bugku-writeup-MISC-隐写2



01—binwalk查看文件

binwalk -e yinxie2.jpg

(kali⊛kal ∟ <mark>\$</mark> binwalk -	i)-[∼] e <u>vinxie2.jpg</u>	
DECIMAL	HEXADECIMAL	DESCRIPTION
0 30 52516 59264	0×0 0×1E 0×CD24 0×E780	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image directory: 8 Zip archive data, at least v1.0 to extract, compressed size: 6732, uncompressed size: 6732, name: flag.rar End of Zip archive. footer length: 22
147852 ome	0×2418C	End of Zip archive, footer length: 22 https://blog.csdn.net/qq_22597955

dd if=yinxie2.jpg of=ynixie2.zip skip=52516 bs=1

使用binwalk命令转换为zip文件。

<pre>(kali@kali)-[~] \$ dd if=yinxie2.jpg of=ynixie2.zip skip=52516 bs=1 95358+0 records in 95358+0 records out 95358 bytes (95 kB, 93 KiB) copied, 0.416004 s, 229 kB/s</pre>									
	ynixie2.zip		_ - ×						
Archive Edit View Help									
🗈 🚹 Open 🔫	🖬 Extract 🕒	•							
< > ^ 🖻	Location: 💼 /								
Name	👻 Size	Туре	Date Modified						
📕 flag.rar	6.7 kB	RAR archive	14 November 2017,						
▶ 提示.jpg	92.4 kB	JPEG image	14 November 2017,						
	https://blog.csd	dn.net/gg_22597955							

告诉你们一个秘密,密码是3个数哦。 查理曼: 查理曼,法兰克王国国王,征服了西欧与中欧大部分 土地,具有了至高无上的权威,下令全国人民信仰基 督教,查理重振了西罗马帝国。 雅典娜: 女神帕拉斯·雅典娜,是希腊神话中的女战神也是智慧 女神,雅典是以她命名的。 兰斯洛特, 英格兰传说中的人物,是亚瑟王圆桌骑士团中的一 员。看上去就是一个清秀年轻的帅小伙儿,由于传说 中他是一名出色的箭手,因此梅花J手持箭支。兰斯洛 特与王后的恋爱导致了他与亚瑟王之间的战争。 Hint: 其实斗地主挺好玩的。

https://blog.csdn.net/qq_22597955

得到zip文件,查看flag.rar需要密码,再看看提示.jpg,提示密码为3个数。考虑使用爆破工具。



02—fcrackzip压缩文件密码爆破

使用fcrackzip进行简单密码的爆破,kali中安装和使用链接:

https://blog.csdn.net/qg 22597955/article/details/118751974?spm=1001.2014.3001.5502

得到密码为871



输入密码,得到3.jpg图像如上所示。

03---010 editor 查看图片

File	Edit	Sea	rch	Viev	w F	orm	nat	Scri	pts	Ter	mpla	ites	De	bug	Тс	ools	Window H	lelp									
L 🗋 -	~ 📂	~ 🔒		.	i i	i 1	‰	t i	i 1	? (L R	۶	<mark>∄</mark> ₿ I	> -	→ 1		🧕 l 🛛 🕂 🛐	¶ []		💼	7	*	<u>a.</u>	之	*	510 16 5	
Start	up	And	lroid	Man	ifest	.xml		3.jp	g×																		
	() 1	2	3	4	5	6	7	Š.	9	Α	В	С	D	Е	F	012345678	9ABCI	DEF								
1990	h:F	E 36	06	F5	EF	70	05	C5	A7	93	81	BA	E7	57	D4	E7	þ6.õïp.ŧ	".°çV	٨Ôç								
19A0	h: 2	6 90	9C	25	9D	71	1A	FB	E1	02	C 0	6F	44	95	0D	57	&.œ%.q.ûá	i.ÀoD	•.W								
19B0	h: 9	E C2	AF	59	1B	9E	6F	1A	DD	6B	B 5	E7	58	F8	34	1E	žÂ Y.žo.Ý	ʹkμçXø	ø4.								
19C0	h: E	B C8	58	81	3B	7B	0D	60	23	2C	14	E0	14	13	4D	9C	ëÈX.;{.`#	ŧ,.à.	. Mœ								
19D0	h: F	1 F2	89	C2	0B	C 0	9C	0A	C7	BE	BF	78	68	50	25	31	ñò‰Â.Àœ.Ç	∰;xhF	P%1								
19E0	h: 0	A 83	C7	43	BF	38	35	0B	11	D3	98	2D	4D	EF	EF	83	.fÇC;85	Ó~-Mi	ïïf								
19F0	h: 9	5 4D	9A	5C	01	54	DA	ЗA	F1	8E	2D	1E	6A	56	E1	B1	•MŠ∖.TÚ:ñ	íŽj∖	√á±								
1A00	h: 7	6 83	BE	19	02	12	19	85	DD	F5	2F	71	D9	F8	ED	F8	v f¾Ý	νõ/qÙ¢	øíø								
1A10	h: D	6 32	7B	25	E4	F1	53	17	8C	80	50	37	D7	1D	BF	9C	Ö2{%äñS.@	E€P7×.	.;œ								
1A20	h: A	0 2E	B0	29	AC	A6	B1	AD	38	00	A 3	62	CF	8C	69	6D	.°)¬¦±-8	.£bÏC	Eim								
1A30	h: C	B 15	9F	6F	6C	A0	86	25	6E	12	70	EΒ	BC	69	6B	41	Ë.Ÿol †%n	ı.pë¼i	ikA								
1A40	h: 2	3 E4	67	D4	FF	D9	20	20	20	20	66	31	40	67	7B	65	#ägÔ <mark>ÿÙ</mark>	f1@ያ	g{e								
1A50	h: 5	4 42	31	49	45	46	79	5A	53	42	68	49	47	68	41	59	TB1IEFyZS	BhIG	hΑΥ								
1A60	h: 3	2 74	6C	63	69	45	3D	7D	20	20	20	20	20	0D	0A	20	2tlciE=}										
1A70	h: 1	A																									
																				http:	sr//bit	00.0	odo	not	100	225	07055
Tem	plate	Resu	ılts -	- JPC	5.bt	C														nups	5.//DI	og.c	sun	.net	'qq_	220	97955

使用010 editor查看图像3.jpg,文件末尾找到flag线索。

04—base64在线解码

← → C ▲ 不安全 ctf.ssleye.com/base64.html	
🏥 应用 🎐 翻译 🃸 百度一下, 你就知道 🧧 学习资料	
€ 在线工具 SSL在线工具 SSL漏洞在线检测 工具网 买证书	
— base编码 base16、base32、base64 eTB1IEFyZSBhIGhAY2tlciE=	
编码 base64 字符集 utf8(unicode编码) 编码	▼ 码
yOu Are a h@cker!	

尝试输入flag,发现错误,对其进行base64解码,得到正确flag。