Bugku-Misc-Wp



CAPTURE THE FLAG CTF 专栏收录该内容

3 篇文章 0 订阅 订阅专栏

Bugku-Misc-Writeup CTF小白 刷完为止

1.签到题 2.这是一张单纯的图片 3.隐写 4.telnet 5.眼见非实(ISCCCTF) 6.啊哒 7.又一张图片,还单纯吗 8.猜 9.宽带信息泄露 10.隐写2 11.多种方法解决 12.闪的好快 13.come_game 14.白哥的鸽子 15.linux 16.隐写3 17.做个游戏(08067CTF) 18.想蹭网先解开密码 19.linux2 20.账号被盗了 21.细心的大象 22.爆照(08067CTF) 23.猫片(安恒)

1.签到题

关注公众号即可获得flag flag{BugKu-Sec-pwn!}

2.这是一张单纯的图片

下载图片后直接用记事本打开

警 ETX = X95RSXE53SD 槜 愍crSOHWGSdACKX8A(ETX 楔 NUL(NUL (NULXEE & #107; & #101; & #121; & #123; & #121; & #121; & #111; & #117; & #32; & #97; & #114; & #101; & #32; & #114; & #105; & #103; & #104; & #116; & #125; 儋

可以看到有一串编码 不知道是什么编码直接丢进解码器 得到flag

结果:

key{you are right}

3.隐写

又是一张图片 这题百度了很久 找到一个比较细自己能理解的答案 用winhex打开图片

2.png																						
Offs	set	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		AN	SI	ASCII	~
00000	0000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG			IHDR	
00000	0016	00	00	01	F4	00	00	01	A4	08	06	00	00	00	СВ	D6	\mathbf{DF}	ô	101		ËÖß	
00000	0032	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	š	рНҮ	s	t	
00000	0048	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68	t Þf	х	Mi	CCPPh	
00000	0064	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otosł	nop	ICC	prof	
00000	0800	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	\mathbf{DF}	ile	хÚ	SwX	"÷ >₿	

八个字节89 50 4E 47 0D 0A 1A 0A为png的文件头
四个字节00 00 0D 代表数据块的长度为13
四个字节49 48 44 52 (即为ASCI码的IHDR)是文件头数据块的标示(IDCH)
13位数据块(IHDR)
前四个字节代表该图片的宽 00 00 01 F4
后四个字节代表该图片的高 00 00 01 A4

把高度改成和宽度一样保存 这步我没整明白 get新技能

BUGKU{a1e5aSA}

得到flag

4.telnet

下载文件后得到一个pcap格式的文件 没见过--百度得知pcap是wireshark的用于网络分析一个程序创建的数据文件也就是一个 流量包文件 那我们就放到wireshark走一遍

因为提示的是telnet 所以使用规则过滤显示telnet的包,然后右键追踪tcp流 得到flag

		networking.pcap				
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y)	无线(W) 工具(<u>T)</u> 帮助(<u>H</u>)				
📶 🔲 慮 🕲 🛓 🚞 🔉 🙆 🔍 < + A + + +		a o 🔛				
telnet						
No. Time Source Destination	Protoc ~	Length Info				
4 0.078000 192.168.221.128 192.168.221.164	TELNET	标记/取消标记 分组(M)	Ctrl+M			
6 4.508408 192.168.221.164 192.168.221.128	TELNET		Currin			
7 4.555208 192.168.221.128 192.168.221.164	TELNET	忽略/取消忽略 分组(l)	Ctrl+D			
8 4.570808 192.168.221.164 192.168.221.128 9 4 649909 192.169.221.129 192.168.221.164	TELNET	设置/取消设置 时间参考	Ctrl+T			
10 4.648808 192.168.221.126 192.168.221.104	TELNET	时间平移	Ctrl+Shift+T			
11 4.726808 192.168.221.128 192.168.221.164	TELNET	公约计算	Ctrl+ Alt+C			
12 4.758008 192.168.221.128 192.168.221.164	TELNET	万组注样	Ctri+Ait+C			
13 4.789208 192.168.221.128 192.168.221.164	TELNET	伯提留托的夕和				
15 4.836008 192.168.221.164 192.168.221.128	TELNET	\$局 7耳 用牛们T 口 \ 10 个小				
Window size value: 256		作为讨滤器应用				
[Calculated window size: 65536]						
[Window size scaling factor: 256]		准备过滤器				
Checksum: 0x3cao [Unverified]		对话过滤器				
Urgent pointer: 0		对话着色				
[SEQ/ACK analysis]		SCTD				
<pre>[Timestamps]</pre>		Je the second se				
TCP payload (21 bytes)		追踪流	>	TCP 流	Ctrl+Alt+Shift+T	
Telnet				UDP 流	Ctrl+Alt+Shift+U	
Will Negotlate About Window Size		夏利		TLS 流	Ctrl+Alt+Shift+S	
0000 00 0c 29 26 7e 0e 00 0c 29 84 86 5f 08 00 45 00 ···))&~··_·	45.20关注15			Ctrl+Alt+Shift+H	
0010 00 3d 07 9a 40 00 80 06 00 00 c0 a8 dd 80 c0 a8		砂以目达坝			CuttAutShiltti	
0030 01 00 3c a6 00 00 ff fb 1f ff fb 20 ff fb 18 ff	< <u></u>	解码为(<u>A</u>)				
0040 fb 27 ff fd 01 ff fb 03 ff fd 03		在新窗口显示分组(W)			https://blog.csdn.net/m0	46108436

hockeyinjune-virtual-machine login: <mark>ccssa</mark>aww

Password: flag{d316759c281bf925d600be698a4973d5}

得到flag

5.眼见非实(ISCCCTF)

, XFC?PKSOHSTXICC4NULDC4NULNULNULBSNULSUBX80區\茕XDAEOT(NULNULXAC6NULNUL 78 NULNULNULNULNULNULNULNUL NULNULNULNULNULNULNULNULNUL NULNULNULNULNULNULNULRUL 非实.docxpKENOACKNULNULNULSOHNULSOHNUL; NULNULNUL/(NULNULNUL NUL

我们加个后缀名.zip试试发现一个如上的文件但还是打不开用winhex打开试试

		_			_											•			
	眼见非实.docx																		
٦	Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII	~
	00000000	50	4B	03	04	0A	00	00	00	00	00	E2	20	0F	49	00	00	PK â I	
	00000016	00	00	00	00	00	00	00	00	00	00	09	00	16	00	D1	DB	ÑÛ	
	00000032	BC	\mathbf{FB}	в7	C7	CA	в5	2F	75	70	12	00	01	19	91	Α4	C1	¼û·Çʵ/up '¤Á	
	00000048	E7	9C	BC	E8	Α7	81	Ε9	9D	9E	E5	AE	9E	2F	50	4B	03	çœ∻è§ é žå®ž/PK	
	00000064	0.4	0.7	00	00	00	00	00	~ 1	0.0	0.77	4.0	00	00	0.0	00	00	4 -	

查阅文件了解了一下发现50 4B 03 04其实是压缩文件的头改后缀名.zip 打开最后在word->document.xml中得到flag

t>flag{F1@g}<,

IN / harm > / hare

6.啊哒

下载后看到是一张表情包 我们先右键看看图片信息 文件大的有点不正常

大小: 213 KB (218,957 字节)

占用空间: 216 KB (221,184 字节)

这里我们看到照相机型号有一串十六进制 先放着

照相机	
照相机制造商	
照相机型号	73646E6973635F32303138

改后缀名为rar打开发现有一个flag.txt

文件加密了 将上面得到的数字进行解密

73646E6973635	F32303138	
16进制转字符	字符转16进制	
sdnisc_2018		



密码正确 得到flag

7.又一张图片,还单纯吗

查看图片信息和上一题图片差不多大没获得有效信息改后缀名无果 丢进kali用binwalk试试 用binwalk命令可以看到里面有两张图片

root@kali:~	/桌面# binwalk 2	.jpg	
DECIMAL	HEXADECIMAL	DESCRIPTION	
 0 12 image direc	0×0 0×C torv: 8	JPEG image data, EXIF standard TIFF image data, big-endian, offset of first	jpg-文件 文件(F) 编辑(E) 视图(V) 转到(G) 帮助(H)
158792 158822	0×26C48	JPEG image data, JFIF standard 1.02	← → 个 龠 ■ /root/桌面/output/jpg/
image direc 159124 162196 168370 -Packard Co	tory: 8 0×26D94 0×27994 0×291B2 mpany"	JPEG image data, JFIF standard 1.02 JPEG image data, JFIF standard 1.02 JPEG image data, JFIF standard 1.02 Copyright string: "Copyright (c) 1998 Hewlett	设备 ○ 文件系统 ⑥ Kali Live
root@kali:~ Processing: * root@kali:~	/桌面# foremost : 2.jpg /桌面#	2.jpg	位置 root https://blog.csdn.net/m0_46108436

使用foremost命令分离 打开桌面上output文件夹在图片中得到flag

falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

附一个binwalk使用方法 https://www.cnblogs.com/xishaonian/p/7633038.html

8.猜

flag{liuyifei}

Submit

无脑题目 百度识图后得到刘亦菲名字全拼

9.宽带信息泄露

下载得到一个bin文件用记事本打开会乱码那么就用专业工具RouterPassView打开题目提示宽带用户名那我们搜一下username

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

关键字 果然 得到flag

10.隐写2

root@kali:~/#	🌆 # binwalk -e	1.jpg
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0×0	JPEG image data, JFIF standard 1.01
30	0×1E	TIFF image data, big-endian, offset of first
image directo	rv: 8	
52516	0×CD24	Zip archive data, at least v1.0 to extract, c
ompressed siz	e: 6732, uncompr	essed size: 6732, name: flag.rar
59264	0×E780	End of Zip archive, footer length: 22
147852	0×2418C	End of Zip archivettp \$99900 . Leagthet/AD_46108436

分离后得到一张图片 提示我们密码是三位数 以及一个加密的rar包

口令已成功恢复!		×
Advanced Arch	iive Password Recovery 统计信息;	:
总计口令	971	
总计时间	26ms	
平均速度(口令/秒)	37,346	
这个文件的口令	871	<u>6</u>
十六进制口令	38 37 31	G
	 https://blog. 父 .确定,	i/m0_46108436

直接使用ARCHPR暴力破解得到密码871

#äqÔÿÙ f10g{e TB1IEFyZSBhIGhAY 2tlciE=}

卧槽又得到一张图片3.jpg 老样子丢进winhex 拉到最后发现base64加密的flag

解密得到f1@g{y0u Are a h@cker!}

没仔细看的时候把1打成了一直通不过东问西文发现是自己打错了还是要细心啊

11.多种方法解决

得到一个exe直接丢进winhex 得到一串base64 用工具转成图片



*请上传小于300KB的.jpg/.jpeg/.gif/.bmp/.png/.ico格式图片,不建议将大图转换。

ogBase64还原图片08 3清

利用QRCode工具得到flag

12.闪的好快

可以看到一张如题所述闪的很快的gif图 这里肯定是采用Stegsolve神器一帧帧分析



一共18帧 一帧帧解码 得到结果是SYC{F1aSh-so-f4sT}但是不正确 查了一下把-替换成_即可

13.come_game

本题是一个游戏



一开始在这界面摸了好久--后来发现按shift可以进入玩了一把之后发现文件夹里多出一个文件

DeathTime	2020/1/30 20:29	文件	1 KB
joker's.exe	2016/10/9 23:45	应用程序	8,106 KB
save1	2020/1/30 20:29	文件	1 KB

直接用winhex打开

save1																				
Offset	0	1	2	3	4 5	6	7	8	9	10	11	12	13	14	15			ANSI	I ASCII	
00000000	00	01	32	00 0	0 41	00	05	43	00	00	00	00	00	00	00	2	А	С		
00000016	00	00	00	00 0	0 00	00	00	00	00	00	00	00								

发现把2改成5再进入游戏读取存档就好了

joke	er's I wanna	a Medium	SaveDa	ta1 [Esc]	end Deat:	h[1]:8 Tim	e[1]:0:0:	18	
뒤		FFFF	rrrr	FFFF	FFFF		FFFF	FFFF	
ĘĻ									一支
ĘĹ									- <u>5</u> -
<u>ل</u> م			(100)						국무
<u>-</u>			P	L	A	G			ŢŢ
<u>-</u>						-			<u>1</u>
	6	Ξ	2	3	F	2	5	.9	2
									국문
<u>5</u>	D	9	8	D	F	1	5	3	
ĘĻ		Trender							ŢŢ
ξĻ									<u>1</u>
ĘĽ									
									국문
کے									
<u>j</u> -r							C		
-						nttps://blc	g.csan.n	avmu_461	08436

结果提交一直通不过 查了一下吧flag换成SYC就好了

14.白哥的鸽子

下载后改后缀名为jpg试试结果真是只鸽子



丢进winhex看一看

П	00012230	щU	05	n,	20	1 7	± ±	тυ	12	00	20	20	UE.	лэ	цυ	чv	20	α 3 λ⊓ (∓ 6
	00012272	78	DC	59	69	DA	8F	64	6E	E6	7B	A3	57	31	EE	8D	DC	xÜYİÚ dnæ{£Wlî Ü
	00012288	СВ	62	45	62	89	EE	5B	DC	в6	73	01	E3	FF	D9	66	67	ËbEb‰î[ܶs ãÿÙfg
	00012304	32	69	76	79	6F	7D	6C	7в	32	73	33	5F	6F	40	61	77	2ivyo}l{2s3 o@aw
	00012320	5F	5F	72	63	6C	40											rcl@

fgl这些敏感字符都有 根据经验是栅栏密码没错了

结果:	
得到因数(排除1和字符串长度):	
2 3 4 6 8 12	
# 1 b 52 - 122 1 - 1 [- 0 0	
弗1柱: f2vol23oa_rlgiy}{s_@w_c@	
第2栏: fio{3@_cgv}2_a_l2ylsowr@	
第3栏·fyl3argy{wc2o2o_li}s@ @	
4 4 4 4 6 0 1 01 : [0 0 1 0	
弗4柱: fo3_g}Zlori{@cv2alysw@	
第5栏: flag{w22_is_v3ry_cool}@@	
第6栏·f3g 20j@yaywo } lr{c2ls@	
1,001=. 108_2010/04/#0_J_11 [02138	

解密解一下就出来了 flag{w22_is_v3ry_cool}

15.linux

这题下过来的文件是.tar.gz本以为需要用linux命令进行解压结果直接打开了

🦻 📜 C:\Users\Jin\[ownloads\1.ta	r.gz\1.tar\test	:\flag\				
名称	大小	压缩后大小	模式	修改时间	创		
📕 .Trash-0	56	1 024	drwx	2016-06-2			
Iost+found	0	0	drwx	2016-06-2			
[SYS]	1 048 576	1 053 696					
📄 flag.txt	38	1 024	-rw-rr	2016-06-2			
🧾 flag.txt - 记事本							
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)							
kov/feb81d383/	00123-000	3f475546/	1060h1				

key{feb81d3834e2423c9903f4755464060b} https://blog.csdn.net/m0_46108436

16.隐写3

题目明确说了隐写打开发现是只有头的大白 高度有点不对劲 丢进winhex改一下



https://blog.csdn.net/m0_46108436

	L (💷 🥪 🗠	==			/ -			ei 010			HEX	··•▶B HE	×		WA 1			~ ~ ~	W	/	99e	06 55 - 1
	save1 jpg.jpg	dal	bai.p	ong																		
1	Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		Al	NSI ASCII	E 🔥	
	00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG		IHDE	R	
	00000016	00	00	02	Α7	00	00	01	00	08	06	00	00	00	6D	7C	71	S		m c	a 🛛	
	00000032	35	00	00	00	01	73	52	47	42	00	AE	CE	1C	Е9	00	00	5	sR	GB ®Î é		
1						-				-	-	-										

前面是文件头,固定的。从第二行开始,前四位是宽,后四位是高。吧00改成F0即可获得flag





17.做个游戏(08067CTF)

又是一个游戏 不得不说各位师傅真的鬼才





没遇到过jar包的misc 看了一下别人的wp发现要用gui反编译一下 ps: 现在才知道jar包原来可以反编译--这里方便大家直接提供工具 打开之后直接到Main类中找

```
MANIFEST.MF × PlaneGameFrame.class
Manifest-Version: 1.0
Class-Path: .
Main-Class: cn.bjsxt.plane.PlaneGameFrame
 if (!this.p.isLive())
  ł
   printInfo(g, "兄弟就死了的嘛", 50, 150, 200);
   int period = (int)((this.endTime.getTime() - this.startTime.getTime()) / 1000L);
   printInfo(g, "你的持久度才" + period + "秒", 50, 150, 250);
   switch (period / 10) {
   case 0:
     printInfo(g, "真.头顶一片青青草原", 50, 150, 300);
     break:
   case 1:
     printInfo(g, "这东西你也要抢着带? ", 50, 150, 300);
     break;
   case 2:
     printInfo(g, "如果梦想有颜色,那一定是原谅色", 40, 30, 300);
     break;
   case 3:
     printInfo(g, "哟, 炊事班长呀兄弟", 50, 150, 300);
     break;
   case 4:
     printInfo(g, "加油你就是下一个老王", 50, 150, 300);
     break;
   case 5:
     printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 30, 300);
     break:
   case 6:
     printInfo(g, "flag{RGFgaURhbGlfSmlud2FuQ2hpamk=}", 50, 150, 300);
     break;
   }
 }
}
```

base64解密后得到flag get新技能

18.想蹭网先解开密码

.cap的文件 没见过--又要看看别人的wp先了 得知需要用ewsa工具

附工具

手机号肯定为11位已经给出7位所以还差四位用python写个脚本跑一个字典出来



1.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

跑包的速度有点慢应该是软件下的不对--不过出来了就好



19.linux2

一个没有后缀名的文件 用winhex打开居然全是0

169169 Gapar	פייק		en	ienge																
Offset	0	1	2	3	4	- 5	6	7	8	9	10	11	12	13	14	15	ANSI	ASC	II	~
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000144	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				

用notepad打开搜flag无果题目给出key的提示搜key试试居然真的有--我记得第一次在杭电的比赛也是莫名其妙就搜出来了

110	
177	
178	
179	KEY{24f3627a86fc740a7f36ee2c7a1c124a}
180	NULNULNULNULNULNULNULNULNULNULNULNULNULN
181	
182	NULNULNULNULNULNULNULNULNULNULNULNULNULN
183	<u>DNULNULNULNULNULNULNULNULNULNULNULNULNULN</u>

20.账号被盗了

这题我估计是挂了

C ① 不安全 | 123.206.87.240:9001

노 🖏

404 Not Found

nginx

https://blog.csdn.net/m0_46108436

21.细心的大象

i.jpg

1 头部错误:1.jpg

发现无法解压并且文件大的异常 打开kali丢进binwalk试试

.

		_1.jpg.zip.extracte	ed - 文件管理器	_ = ×
文件(F) 编辑(E)	视图(V) 转到(G)	帮助(H)		
$\leftrightarrow \rightarrow \uparrow$	noot/_1.j	pg.zip.extracted/	1	C
设备				
읻 文件系统			root@kali:~	
💿 Kali Live	±		文件(E) 动作(A) 编辑(E) 查看(V) 帮助(H)	
位置	0.zıp	1.jpg	root@kali: ~ 🛛 🛛	
🛅 root			root@kali:~# ls	
桌面			1.jpg.zip 公共 模板 视频 图片 文档 rootakali:~# binwalk -e 1.jpg.zip	下载 音乐
阿 回收站)N
网络				
🔳 浏览网络			0 O×0 Zip archiv ompressed size: 6408284, uncompressed si 6408370 O×61C8B2 End of Zip	ve data, at le ze: 6408284, archive, foo
			root@kali:~#	
			https://blog.csdn.net/n	n0_46108436

得到一个压缩包 里面是一个大象的图片 估计就是从这里突破了 右键看看有没有提示

1.jpg 属t	生			
剱 安	全 详细信息 以前的版本			
属性	值	^		
说明 —		_		
标题	出题人已经跑路了			
主题	出题人已经跑路了			
$\begin{array}{ccc} & & & & & & \\ & & & & & & & \\ & & & & $				
标记				
备注	TVNEUzQ1NkFTRDEyM3p6			
来源一		_		
作者	Bugku			
拍摄日期	2017/8/10 11:53			
程序名称	sagit-user 7.1.1 NMF26X V8.2.26.0.NCAC			
获取日期	3			
版权				
图像一		_		
图像 ID				
分辨率	3016 x 4032			
宽度	3016 像素			
高度	4032 像素			
水平分辨	率 72 dpi			
垂直分辨	率 72 dpi			
位深度	24			
FT #=		~		

确定	取消 tos://org/selon	et/m0型目108436

TVNEUzQ1NkFTRDEyM3p6

解密先留着 后面应该会用到

图片依旧很大再次分离一下得到一个加密的压缩包 里面是张图片

_1.jpg.extracted - 文件管理器		_							
) 转到(G) 帮助(H)									
/root/_1.jpg.zip.extracted/_1.jpg.extract	ed/	C		root@ka					
			动作(<u>A</u>) 编	辑(<u>E)</u> 查看(
			ali: ~/zip.ex	ctracted 🗵					
	61	6188AF.rar - xarchiver 0.5.4.14							
6188AF.rar	归档文件(A) 动作(C) 帮助((H)							
	<u>↑</u>	R 🔹 💿							
	位置:								
	归档文件树:	文件名 Origina	al Size 压缩后	Occupancy					
		o 2.png 17675	16224	91%					
		https://blog	g.csdn.net/m0_	46108436					

把前面的base64解密后输入果然对了怪不得我字典爆破那么久都没结果--后来看了别人的wp发现一般需要爆破的都会给你提示的

将得到的图片丢进winhex改高度得到flag!





22.爆照(08067CTF)

得到一张穹妹的图片 右键无果 丢进binwalk分析一下

(` ` •)		98	E33.zip - xarchiver 0.5.4.14	
	归档文件(A) 动作(C) 帮助	b(H)		
· • • • • • • • • • • • • • • • • • • •	<u> <u> </u></u>	Ra 🔫	۲	
	位置:			
····)	归档文件树:	文件名		Origin
* /		8		92278
		🖹 88		15739
()		🛓 888		18479
÷ ۲		🛓 8888		11782
		🛓 88888		92278
c')		🛓 888888		92278
		🖹 8888888		92278
		🖹 8888888		92278
÷)		> \$ \$ \$ \$ \$ \$	-++ \$=\$+\$\$\$\$\$\$.gif	58893
$\overline{\cdot}$	9 个文件 (553.0 KB)		1个文件选中的(9	90.1 KB
۰, Y		http:	s://blog.csdn.net/m0_4610	8436

得到8张图片 第二张是带二维码的 扫了一下结果是bilibili 提交了一下发现不对--对每张图片都分析了一下 发现88 888 8888这三张里面是有东西的

nootakali/	所建立件本 / 9 ind	ovtwactod# hinwalk _0_888
	m 是又许天/_o.jpg	.extracted# Dinwatk -e 000
DECIMAL	HEXADECIMAL	DESCRIPTION
	`/root/∦	f建文件夹/_8.jpg.extracted/
0	0×0	JPEG image data, JFIF standard 1.01
30	0×1E	TIFF image data, big-endian, offset of first
image directo	ory: 8	
root@kali:~/	新建文件夹/_8.jpg	.extracted# binwalk -e 88
DECIMAL	HEXADECIMAL	DESCRIPTION 8 9E33.20 88
DECIMAL	HEXADECIMAL	DESCRIPTION
DECIMAL 0	HEXADECIMAL	JPEG image data, JFIF standard 1.01
DECIMAL 0 30	HEXADECIMAL 0×0 0×1E	DESCRIPTION JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first
DECIMAL 0 30 image directo	HEXADECIMAL 0×0 0×1E Dry: 8	DESCRIPTION JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first
DECIMAL 0 30 image directo root@kali:~/	HEXADECIMAL 0×0 0×1E ory: 8 新建文件夹/_8.jpg	DESCRIPTION JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first c.extracted# binwalk -e 8888

0	0×0	SSSS JPEG image data, JFIF standard 1.01
30	0×1E	TIFF image data, big-endian, offset of first
image dire	ectory: 8	
10976	0×2AE0	Zip archive data, at least v2.0 to extract, c
ompressed	size: 644,	uncompressed size: 1202, name: 1509126368,png.dn not/m0_46109436
11760	0×2DF0	End of Zip archive, footer length: 22

88已经用过了对888进行分离无果对8888进行分离得到一个二维码 扫出来后得到panama 对888图片右键查看发现base64 解密

🛋 888.j	pg 属性								
常规	安全	详细信息	以前的版本						
属性	3	值							
标题	3								
主题 分级		* * * * * *							
标记		c2lsaXNp	bGk=						
来源	<u> </u>	https://	/blog.csdn.net/m0_46108436						

得到silisili

所以按照顺序应该是flag{bilibilisilisilipanama} 结果错了发现有提示改成flag{bilibili_silisili_panama}就好了

23.猫片(安恒)

看到题目我就感觉我做不了 提示给的 LSB BGR NTFS 只知道NTFS是和硬盘有关 得到一个无后缀的文件 直接丢进winhex 发现头是png 改后缀名





得到猫片--右键无果 丢binwalk无果 回去看了看提示发现之前好像看过一个叫LSB隐写的东西 故去百度了一下用神器StegSolve 分析了一波无果--看大神的wp去了

Extract Preview fffe8950 #e470d0a 1a0a000000d4948 PNG IH 445200001180000 008c08020000008 DR IDATxQ colspan="2">colspan="2"colspan	\times
fffe89504e470d0a 1a0a0000000d4948 PNG. IH 4452000001180000 008c080200000008 DR IDATxQ c7edb0000059c49 44154789ceddd51 IDATxQ 6alc3b1440c13864 ff5b761610145038 j.;.0.8d.[vP8 3792ecaadf37afdd eef141908bd43f7e 7	
1012047eedfe0fd3 739b95dd39c3f4dc ~ s9 Bit Planes Order settings Alpha 7 6 5 4 3 2 1 0 Red 7 6 5 4 3 2 1 0 Bit Order \bigcirc MSB First LSB First Green 7 6 5 4 3 2 1 0 Bit Plane Order Bit Plane Order Bit Plane Order 1 1 1 1	
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	
Green ☐ 7 ☐ 6 ☐ 5 ☐ 4 ☐ 3 ☐ 2 ☐ 1 🗹 0 Bit Plane Order	t
Preview Settings Include Hex Dump In Preview 🖌	

像这样选中后单击Preview保存为1.jpg

结果发现打不开用winhex打开后更改头部 删掉前两位即可

set	U (L	2	3	4	5	6	1	8	9	τu	$\perp \perp$	12	13	⊥4	15	ANSI	ASCII
0000	FF	FE	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	ÿþ%PNG	IH
			~ ~	~ ~		4.6	0.0	~ ~	0.0		~ ~	~ ~	0.0	~ ~	~ ~	~ ~		

得到半张二维码于是就要接着去改图片的高宽,我打开图片的属性可以发现高度为140像素,需要改为280,而winhex里面都是以16进制的方式来显示的,所以应该是找到8C(140)把它改成118(280)

	0	1	2	3	4	5	6	7	8	9	A	B	Ç	D	E	F	0123456789ABCDEF
00h:	89	50	15	17	0D	A0	1A	A 0	00	00	00	0D	49	48	44	52	%PNGIHDF
10h:	00	00	01	18	00	00	01	18	08	02	00	00	00	08	EC	7E	ìr
20h ·	DB	00	00	05	9C	49	44	41	54	78	90	ED	DD	51	6A	1C	ÛœTDATxœíÝOi.

- UII.		~~	~~						- ·								
30h:	3B	14	40	C1	38	64	FF	5B	76	16	10	14	50	38	37	92	;.@Á8dÿ[vP87'
40h:	EC	AA	DF	37	AF	DD	EE	F1	41	90	8B	D4	3F	7E	00	00	ìª₿7 ÝîñA.∢Ô?~
50h:	00	00	00	00	C0	9F	3E	56	FF	E1	F3	F3	F3	7F	DE	C7	ÀŸ>Vÿáóóó.ÞÇ
60h:	3F	FB	F8	58	FE	A0	89	D5	73	D8	FD	B9	D3	D7	59	A9	?ûøXþ.‰ÕsØý¹Ó×Y@
70h:	9E	CF	EE	FD	57	9F	BF	CD	EA	FE	7F	FE	E7	FB	80	2F	žÏîýWŸ;ĺêþ.þçû€/
80h:	49	48	10	10	12	04	84	04	01	21	41	40	48	10	10	12	IH,!A@H
90h:	04	7E	ED	FE	0F	D3	73	9B	95	DD	39	C3	F4	DC	63	FA	.∼íþ.Ós>•Ý9ÃôÜcứ
A0h:	E7	AE	9C	9A	5F	4D	7F	7E	FA	3A	BB	76	BF	17	2B	12	箜š_M.∼ú:»V;.+.
B0h:	04	84	04	01	21	41	40	48	10	10	12	04	84	04	01	21	
COh.	41	60	7B	8E	B4	52	ED	27	39	35	37	58	99	9E	F3	4C	A`{Ž'R1'957X™žóI

得到完整的二维码后扫出来结果是个百度云地址结果--

名称	大小	压缩后大小	修改时间	创建时间	访问时间
📄 flag.txt	63	63	2017-12-0		
🧾 flag.txt - 记事本					
文件(F) 编辑(E) 格	式(O) 查看(V)	帮助(H)			
flag不在这里哦	你猜猜flag在	哪里呢?	找找看吧		

最后还是靠着大佬的wp