BugKu ——WP（MISC[二]）

原创

窝窝头_233 于 2019-11-28 16:35:18 发布 152 收藏

分类专栏： CTFwriteup 文章标签： ctf BugKuCTF

本文链接：https://blog.csdn.net/hahaha233330/article/details/103264093

BugKu ——MISC部分

[0] 工具：

①Winhex：图片隐写工具，可通过搜索“ctf”“CTF”“key”“flag”等关键字得到flag。
②在线工具HtmlEncode/BASE64转换：注意源代码里奇怪的字符串，可以尝试解码（分清类型）。
③Binwalk：可查看多重文件。使用说明
④VMware（kali_Linux）：虚拟机，方便解压、写一写脚本。

- **11、多种方法解决**
  在做题过程中你会得到一个二维码图片

用winhex打开显示的是base64码，联想该题的提示：在做题过程中你会得到一个二维码图片，通过在线解码器将base64码转成图片。扫一下码就可以得到flag。

KEY.exe

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	64	61	74	61	3A	69	6D	61	67	65	2F	6A	70	67	3B	62	data:image/jpg;b
00000010	61	73	65	36	34	2C	69	56	42	4F	52	77	30	4B	47	67	ase64,iVBORw0KGg
00000020	6F	41	41	41	41	4E	53	55	68	45	55	67	41	41	41	49	oAAAANSUhEUgAAAI
00000030	55	41	41	41	43	46	43	41	59	41	41	41	42	31	32	6A	UAAACFCAYAAAB12j
00000040	73	38	41	41	41	41	41	58	4E	53	52	30	49	41	72	73	s8AAAAAXNSR0IArs
00000050	34	63	36	51	41	41	41	41	52	6E	51	55	31	42	41	41	4c6QAAAARnQU1BAA
00000060	43	78	6A	77	76	38	59	51	55	41	41	41	41	4A	63	45	Cxjwv8YQUAAAAJcE
00000070	68	5A	63	77	41	41	44	73	4D	41	41	41	37	44	41	63	hZcwAADsMAAA7DAc
00000080	64	76	71	47	51	41	41	41	72	5A	53	55	52	42	56	48	dvqGQAAArZSURBVH
00000090	68	65	37	5A	4B	42	69	74	78	49	46	67	54	76	2F	33	he7ZKBitxIFgTv/3
000000A0	39	36	54	78	35	36	34	47	31	55	6F	75	69	63	4B	67	96Tx564G1UouicKg
000000B0	31	39	68	77	50	43	44	63	72	4D	4A	39	6D	37	2F	37	19hwPCDcrMJ9m7/7
000000C0	6E	34	35	7A	66	64	78	65	35	5A	33	73	4A	37	70	72	n45zfdxe5Z3sJ7pr
000000D0	48	62	66	39	72	58	4F	33	50	34	6C	4C	76	59	50	63	Hbf9rXO3P4lLvYPc
000000E0	74	62	65	4D	38	30	64	76	74	50	2B	33	70	6E	44	70	tbeM80dvtP+3pnDp
000000F0	39	79	46	37	74	6E	65	51	76	76	6D	63	5A	75	2F	32	9yF7tneQvvmcZu/2
00000100	6C	66	37	38	7A	68	55	2B	35	69	39	79	78	76	34	54	lf78zhU+5i9yxv4T
00000110	33	54	32	4F	30	2F	37	65	75	64	36	38	4F	54	32	48	3T2O0/7eud68OT2H
00000120	33	4C	43	66	74	30	6C	2F	61	65	39	5A	6C	54	6F	2B	3LCft0l/ae9ZlTo+
00000130	32	33	70	50	76	58	37	2F	72	77	4A	48	62	66	63	73	23pPvX7/rwJHbfcs
00000140	49	2B	33	61	57	39	5A	33	33	6D	31	47	6A	37	4C	65	I+3aW9Z33m1Gj7Le
00000150	6E	2B	39	62	73	2B	50	49	6E	64	74	35	79	77	54	33	n+9bs+PIndt5ywT3
00000160	64	70	37	31	6D	66	4F	54	58	61	66	6B	75	36	66	2F	dp71mfOTXafku6f/
00000170	32	75	44	30	39	69	39	79	30	6E	37	4E	4E	64	32	6E	2uD09i9y0n7NNd2n
00000180	76	57	5A	30	36	4E	74	74	2B	53	37	6C	2B	2F	36	38	vWZ06Ntt+S7l+/68
00000190	4D	4A	63	35	4F	30	4F	53	57	70	63	79	65	78	6E	46	MJc5O0OSWpcyexnF
000001A0	6A	66	63	73	49	2B	4A	57	31	75	6B	70	52	66	76	2B	jfcsI+JW1ukpRfv+
000001B0	76	44	43	58	4F	54	74	44	6B	6C	71	58	4D	6E	73	5A	vDCXOTtDklqXMnsZ
000001C0	78	59	33	33	4C	43	50	69	56	74	62	70	4B	55	58	37	xY33LCPiVtbpKUX7
000001D0	2F	72	77	77	6C	7A	6B	37	51	35	4A	61	6C	7A	4A	37	/rwwlzk7Q5JalzJ7
000001E0	47	63	57	4E	39	79	77	6A	34	6C	62	57	36	53	6C	46	GcWN9ywj4lbW6SlF
000001F0	2B	2F	36	38	4D	4A	63	35	4F	30	4F	53	57	70	63	79	+/68MJc5O0OSWpcy
00000200	65	78	6E	46	6A	66	63	73	49	2B	4A	57	31	75	6B	70	exnFjfcsI+JW1ukp
00000210	52	66	76	2B	76	44	43	58	4F	54	57	45	37	61	2F	69	Rfv+vDCXOTWE7a/i
00000220	37	32	50	73	74	4A	32	7A	66	73	48	6E	4F	54	70	50	72PstJ2zfsHnOTpP
00000230	7A	36	58	52	39	4F	6D	4A	76	45	63	74	4C	32	64	37	z6XR9OmJvEctL2d7
00000240	48	33	57	55	37	61	76	6D	48	33	6D	4A	73	6B	35	64	H3WU7avmH3mJsk5d
00000250	66	76	2B	6E	44	43	33	43	53	57	6B	37	61	2F	69	37	fv+nDC3CSWk7a/i7
00000260	33	50	63	74	4C	32	44	62	76	48	33	43	51	70	76	33	3PctL2DbvH3CQpv3

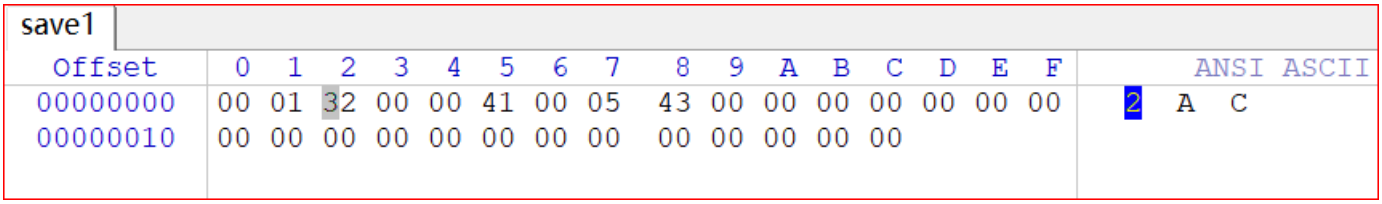
- **12、闪得好快**
  这是二维码吗？嗯。。。是二维码了，我靠，闪的好快。。。

看格式是gif图片，打开后发现这个二维码在不停的闪，无法正确扫码。利用PS工具，将gif文件一帧一帧的查看并扫描，拼接扫描信息，拿到flag。

- **13、come_game**
  听说游戏通关就有flag。

总觉得不可信，先玩一把试试，打开竟然是噩梦游戏I wanna，我这么菜肯定玩不了通关。然后发现桌面上多了三个文件，中间那个叫`save1`，猜测可能是保存游戏数据的。用notepad++、vc6.0、java、记事本等打开都是乱码，最后一试：winhex，就决定是你了！

打开发现只有一个数字。猜测可能是记录关卡进度的。改成较大数字试试。



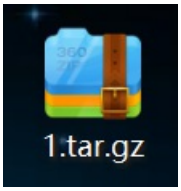
再打开.exe就可以看到flag了。
注意直接提交会被提示错误，这里没有提示格式，其实格式是`SYC{*******}`，别问我怎么知道，我也是看大佬解的orz...

- **15、linux**
  linux基础问题

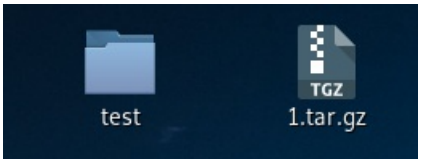
既然题目叫linux，不妨把它放在虚拟机下试试。
题目打开是个`tar.gz`文件，放在linux下解压。

*这里插播广告一则，关于在VMware怎么安装kali的教程

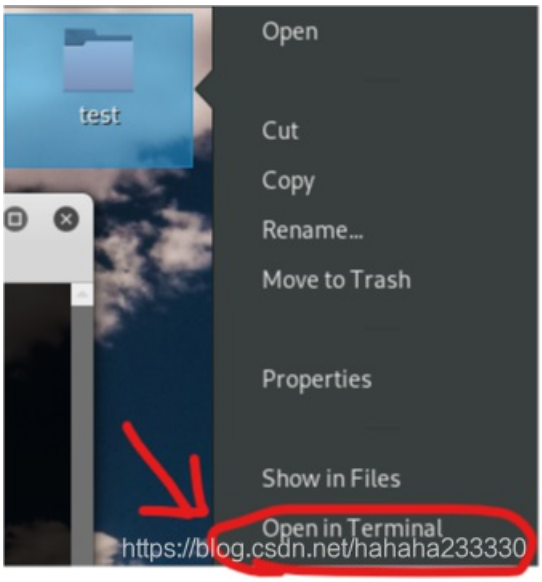
*另外，怎么在虚拟机和本机之间互传文件



直接把包拖到虚拟机里去。解压得到了文件夹里面是 flag。但是不知道文件格式，无法正常打开。

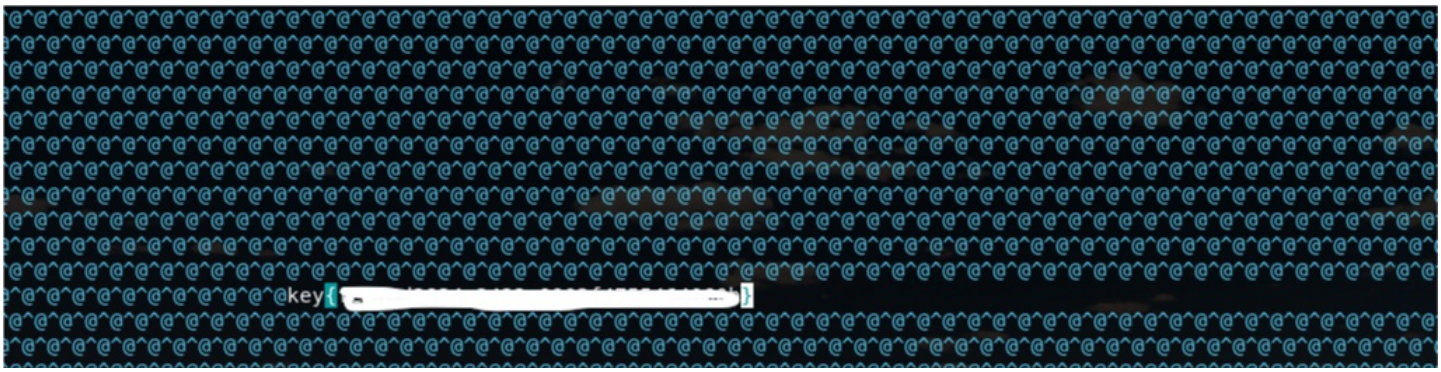


选中test文件，右键鼠标用终端`terminal`打开。



输入`vi flag`，进入编辑文件。

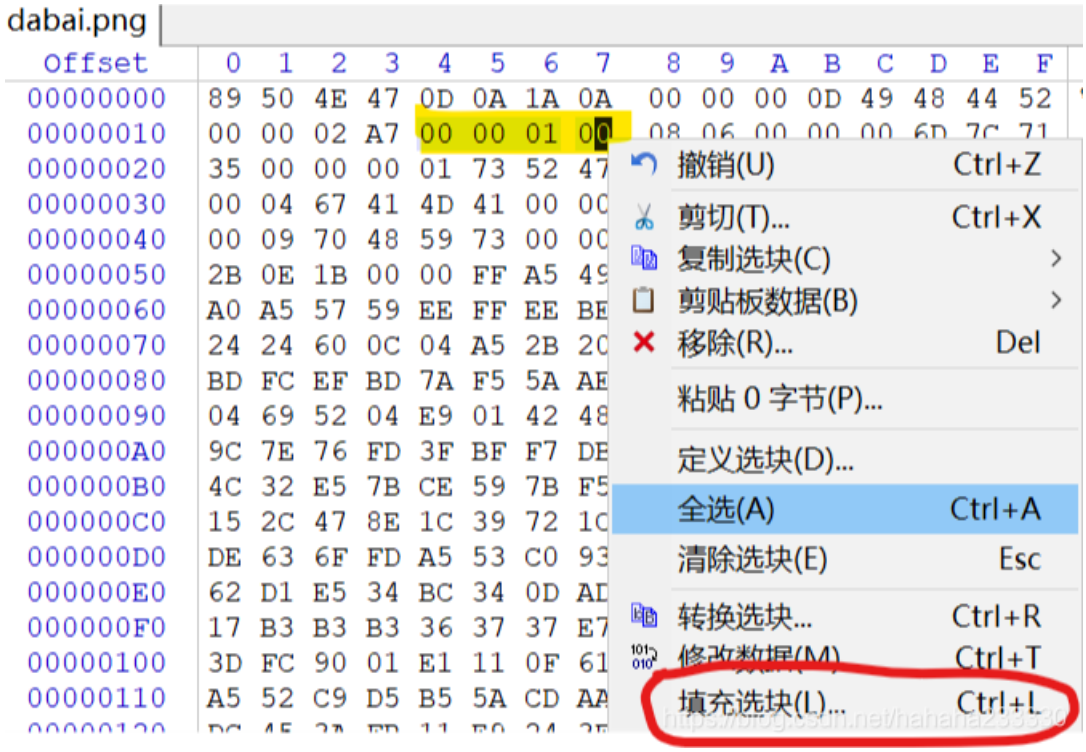
一点点往下浏览，查找有无flag，提示：全屏更好找。



- **16、隐写3**

图片正常，可以直接打开，但总觉得图片太矮了。思考图片隐写相关类型，可能是高度异常，并查看该图片属性，该图可能被截取了下半部分。开始尝试用winhex修复JPG文件的原始高和宽。

如下图黄色位置代表宽，选中最后两位修改数值：鼠标右键——编辑——填充文件，直接将图片大小修改为“FF”（最大），点击保存，再打开就可以看到图片最下方的flag信息。




Hello~
flag[redacted]
https://blog.csdn.net/hahaha233330