36 34 3A 28 4D 7A 63 33 59 32 4A : base64: (Nztc3Y2J 68 5A 47 52 68 4D 57 56 6A 59 54 4A 6D 4D 6D 59 hZGRhWNVj YTJ mMmY 33 4D 32 51 7A 4E 6A 49 33 4E 7A 63 34 4D 57 59 3NztC2NJ I 3Nztc4WNV 77 4D 47 45 3D 29 0D 0A 2A 2A 2A 2A 2A 2A 2A 2A 2A WNEE=)..*******

IZC3 YZJNZGKNIN	/WVjYTJmMmY3M2	2QzNjI3Nz	c4MWYwMGE=	
翩 (Encode)	解码 (Decode)	\$ 交换	(编码快捷键: Ctrl +	Enter)

第二十二题 FLAG

下载好附件之后发现是一个很很很搞笑的照片,我们还用之前的思路,拿二进制打开的话是一点信息都没有的,是一个很纯很纯的.png文件,所以我们猜测可能是用了LSB隐写,我们拿StegSolve打开它,分析它的数据

٩			
		Extract	t Preview
504b030414000000	0800dd855d49fd91	PK]I
e24cd90800003d21	0000010000031ed	.L=!	1.
5959cc0b5114be1d	b5336aafbdb10589	YYQ	.3j
aa7d0b5afc4ca5f6	da6219d5e94fe942	.}.Z.L	.bO.B
3bb56fb145637df0	8044e2c10389074f	;.o.Ec}.	.D0
b648ac41c4c34f42	244844ec5bec1141	.H.AOB	\$HD.[A
9d7be74c6f67e127	112fdce6ce37e7bb	.{.Log.'	./7
e79c7beedab9336b	ca4223048783e849	{3k	.B#I
20830995fc4e3f93	fdc82faccf00b97e	N?.	/~
a4265c5b9316a41a	c855753d867e037e	.&\[.Uu=.~.~
	0.100.01.0000.01.000	1 0 0 1	

发现这里应该是隐藏了.zip文件,我们将它分离出来,命名成.zip文件,打开的话提示我们数据损坏



这里可以不用管它,继续打开里面的文件就好

打开发现是一堆乱码,但是我们在乱码中找到了最重要的东西

题目上提示了把hctf换成flag就好

第二十三题 假如给我三天光明

呼~

这应该是目前遇到最难的一道题了

打开附件后发现,有一个照片和被加密的压缩包,那么密码肯定在这个照片里

打开发现照片底下的确藏有东西,但是不知道是什么

٠	٠	•	•	٠		٠	•	٠		٠	٠	٠
			•		•		•			•		٠
٠	٠			•		•		•	 	٠		0

首先猜测的是二进制,但是按它两位两位排列只能写三个数字,所能隐藏的信息太少了,所以应该不是二进制题目给了我们很大的提示"假如给我三天光明",这该不是盲文吧,百度一下,嘿!盲文还真的就长这个样子



然后就推出密码是kmdonowg

打开压缩包发现是个音频文件,听的话是摩斯密码,但是我实在太菜了,靠听真的听不出来,所以只能借助工具——Audacity 我们获得这个.wav的波形图



长的一段是-,短的一段是.然后结合摩斯密码表就得到了答案

1		С
2	-	t
3		f
4		W
5		р
6	•	е
7		i
8		0
9		8
10		7
11		3
12		2
13		?
14		2
15		3
16		d
17		Ζ

第二十四题 神秘的龙卷风

根据题目知道,这个压缩包的是由四位密码组成的,我们用爆破工具爆破

开始时间	状态与结果	
2021-5-28 16:16:26	开始恢复文件的密码:神秘龙卷风.rar	
2021-5-28 16:16:53	恢复成功,密码是: 5463	

打开压缩包发现是一个.txt文档,可是打开后发现真的是外星人语言



这下可真的啥也不知道了,只能百度搜题解,发现这是一种编程语言叫brainfuck

可以在线执行(http://bf.doleczek.pl/)



第二十五题 后门查杀

这是一道看起来很难很难的题,它有一大堆的.php文件

题目上提示是webshell上传,我们直接用杀软扫描刚刚下载好的附件,如果真的存在webshell上传的话,那么一定会报毒的

F:\CTF\BUUCTF\后门查杀\html\include\include.php	待处理	详情
后门病毒 Backdoor/PHP.WebShell.h		

我们按照路径找到那个文件



很容易就能找到flag

第二十六题 荷兰宽带数据泄漏

根据题目信息得到这是文件应该是宽带数据流量,那么我们就需要用相对应得工具打开,百度到的是需要用routerpassview打开

那就下个它打开文件



按照我们之前做题的经验,flag一般会藏在用户名或者密码当中,我们就在这堆数据里找username和password,然后一个一个 去提交,看那个是真正的flag

终于我们找到了那个万恶的flag

<Username val=053700357621 />
<Password val=210265 />

就是用户名

第二十七题 来首歌吧

打开附件之后发现是一个音频文件

我们还用Audacity进行查看,发现在这首歌中有两个轨道



而上面那一条轨道正是莫斯密码

我们将其写下来

再在线转换一下就得到了flag

英文字母:
5BC925649CB0188F52E617D70929191C
转换为摩斯电码 清除 生成摩斯代码的分隔方式: ◎ 空格分隔 ○ 单斜杠/分隔
摩斯电码: (格式要求: 可用空格或单斜杠/来分隔摩斯电码, 但只可用一种, 不可混用)
<i>//</i>

第二十八题 数据包中的线索

下载好附件后用wireshark打开,我们可以一个一个分析这些数据包,发现只有一种类型的数据包是很可疑的,它与其他数据包 很不一样,其他数据包没有多少信息,而只有这个数据包里含有很多信息

	0000	0c	da	41	9e	СС	85	20	89	84	32	73	c5	08	00	45	00	···A···· · ·2s····E·	
	0010	01	a9	45	dc	40	00	40	06	00	00	ac	10	42	64	ac	10	••E•@•@••••Bd••	
	0020	50	78	07	5b	00	50	c1	88	86	87	21	e5	02	ac	50	18	Px · [· P · · · · ! · · · P ·	
	0030	40	29	ec	98	00	00	47	45	54	20	2f	66	65	6e	78	69	@)····GE T /fenxi	
	0040	2e	70	68	70	20	48	54	54	50	2f	31	2e	31	Ød	0a	48	.php HTT P/1.1 ··H	
	0050	6f	73	74	3a	20	31	37	32	2e	31	36	2e	38	30	2e	31	ost: 172 .16.80.1	
	0060	32	30	Ød	0a	43	6f	6e	6e	65	63	74	69	6f	6e	3a	20	20 ·· Conn ection:	
	0070	6b	65	65	70	2d	61	6c	69	76	65	Ød	0a	41	63	63	65	keep-ali ve··Acce	
	0080	70	74	3a	20	74	65	78	74	2f	68	74	6d	6c	2c	61	70	pt: text /html,ap	
I	0000	70	60	60	62	61	74	60	6f	60	2f	70	60	74	64	60	ah	plicatio n/vhtml;	

我们进行追踪它的TCP流

📕 Wireshark · 追踪 TCP 流 (tcp.stream eq 7) · 流量中的	案,pcapng	- 0	×
GET /fenxi.php HTTP/1.1			^
Host: 172.16.80.120			
Connection: keep-alive			
Accept: text/html,application/xhtml+xml	application/xml;q=0.9,image/webp,*/*;q=0.8		
Upgrade-Insecure-Requests: 1			
User-Agent: Mozilla/5.0 (Windows NT 6.1	; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro	me/44.0.2403.130 Safari/	
537.36			
Accept-Encoding: gzip, deflate, sdch			
Accept-Language: zn-CN,zh;q=0.8			
HTTP/1.1 200 OK			
Date: Tue, 18 Aug 2015 09:09:39 GMT			
Server: Apache			
X-Powered-By: PHP/5.3.3			
Connection: close			
Transfer-Encoding: chunked			
Content-Type: text/html; charset=UTF-8			
1513c			
/9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAAIBAQI	BAQICAgICAgICAwUDAwMDAwYEBAMFBwYHBwcG		
BwcICQsJCAgKCAcHCg0KCgsMDAwMBwk0Dw0MDgs	MDAz/2wBDAQICAgMDAwYDAwYMCAcIDAwMDAwM		2
DAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw	MDAwMDAwMDAwMDAz/wAARCAHgAkQDASIA		
AhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAA	CAWQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQA		
AAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0K	kwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3		
ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3F	ldnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWm		
p6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19j	Z2uHi4+T15ufo6erx8vP09fb3+Pn6/8QAHwEA		
AwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/BQ	ATREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSEx		
BhJBUQdhcRM1M0EIFEKRobHBCSMZUVAVYnLRChY	<pre>cNOE18RcYGRomJygpKjU2Nzg50kNERUZHSE1K</pre>		
UIRVVIdYWVPJZGVmZZnpanN0dXZ3eH16gOUEnYa	11 Inkkp0012axmJmaoq0kpaanqkmqsr00tba3		
ULmowsPExcoHymnk@tP01dbX2Nna4uPkSebnoor	28VP09TD3+Ph6/90ADAMBAAIKAXEAPWD9/KKK		
KALIIIgAODOOAKKKKALIIIgAODOOAKKKKKALIIIg	ACODDAKKKKALIIIgADODDAKKKKALIIIgADOOD		
AKKKKACIIIgAOOOOAKKKKACIIIgAOOOOAKKKKAC	(KACiiigAooooAKKKKACIIIgAOOOOAKKKKACIIIgA		
iighoocoAKKKKACIIIghoocoAKKKKACIIIghoocoAK	AKACIIIgADODDAKKKACIIIgADODDAKKKKACI		
KACijigAooooAKKKKACijigAooooAKKKKKACijig	A0000AKKKKACijijgA0000AKKKKACijijgA0000		
AKKKKACijjgAooooAKKKKACijjgAooooAKKKKAC	iiigAcoonAKKKKACiiigAcoonAKKKKACiiigA		
0000AKKKKACiiigA0000AKKKKACiiigA0000AKK	(KACiiigAooooAKKKKACiiigAooooAKKKKACi		
iigAooooAKKKKKACiiigAooooAKKKKKACiiigAooo	DAKKKKACiiigAqqqqaAKKKKACiiigAqqqqaKKK		
KACIIIaAaaaaAKKKKACIIIaDifix.mmDuaua3	SVANDADECADATINATINASES NUT YOVE INNEED		~
71里 62+1 高パ ⁴ 間 分間, 60 屋赤器 分里, 1 seca(s), 点击盛祥。 (軟へ3):ス (ostra)	mundation appret		
THE COULD	Show data as Abort	7 38 	-
童我:		重我下一个	-00
	滤掉此液 打印 另存为…	返回 Close Hel;	2

这里看起来就很可疑了,貌似是base64编码,我们在一个网站进行在线解码一下(https://the-x.cn/base64)

常規Base64	CSS Base64	DES加密/解密	3DES加密/解密	AES加密/解密	RSA	密/解密			点击关闭
/9j/4AAQSkZJRgAE BwclCQsJCAgKCA DAwMDAwMDAwM AhEBAxEB/80AHw AAF9AQIDAAQRBF ODk60QRFRkdISU p6ipqrKztLW2t7i5us AwEBAQEBAQEBA	IAQEAYABgAAD/2 CHCg0KCgsMDAw DAwMDAwMDAwM AAAQUBAQEBAC RIhMUEGE1FhByJ pTVFVWV1hZWm iLDxMXGx8jJyILT1 QAAAAAAAAAAAAECA	wBDAAIBAQIBAQIG MBwkODw0MDgsh MDAwMDAwMDAwM EAAAAAAAAAAA IxFDKBkaEII0KxwR NkZWZnaGlqc3R1d NXW19jZ2uHi4+TI5 wQFBgclCQQL/8Q/	CAGICAGICAwUDAwMI IDAz/2WBDAQICAGMU MDAwMDAwMDAwMD CAw0FBgcICGoL/80/ VS0fAkM2JygkKFhcY Ind4eXqDhIWGh4JlgK Sufo6erx8vP09b3+Pn6 ttREAAgECBAQDBAct	DAWYEBAMFBWY MAWYDAWYMCAci AwMDAwMDAz/w AlRAAAgEDAwlE/ GRolJicoKSo0NT TIJWW15iZmqKjpł /8QAHwEA FBAQAAQJ3AAE	HBwcG DAwMDA AARCAH AwUFBAQ Y3 (Wm CAXEEBS	wM 9AKQDASIA A Ex			
		编码源格式	: O文本	课 : 自动检测	Ý	中文编码:	UTF-8	~ 【编码	解码
该内容已经被插件设 但未提供可供调的文 如需查看hex内容,	捌为二进制数据。 (本信息,旦数据量 请关闭自动模式!	较大,故不在此处显	示hex内容。			401 UT	插件【Jpeg】 弓存为: Jpg 付加信息: Size:580x4 forast:261	Jpeg Image(文件 180	JFIF)
						ton tota	显示内容非则 数据长度:6: 插件数:18,	酸 治信息 ❷ 3,089 Bytes 耗时:2ms	×

发现是一个.jpg文件,我们下载打开,就发现了神奇的小秘密



第二十九题 九连环

我们下载好附件后发现是一个.jpg文件,按照之前的旧思路用二进制编辑器打开,我们去搜索.zip的文件头(504B0304)发现 有很多,而且根据题目"九连环"也感觉这个文件不是那么简单

10	84	02	10	84	07	FF	D9	50	4B	03	04	0A	00	00	08
00	00	Æ	54	53	4B	00	00	00	00	00	00	00	00	00	00
00	00	04	00	00	00	61	73	64	2F	50	4B	03	04	14	00

我们就打开kali用binwalk分析一下

root@kali2020:	~/桌面# binwalk	123456cry.jpg
DECIMAL	HEXADECIMAL	DESCRIPTION
0 19560 48454 48657 48962	0×0 0×4C68 0×BD46 0×BE11 0×BF42	JPEG image data, JFIF standard 1.01 Zip archive data, at least v1.0 to extract, name: asd/ Zip archive data, at least v1.0 to extract, compressed size: 184, uncompressed size: 184, name: asd/qwe.zip End of Zip archive, footer length: 22 End of Zip archive, footer length: 22

发现果然有东西,那就用foremost分离一下



得到了一个.zip文件

打开的话发现是有密码的,那就用二进制编辑器判断一下是不是伪加密

31 83 48 D8 01 50 48 01 02 3F 00 14 00 01 08 08 1. H. PK. ?..... 00 48 4E 53 4B 8C 3A D5 7E 88 70 00 00 28 75 00 . HNSK :. ~. p. . (u.

果然是伪加密,将0108修改成0008,绕过伪加密



good-已合并. jpg



发现里面只有一个.jpg和一个加密了的压缩包

而照片里没有提供任何信息(用之前解密.jpg的思路)

这里用steghide来破解

root@kali2020:~/桌面# steghide extract -sf good-已合并.jpg Enter passphrase: wrote extracted data to "ko.txt".

1 看到这个图片就是压缩包的密码:

·2 bV1g6t5wZDJif^J7

输入密码解压之后就能看到flag了

第三十题 面具下的flag

打开附件发现是一个.jpg照片,用二进制编辑器打开的话可以搜索到文件中包含504B0304,可以断定文件中隐藏了.zip文件

用binwalk分析一下

root@kali2020	otäkal12020:-/桌图# binwalk mianju.jpg							
DECIMAL	HEXADECIMAL	DESCRIPTION						
0 12 478718 632615	0×0 0×C 0×74DFE 0×9A727	JPEG image data, EXIF standard TIFF image data, Little-endian offset of first image directory: 8 Zip archive data, at least v2.0 to extract, compressed size: 153767, uncompressed size: 3145728, name: flag.vmdk End of Zip archive, footer length: 22						

思路正确

那就用foermost分离出来



打开压缩包解压的时候发现被加密了,二进制编辑器打开发现是伪加密,直接改掉

I	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	90	۲I	υı	5V 4D	MN
	01	02	3F	00	14	00	09	00	08	00	6C	87	42	49	56 A1	?I.BIV.
	A2	02	A7	58	02	00	00	00	30	00	09	00	24	00	00 00	X 0 \$

改成<mark>00 00</mark>

打开发现是一个.vmdk文件,本来的思路是将它挂载到kali上,但是只能发现一半的flag,另一半怎么也发现不了,最后百度了一下,发现这个东西不需要挂载到kali上,直接用kali里的命令7z解压就行,命令:

7z x flag.vmdk -o./

解压以后会在flag_part_two中发现一个挂载没有的文件



依次打开part_one和part_two中的文件,一个是我们之前提到过的brainfuck一个是Ook

在这个网站中解码就好

https://www.splitbrain.org/services/ook

然后就可得到flag

flag{N7F5_AD5_i5_funny!}



详细解法请参考第第二十五题