CTF平台题库writeup(三)--BugKuCTF-杂项(1-20题详 解)



Hacking黑白红 于 2020-06-29 09:36:17 发布 4226 收藏 18 分类专栏: <u>CTF 信息安全 bugku</u> 文章标签: <u>安全 信息安全</u> 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/zsw15841822890/article/details/107013549</u> 版权



<u>CTF 同时被 3 个专栏收录</u> 15 篇文章 6 订阅



<u>信息安全</u> 39 篇文章 8 订阅 订阅专栏



7篇文章2订阅 订阅专栏

一、BugKuCTF-杂项(1-20)

眼见非实(ISCCCTF)	啊哒	又一张图片,还单纯吗	猜
50	50	60	60
宽带信息泄露	隐写2	多种方法 解决	闪的好快
60	60	60	60
come_game	白哥的鸽子	linux	隐写3
60	60	80	80
做个游戏(08067CTF)	想讚网先解开蜜码	Linux2	账号被盗了
80	100	100	100
细心的大象	爆 照(08067CTF)	猫片(安恒)	多彩
100	100	100	100
旋转跳跃 100	普通的二维码 100	乌云邀请码 100 http://	神秘的文件 100 /blog.csdn.net/zsw15841822890

扫描二维码直接获取flag

2、这是一张单纯的图片

http://120.24.86.145:8002/misc/1.jpg



(1).启蒙级隐写术

linux下保存到本地当作文本文件cat一下(或记事本、winhex等打开)

cat 1.jpg

(2).在末尾发现

key{you are righ

unicode解码得到flag

利用网页上搜索的unicode转ascii进行转换即得FLAG! (工具可以用小葵花)

key{you are right}

```
key{you are r&#105
;ght}
ASCII 转换 Unicode I Unicode 转换 ASCII 夏利 清空结果
```

key{you are right}

3、隐写(文件头)

Linux下提示

Bu

下载2.rar,解压得到一张图片,首先放在winhex里看看

	-	a ve	-	1			-	-	-	-60 08	v			PIE2	10	HEA		~ ~ ~ ~
2.png	CTF	.png																
Offs	et	0	1	2	3	4	5	6	7	8	9	A	В	С	D	Ε	F	^
00000	000	89	50	4E	47	OD	0A	1A	0A	00	00	00	OD	49	48	44	52	\$FNG IHER
00000	010	00	00	01	F4	00	00	01	<u>a</u> 4	08	06	00	00	00	CB	D6	DF	ć 🛥 ĖČß
00000	020	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	3 pHYs t
00000	030	74	01	DE	66	1F	78	00	00	OA	4D	69	43	43	50	50	68	t Ff x kiCCFFh
00000	040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	ctcshcp ICC prof
00000	050	69	60	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile xÚ SwX"÷ >ß
00000	060	F7	65	OF	56	42	DS	FO	B1	97	6C	81	00	22	23	AC	08	÷e VE£¢±−1 "#-
00000	070	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	OA	È Y¢ ' a, GA_ '
00000	080	56	14	15	11	90	48	55	C4	82	D5	0A	48	9D	88	E2	AO	ν αHUĂ,Ĉ H ^á
00000	090	28	B8	67	41	8A	88	5A	8B	55	5C	38	EE	1F	DC	A7	B5	(.gAŠ^2 <u\si td="" usp<=""></u\si>
00000	OAO	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	FC	CE	79	CF	}zĭíi0×0≒çaçüÍyÏ
00000	ово	OF	80	11	12	26	91	E6	A2	6A	00	39	52	85	зс	3A	DS	€ & 'a¢j SR<:Ø
00000	000	1F	8F	4F	48	C4	C9	BD	80	02	15	48	E0	04	20	10	E6	CHĂÉ≒€ Hả æ
00000	ODO	CB	C2	67	05	C5	00	00	FO	03	79	78	7E	74	BO	3F	FC	ÉÂG Å č yx~t°?ü
00000	OEO	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	FF	83	BA	°c p€.\$ Çáyf°
00000	OFO	50	26	57	00	20	91	00	EO	22	12	E7	0B	01	90	52	00	FSW 'd'Ç R
00000	100	C8	2E	54	C8	14	00	C8	18	00	BO	53	BS	64	OA	00	94	É.IÉ. É 505 42 70 200
00000	110	00	00	6C	79	70	42	22	00	AA	OD	00	EC	F4	49	3E	05	ly E" * idI>

89 50 4E 47PE头是png照片的,就是说没有可能照片中嵌入了Exif信息

在查看PNG文件格式时,IHDR后面的八个字节就是宽高的值

IHDR

文件头数据块IHDR(header chunk):它包含有PNG文件中存储的图像数据的基本信息,并要作为第一个数据块出现在P NG数据流中,而且一个PNG数据流中只能有一个文件头数据块。

文件头数据块由13字节组成,它的格式如下表所示。

域的名称	字节数	说即
Width	4 bytes	图像宽度,以像素为单位
Height	4 bytes	图像高度,以像素为单位
Bit depth	1 byte	图像深度: 索引彩色图像: 1, 2, 4或8 灰度图像: 1, 2, 4, 8或16 真彩色图像: 8或16
ColorType	1 byte	該色类型: 0: 灰度图像, 1, 2, 4, 8或16 2: 真彩色图像, 8或16 3: 索引彩色图像, 1, 2, 4或8 4: 带动通道数据的灰度图像, 8或16 6: 带动通道数据的真彩色图像, 8或16
Compression method	1 byte	压缩方法(LZ77派生算法)
Filter method	1 byte	建波器方法
Interlace method	1 byte	隔行扫描方法: 0:非隔行扫描 1: Adam7(由Adam M. Costello开发的7遍隔行扫描方法)

将图片放在Linux下,发现是打不开的,说明图片被截了



将图片的高改成和宽一样,即将A4改成F4,然后另存为

2.png																	
Offset	0	1	2	3	4	5	6	7	8	9	А	В	С	D	Е	F	~
00000000	89	50	4E	47	0D	0A	1A	0A	,00	00	00	0D	49	48	44	52	%FNG IHER
00000010	00	00	01	F4	00	00	01	F4	08	06	00	00	00	СВ	D6	DF	ĉ ĉ ĖČB
00000020	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	Š pHYs t
00000030	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	<u>50</u>	68	t Ff x MiCCFFh
00000040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	ctcshop ICC prof
00000050	69	6C	65	00	00	78	DA	9D	53	77	<u>58</u>	93	F7	16	3E	DF	ile xÚ SwX"÷ >ß
00000060	F 7	65	0F	56	42	D8	FO	B1	97	6C	81	00	22	23	AC	08	÷e VE26±−1 ″#−
00000070	C8	10	59	A2	10	92	00	61	84	10	12	40	С5	85	88	0A	È ұ¢′а" @Å…^
00000080	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88	Е2	A0	dVine@HUÄ, 65H41822890
nnnnnan	28	R8	67	41	яz	88	54	8R	55	50	38	EE	1 F	DC	Δ7	R5	/ อุธิรักยุ/กุ/สรี ที่จะก

Bugku

打开刚存的图片就可以得到FLAG了



https://blog.csdn.net/zsw15841822890

BUGKU{a1e5aSA}

4.telnet

将1.zip下载解压得到一个流量包文件,放到Wireshark中走一遍,因为提示的是telnet,所以使用规则显示telnet的包,然后追踪tcp流

	🚺 networking.pcap								_		×
3	★(F) 编辑(E) 视图(V)	跳转(G) 捕获(C) 分析(<u>A)</u> 统计(<u>S</u>)电	话(Y) 无线(W)	工具(T)	帮助(<u>H</u>)					
	[🔳 🧟 💿 📙 🛅 🗙	🔓 🭳 🗢 🗢 😤 👔	🕹 📃 🔳 🔍	୍ ର୍ 🔍 🎹							
C	telnet	过滤						X		表达式…	+
N). Time	Source	Destinati	on	I	Protocol	Length Info				^
	4 0.078000	100 160 001 100	102 165	2.221.164	٦	TELNET	75 Telnet Data	a			
	6 4.50840	你吃/蚁洞你吃 万狙(Ⅲ)	Ctri+IVI	.221.128	1	TELNET	66 Telnet Data	a 🔪 .			
	7 4.55520	忽略/取消忽略 分组(1)	Ctrl+D	.221.164	1	TELNET	57 Telnet Data	a			
	8 4.57080	设置/取消设置 时间参考	Ctrl+T	.221.128	1	TELNET	66 Telnet Data	a 🔪			
	9 4.64880	时间平移	Ctrl+Shift+T	.221.164	1	TELNET	63 Telnet Data	a			
	10 4.64880	分组注释	Ctrl+Alt+C	.221.128	1	TELNET	72 Telnet Data	a			
	11 4.72680			.221.164	1	TELNET	71 Telnet Data	a			
	12 4.75800	编辑解析的名称		.221.164	1	TELNET	60 Telnet Data	a		点击右	键
	13 4.78920	作为过滤器应用	•	.221.164	1	TELNET	65 Telnet Data	a			
	15 4.83600	准备讨法器	•	.221.128	1	TELNET	63 Telnet Data	a			
	16 4.89840	24年1月1月1日	•	.221.164	1	TELNET	57 Telnet Data	a			
	17 4.92960		,	.221.164	1	TELNET	57 Telnet Data	a			
	18 4.96080	刘话看巴		.221.164	٦	TELNET	57 Telnet Data	a			
	20 4.99200	SCTP	•	.221.128	٦	TELNET	74 Telnet Data	a			
	22 5.02320	追踪流		.221.128	٦	TELNET	90 Telnet Data	a			
	24 16.1148	复制	追踪TCP流	.221.164	٦	TELNET	55 Telnet Data	a			
	25 16.1304	22.00		.221.128	1	TELNET	60 Telnet Data	a			
	27 16.4112	协议首选项	•	.221.164	٦	TELNET	55 Telnet Data	a			
	28 16.4112	解码为(<u>A</u>)		.221.128	٦	TELNET	60 Telnet Data	a			
	30 16.5048	在新窗口显示分组(<u>W</u>)		.221.164	1	TELNET	55 Telnet Data	a			
	31 16.504829	192.168.221.164	192.168	3.221.128	1	TELNET	60 Telnet Data	a			
	33 16.785629	192.168.221.128	192.168	3.221.164	1	TELNET	55 Telnet Data	a			
Ц	24.46.004220	400 400 004 404	402.400			TELNET					~
>	Frame 4: 75 bytes	on wire (600 bits)	, 75 bytes ca	aptured (600	bits)						^
>	Ethernet II, Src:	Vmware_84:86:5f (00	0:0c:29:84:8	6:5f), Dst: \	Vmware_2	26:7e:0e	e (00:0c:29:26:7e:	0e)			
>	Internet Protocol	Version 4, Src: 192	2.168.221.12	B, Dst: 192.1	168.221.	164					
>	Transmission Contr	rol Protocol, Src Po	ort: 1146, D	st Port: 23,	Seq: 1,	Ack: 1	l, Len: 21				
	Telnet										×
6	000 00 0c 29 26 7	e 0e 00 0c 29 84 80	5 5f 08 00 4	5 00 · ·)&~	···)··_	E-	https://blog.o	ada not	1	20620	2.4.0
(🕽 🍸 networking. pcap						分组: 59 · 已显示: 3	86 (61.0%)	Profi	le: Defa	ilt

在tcp流中就能直接看到flag,在telnet协议下任意数据流都能看到flag

```
Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · networking.pcap
Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · networking.pcap
....*P.....'.
38400, 38400...'....XTERM.....!Ubuntu 12.04.2 LTS
hockeyinjune-virtual-machine login: ccssaaww
Password: flag{d316759c281bf925d600be698a4973d5}
Login incorrect
hockeyinjune-virtual-machine login: .
...*C
```

5、眼见非实(ISCCCTF)

下载下来是一个文件的格式,放到winhex中,发现有50 4B 03 04这是压缩文件的头,还有.docx格式文件,应该压缩包里有一个文档,改文件后缀为.zip,解压得到文档

2.png zip	(眼	见非	实(ISC	CCT	F))	E	即	非实	do	cx							
Offset	0	1	2	3	-	5	6	7	8	9	A	В	С	D	Е	F		^
00000000	50	4B	03	04	1	00	00	00	08	00	1A	80	87	49	5C	DC	ER €≠I\Ü	
00000010	54	28	04	28	00	00	AC	36	00	00	OD	00	00	00	D1	DB	ăÚ (−6 ÑÛ	
00000020	BC	FB	B7	C7	CA	B5	2E	64	6F	63	78	9D	7A	05	40	15	4û-Çiu.dccx / Ø	
00000030	DB	F7	F5	25	25	25	25	A5	BB	A4	BB	A5	BB	BB	BB	E1	Ú÷28888€±×=×¥×××á	
00000040	22	1D	92	D2	8A	74	09	48	77	4A	77	77	87	74	8A	80	" 'ČŠt HwJww‡tŠ€	
00000050	34	D2	82	CO	87	BE	E7	7B	80	FA	7E	FE	BF	CB	B9	77	4C, À #4¢ (€ú~þ¿É'w	
00000060	CF	65	CE	90	B3	EE	DA	7B	CF	90	3D	B3	64	25	CO	CO	leía'iÚ{la='d\$ÀÀ	
00000070	61	00	DF	5E	1F	FO	11	C4	00	B7	5E	DO	00	34	CO	C8	a ß^ ĉ Ä ·^E 4ÀÈ	
00000080	6C	FD	45	55	57	6F	05	AD	03	10	19	00	82	19	9E	D1	lýEUWc - , žÑ	
00000090	B2	9E	58	FF	29	DB	7B	23	29	79	B5	28	99	56	F6	9F	=2Xý)Ú(≇)yµ(₽VċŸ	
000000A0	83	5B	EE	1D	80	02	co	FF	F7	60	03	07	3B	7B	1.B	2B	fli @ Ag+ : : +	
000000B0	55	2B	СВ	9B	61	1E	03	40	9E	CF	78	17	DF	19	E6	DF	0+É>a gžíx B aB	

得到眼见非实.docx是打不开的,放到winhex中发现还是zip格式的文件

zip 眼见非	实.d	ocx																
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	ANSI ASCII	^
00000000	50	4B	03	04	0A	00	00	00	00	00	E2	20	0F	49	00	00	PK & I	
00000010	00	00	00	00	00	00	00	00	00	00	09	00	16	00	Dl	DB	ÑÛ	
00000020	BC	FB	B7	C7	CA	B5	2F	75	70	12	00	01	19	91	A4	Cl	4û Çʵ/up '¤Â	
00000030	E7	90	BC	E8	A7	81	E9	9D	9E	E5	AE	9E	2F	50	4B	03	çœuès é žásž/PK	
00000040	04	0A	00	00	00	00	00	C1	20	OF	49	00	00	00	00	00	ÁI	
00000050	00	00	00	00	00	00	00	13	00	20	00	Dl	DB	BC	FB	B7	ÑÛ4û ·	
00000060	C7	CA	B5	2F	63	75	73	74	6F	6D	58	6D	6C	2F	75	70	Çʵ/customXml/up	
00000070	10	00	01	7D	DA	81	AF	E7	90	BC	E8	A7	81	E9	9D	9E)Ú ⊂çœ4è§éž	
08000000	E5	AE	9E	2F	63	75	73	74	6F	6D	58	6D	6C	2F	50	4B	å&ž/customXml/PK	
00000090	03	04	14	00	00	00	08	00	00	00	21	00	35	65	18	58	! 5e X	
0A000000	9D	00	00	00	FE	00	00	00	10	00	29	00	Dl	DB	BC	FB	þ) ÑÛ4aù	
000000B0	B7	C7	CA	B 5	2F	63	75	73	74	6F	6D	58	€D	6C	2F	69	CÊu/custonXml/1	
00000000	74	65	6D	31	2E	78	6D	6C	75	70	25	00	01	90	87	34	teml.xmlup% a#4	

继续改后缀为.zip, 然后解压得到一个文件夹

nux	SH2/ \	初10年	11/16
> Bug	Ku平台文件 > zip > 眼见非实 >	眼见非实	
^	名称 个	修改日期	类型
	_rels	2016/8/15 4:06	文件夹
	customXml	2016/8/15 4:06	文件夹
*	docProps	2016/8/15 4:06	文件夹
*	word	2016/8/15 4:06	文件夹
*	[Content_Types].xml		8_XML文档()

检索flag, 然后在word->document.xml中找到了flag



【注】:

方法二

Kaili 下执行binwalk,和foremost命令可以不用修改文件扩展名

root@kali:~	/桌面# binwalk zi	p(眼见非实\(ISCCC	TF\))
DECIMAL	HEXADECIMAL	DESCRIPTION	
10346	0x286A	End of Zip archi	ve
<pre>root@kali:~ Processing: foundat=0[</pre>	/桌面# foremost z zip(眼见非实(IS DOO、docxOz@DOO%	tip(眼见非实∖(ISCC) CCCTF)) %%% 000000000 "∏DҊt	CTF\)) HwJww ôtô04+ô000{ô0-ô0 ° wôeMô00{F=0d%00a

く 提取 +	ÑÛ‰û-Çʵ.docx Q ≡ ● ⊕ (
🥑 🛱 < > 🏠 位置(L):	■ /88	见非实/									
H 名称	Ŧ	大小	类型	已修改	1						
🗕 🛓 🚞 customXml		891字节	文件夹	2016年8月15日 04:00	6						
docProps		1.5 KB	文件夹	2016年8月15日 04:0	6						
실 裀 🚞 _rels		590字节	文件夹	2016年8月15日 04:0	6						
🗃 📧 word		43.3 KB	文件夹	2016年8月15日 04:00	6						
Content_Types].xml		1.4 KB	XML 文档	1980年1月1日 00:00	8						

6、啊哒



拿到压缩包,解压后是一个图片,放到winhex中寻找flag,发现有flag.txt字样,但是不知道怎么处理。

png	ada.j	pg																
Offs	et	0	1	2	3	4	5	6	7	8	9	А	В	С	D	Е	F	~
0035	620	00	A0	02	80	0A	00	28	00	A0	02	80	0A	00	28	00	A0	€ (€ (
0035	630	02	80	0A	00	28	00	A0	02	80	0A	00	28	00	A0	02	80	.€ (€ (€
0035	640	0A	00	28	00	A0	02	80	0A	00	28	00	A0	02	80	0A	00	(€(€
0035	650	28	00	A0	02	80	0A	00	28	00	A0	02	80	0A	00	28	00	(€(€(
0035	660	A0	02	80	0A	00	28	00	A0	02	80	0A	00	28	00	A0	02	€ (€ (
0035	670	80	0A	00	28	00	A0	02	80	0A	00	28	00	A0	02	80	0A	€ (€ (€
0035	680	00	28	00	A0	02	80	0A	00	28	00	A0	02	80	0A	00	28	(€ (
0035	690	00	A0	0F	FF	D9	50	4B	03	04	14	03	01	00	00	00	9D	ýÙFK
0035	6A0	7D	52	4D	3E	A1	8B	5D	22	00	00	00	16	00	00	00	08	}RM>;<]"
0035	6B0	00	00	00	66	6C	61	67	2E	74	78	74	3F	B1	6E	80	97	flag.txt2en€-
0035	6C0	FE	BF	44	3B	35	6A	56	E1	E5	75	A1	СЗ	C1	Α4	2D	93	þöby Ejliðau jÂÁn-"
0035	6D0	5A	FA	C4	B9	49	B0	AC	A9	D5	00	AD	07	73	50	4B	01	ZúÄ⁺I°−©Ĉ – sFK
0035	6E0	02	3F	03	14	03	01	00	00	00	9D	7D	52	4D	3E	A1	8B	2 }RN≥; <
0035	6F0	5D	22	00	00	00	16	00	00	00	08	00	24	00	00	00	00]"\$
0035	700	00	00	00	20	80	Α4	81	00	00	00	00	66	6C	61	67	2E	€≏ flag.
0035	710	74	78	74	0A	00	20	00	00	00	00	00	01	00	18	00	00	txt
0035	720	F9	СЗ	77	B6	66	D4	01	00	26	F5	78	B6	66	D4	01	00	ùÂw¶fĈ &ĉx¶fĈ
0035	730	F9	СЗ	77	B6	66	D4	01	50	4B	05	06	00	00	00	00	01	r ùâ#112 ¢v fk 5841822890
10035	740	nn	01	nn	52	nn	nn	nn	48	nn	nn	nn	nn	00				2 H



root@kali:~/#	面# binwalk ada	.jpg	-
DECIMAL	HEXADECIMAL	DESCRIPTION	
0 30 ory: 8	0x0 0x1E	JPEG image data, JFIF standard 1 TIFF image data, big-endian, off:	.01 set of first image direct
5236 7782 ada.jpg pmeta>	0x1474 0x1E66	Copyright string: "Copyright App Unix path: /www.w3.org/1999/02/22	le Inc., 2018" 2-rdf-syntax-ns#"/>
218773 pressed size: 218935	0x35695 34, uncompresse 0x35737	Zip archive data, encrypted at lo d size: 22, name: flag.txt End of Zip archive	east v2.0 to extract, com
root@kali:~/≢ Processing: ad foundat=flag *	面# foremost ad da.jpg .txt?@n@@@@D;5jV0	a.jpg 00u0000-0Z0ĹI0000	
root@kali:~/#	面#	https://	/blog.csdn.net/zsw15841822890

内含一个zip压缩包,分离文件:



压缩包需要密码:



回去看看源图片文件ada.jpg的详细信息

照相机制造商 照相机型号 光圈值 曝光时间 ISO 速度 喝平110	7364626973635732303138	
---	------------------------	--

16进制,转化成字符串(Notepad++中的插件,直接16进制转ASCII):

73646E6973635F32303138

婆 转换工具 by zj1244[小葵]	-	
要转的:		
dnisc_2018		给我转!
UNDAR		还原
SQL_En:		还原
Hex:		
73646E6973635F32303138	https://blog.csdn.net/zsw1584	[2] 还康] (]

有疑问,为什么在小葵花里解密密码是 dnisc_2018,网上wp上是sdnisc_2018

得到解压密码: sdnisc 2018



分离文件

(1) 使用dd命令分离(linux/unix下)

我们可以使用dd命令分离出隐藏文件:

dd if=carter.jpg of=carter-1.jpg skip=140147 bs=1

if是指定输入文件, of是指定输出文件, skip是指定从输入文件开头跳过140147个块后再开始复制, bs设置每次 读写块的大小为1字节。

dd命令: http://www.cnblogs.com/qq78292959/archive/2012/02/23/2364760.html

(2) 使用foremost工具分离

foremost是一个基于文件文件头和尾部信息以及文件的内建数据结构恢复文件的命令行工具,直接将文件拆解



7. 又一张图片,还单纯吗

图片隐写, 套路化, notepad++、winhex、右键属性、binwalk、foremost打一遍 Binwalk和foremost问题解决

root@ka1	li:~/	′桌面# binwalk	2.jpg
DECIMAL		HEXADECIMAL	DESCRIPTION
0 12 ory: 8	n di l	0x0 ≝⊢0xC	JPEG image data, EXIF standard TIFF image data, big-endian, offset of first image direc
1301/ escripti	ion r	0X32D9 df:about="" xr 26C48	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf: lns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns JPEC image data JETE standard 1.02</rdf:
158822 ory: 8		0x26C66	TIFF image data, big-endian, offset of first image direc
159124 162196		0x26D94 0x27994	JPEG image data, JFIF standard 1.02 JPEG image data, JFIF standard 1.02
164186 escripti	ion r	□ 0x2815A df:about="" xr 0v20182	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf: lns:dc="http://purl.org/dc/elements/1.1/" xmlns:xap="htt Copyright string: "Copyright (c) 1008 Howlott Packard Co</rdf:
pany"			copyright string. copyright (c) isso newtert-rackard co
root@kal Processi *	li:~/ ing:	/桌面# foremost 2.jpg	2.jpg
2020年(96月 9	業面# date 28日 星期日 08	:25:52 CST https://blog.csdn.net/zsw1584182289

Foremost后out文件夹下看到



falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

8、猜

flag格式key{某人名字全拼}



百度识图:



Key{liuyifei}

9、宽带信息泄露

flag格式: flag{宽带用户名}

使用RouterPassView工具查看,

大多数现代路由器都可以让您备份一个文件路由器的配置文件,然后在需要的时候从文件中恢复配置。路由器的备份文件通常包含了像您的ISP的用户名重要数据/密码,路由器的登录密码,无线网络的KEY。

如果你忘记了这些密码,但你仍然有你的路由器配置的备份文件,那么RouterPassView可以帮助你从路由器配置文件中恢复您的密码。该软件可以读取这个路由配置文件。

运行软件,打开"文件"菜单->"打开路由器配置文件",打开保存的路由器配置文件。 或者Grab Password From IE Window。

```
    MouterPassView - C:\Users\bbjz\Desktop\BUGKU\9-(宽带信息泄露)conf.bin
    文件(E) 编辑(E) 查看(V) 选项(Q) 帮助(H)
    ② ④ □ □ ③ □ ④ □ ③ ④ ④
```



Flag{ 053700357621}

注: 秘钥破解工具

Aircrack-ng kaili下自带

命令: Aircrack-ng miyao.ivs (2017年9月部科信局在线测试题)

10、隐写2

Welcome_.jpg



想拿到flag?心の中ないいくつかB数かの?

图片隐写,套路化,notepad++、winhex、右键属性、binwalk、foremost打一遍

Notepad++

	:D8 ETX xFE {痣 xF	媵銉xAF?炁疹[SYN
	掬F<珪NUL镋DC4PI	xF1SYN]殯名nxC4
	NUL <mark>flag</mark> .rarPKE	NULNUL <mark>flag</mark> .rar
搜索flag发现文件	ETX鹗tEOT/蓁xFF	X?NULDC4NULNULE

Winhex打开

						-			- C - C -	·			- nc/				VVI 3 P		-
2.jpg 隐写2-	Weld	com	ejp	g	3.jpg	9 \	Nelc	ome	_ jpg										
Offset	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	E	F			\wedge
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	78	<mark>ÿ</mark> Øÿà JFIF	x	
00000010	00	78	00	00	FF	E1	10	B0	45	78	69	66	00	00	4D	4D	x (ÿá °Exi:	e)mm	
00000020	00	2A	00	00	00	08	00	06	01	0E	00	02	00	00	00	06	*		
00000030	00	00	08	62	01	12	00	03	00	00	00	01	00	01	00	00	b		
00000040	87	69	00	04	00	00	00	01	00	00	08	68	9C	9B	00	01	‡i 1	10E >	
00000050	00	00	00	0C	00	00	10	88	9C	9F	00	01	00	00	00	14	^œŸ		
00000060	00	00	10	94	EA	1C	00	07	00	00	08	0C	00	00	00	56	″ê	v	
00000070	00	00	00	00	10	E' 7	00	00	00	00	00	00	00	00	00	00	A		

可以看到图片嵌入了Exif信息,但是看属性没看到什么有用的提示,老方法放到kali里找

使用binwalk提取

2020年 06月 28 root@kali:~/桌 2.jpg Welcome root@kali:~/桌	8日 星期日 08:25 面#ls jpg 面# binwalk Weld	:52 CST come_\ .jpg							
DECIMALtput	HEXADECIMAL	DESCRIPTION							
0 30 orv: 8	0x0 0x1E	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image direct							
4444 scription rdf: 4900 xml:lang="x-c	0x115C about="uuid:faf 0x1324 default">hint: </td <td>Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:de 5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc="http://p Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:li rdf:li></rdf:li </rdf:de </td>	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:de 5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc="http://p Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:li rdf:li></rdf:li </rdf:de 							
52516 ze: 6732, unco	0xCD24 ompressed size: (Zip archive data, at least vl.0 to extract, compressed si 6732, name: flag.rar							
59264 147852	0xE780 0x2418C	End of Zip archive End of Zip archive							
root@kali:~/桌面# foremost Welcome_\ .jpg Processing: Welcomejpg foundat=flag.rarPK圓圓 foundat=提示_ipg@@wP@ 际@E@L"@tID@4									
Bŵwû圖"]@Dût圖 練'ûûûû9û0û:}(*	 00@!!!!`Ha00000000 000%00s0a000g08Fi 	E∰0000000⊞DETZ00(Ho⊞ 0000wv003Eyy709000<0£0000<ቼ00>0°# @t80Er00000@00N⊞0v0 000'00000b0M:y000000;0000002LG\$@G0000@D0 https://Diog.csdn.net/zsw15841822890							

foremost后output文件夹

企 主文件夹	桌面 out	put zi	p ▶	
提取 +]		00000102.2	zip
< > û	位置(L):	i /		
名称			大小	类型
칠 flag.rar			6.7 KB	RAR 1/3
■ 提示.jpg			92.4 KB	JPEG 图

提示.jpg (提示密码为3个数字)

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。s://blog.csdn.net/zsw15841822890

爆破flag.zip,工具 Advanced Archive Password Recovery



压缩包密码: 871

解压后图片



Winhex打开

00001010	55	110	J.n.	50	<u>0</u> 1	0.1	Un.	JA		014	40		on	50		ы±	ليەر كىيەرت / دىت
00001A00	76	83	BE	19	02	12	19	85	DD	F5	2F	71	D9	F8	ED	F8	vf¾ …Ýõ∕qÙøíø
00001A10	D6	32	7B	25	E4	Fl	53	17	8C	80	50	37	D7	1D	BF	9C	Ö2{%äñS Œ€P7× ¿œ
00001A20	A0	2E	B 0	29	AC	Α6	B1	AD	38	00	A3	62	CF	8C	69	6D	.°)¬¦±-8 £bÏŒim
00001A30	CB	15	9F	6F	6C	A 0	86	25	6E	12	70	EΒ	BC	69	6B	41	Ë Ÿol †%n pë≒ikA
00001A40	23	E4	67	D4	FF	D9	20	20	20	20	66	31	40	67	7B	65	#ägÔÿÙ fl@g{e
00001A50	54	42	31	49	45	46	79	5A	53	42	68	49	47	68	41	59	TBliEFyZSBhIGhAY
00001A60	32	74	6C	63	69	45	ЗD	7D	20	20	20	20	20	0D	AO	20	2tlciE=}
00001A70	1A																

密文eTB1IEFyZSBhIGhAY2tlciE=

带"="

base64解密,工具小葵花

J Base64:	
eTB1IEFyZSBhIGhAY2ttciE=	- 解密 Base64
, 解密Base64:	
y0u Are a h@cker!	ar

fl@g{ y0u Are a h@cker!}

11、多种方法解决

提示: 在做题过程中你会得到一个二维码图片

使用winhex打开,发现是一个base64转图片,所以先将后缀改为.txt,然后将base64编码为图片(base64转换为图片工具)

KEY.exe																	
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	ANSI ASCII
00000000	64	61	74	61	ЗA	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	he72KBitxIFgTv/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
00000000	6E	34	35	7A	66	64	78	65	35	5A	33	73	4A	37	70	72	n45zfdxe5Z3sJ7pr
00000D0	48	62	66	39	72	58	4F	33	50	34	6C	4C	76	59	50	63	Hbf9rXO3P41LvYPc
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	3T200/7eud680T2H
00000120	33	4C	43	66	74	30	6C	2F	61	65	39	5A	6C	54	6F	2B	3LCft01/ae9Z1To+
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+S71+/68
00000190	4D	4A	63	35	4F	30	4F	53	57	70	63	79	65	78	6E	46	MJc5000SWpcyexnF
000001A0	6A	66	63	73	49	2B	4A	57	31	75	6B	70	52	66	76	2B	jfcsI+JWlukpRfv+
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	GcWN9ywj41bW6S1F

🥘 KEY - 副本.txt - 记事本

文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H)

 fdxe5Z3sJ7prHbf9rXO3P4lLvYPctbeM80dvtP+3pnDp9yF7tneQvvmcZu/2lf78zhU+5i9yxv4T3T2 +/68MJc5O0OSWpcyexnFjfcsI+JW1ukpRfv+vDCXOTtDklqXMnsZxY33LCPiVtbpKUX7/rwwlzk +nDC3CSWk7a/i73PctL2DbvH3CQpv37XhxPmJrGctP1d7H2Wk7Zv2D3mJkn59bs+nDA3ieWE1 +fW7PjzJ7v12b33LSdtvsfuW75LuX7/rw5Ps3m/31rectP0Wu2/5Lun+9bs+PMnu/XZvfctJ22+x+ +yfzTmppE2U2l5YZ9+Ih/3VfaPxtw00mZKLCfs00/k477K/tGYm0baTInlhH36iSxfIT78TpI605bdF UmdKUmdk5LUaXzdWB/eYX3LCfuUpM6UtDklqTMlqXNSkjqNrxvrwzusbzlhn5LUmZl2pyR1pi +pYT9k0ibaa7pHt6NY3uYJ8Svw3uaWF9vwn7ppE2013SPb2aRnewT4nlBvfUsL7lhH3TSJvpLune

base64编码

转图片

X

OSJ+XTYVkudt9yg5tqpiw2d5C150mKJEsSJ+5KYvovd152gmppcy155b60WKLECSI+J2DYVCtW7mKtrCsAb5Ly2WKLGCSE+J5DYTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrCsAb5Ly2WKLGCSE+J5DVTrCsW7qmKtrNSW5ZWLSWXLSCSW7kLGCSE+J5DVTrCsW7qmKtrNSW5ZW5LKNSVSDV2ULSWNKLGCSE+J5DVTrCsW7QmKtrXHSWXKLKNAPMJDk10mZqpE1jS7px2GJ+qx11To20mZ12p0baT12p0bxJLy2WLKHQD4kQTDk10mZqpE1jS7pxCdKtRAb7KSZWKLKNAPKNSVZULL0CGKxTVWKLeGSW5JKDKLGC3PDVEXAb4QavTgG/JW1utqQbdxq7JMS3ZyW/7RG2kzfYWn95MjE9sxNl22mZDcn7D+tkTbTd1haPzkysT1200ibKdnNCftPa6TN9B2uXh5/S9rcbEk37jR2+5SkzpSkzo4kdaavTgG/JW1utqQbdxq7Dk10mQ2p2DSZek2GktAdaavTgG/JW1utqQbdxq7JMS3ZyW/7RG2kzfYWn95MjS9sxNl22mZDcn7D+tkTbTd1haPzkysT1200ibKdnNCftPa6TN9B2uXh5/S9rcbEk37jR2+5SkzpSkzo4kdaavTgG/JW1utqQbdxq7Dk10mQ2p2DSZek2GktZaWkLgCSGKzWkKNBCGCPbNE1x3uqNtn9h+Nzdsz5wSy8lu3zzBcsVewpS1LmTWG7Y3nLCPm1JN05KLP/D8tRG2CJJTJYVKtSf585Z046TE8j8sT23EnJLUuZNYbtjcsl+bUK3Tkos/8Py1EbMKUmd04nlhu0tJ+zTInTjpMTyP/R/i8Pw1/fJZYb3Jvx8Pd/iI+WWG5wb57D3/8pfIliucG9+Q5//6f4ZynIPkrKrtbffq2WQ07FPD+paTtk9O71sT



https://blog.csdn.net/zsw15841822890

KEY{dca57f966e4e4e31fd5b15417da63269}

12、闪的好快

这是二维码吗? 嗯。。。是二维码了,我靠,闪的好快。。。

题目来源: 第七季极客大挑战



动态的gif图片

1. 发现下载下来是一个gif图片,并且是会动的二维码,我们可以猜测flag很有可能是藏在这些动的二维码里面,这个时候 我们可以使用工具尝试分解gif里面的数据

白你

🎋 gifsplitter2.0 .exe

1. 分离出来发现是18张不完整的gif图片,如果尝试每张去修复,工作量太大了,这个时候我们尝试去使用



1. 保存图片祭出神器StegSolve。 然后Analysis->Frame Browser。这里发现是18张图。也就是18张图片。



我拿手机一个挨着一个扫的。 扫出来的结果是SYC{F1aSh-so-f4sT} 但是提交不正确。 最后更改为SYC{F1aSh_so_f4sT}

13、come_game

听说游戏通关就有flag 题目来源:第七季极客大挑战

下载好题目,解压打开文件,打开可执行文件

名称 ^	修改日期	类型	大小
MACOSX	2016/10/9 23:47	文件夹	
DeathTime	2020/6/28 16:35	文件	1 KB
🧶 joker's.exe	2016/10/9 23:45	应用程序	8,106 KB



进行通关玩耍,会发现生成一个文件,用记事本打开,你会发现发现里面记录了通关数,考虑更为为最后一关

BU	GKU → game_1					
	名称 ^	修改日期	类型	大小		
	MACOSX	2016/10/9 23:47	文件夹			
	📄 DeathTime	2020/6/28 16:35	文件	1 KB		
	🥮 joker's.exe	2016/10/9 23:45	应用程序	8,106 KB		
	📄 save1	2020/6/28 16:35	文件	1 KB		
	🗋 temp	2020/6/28 16:35	文件	1 KB		
		<u> </u>			~~	
NU	B <mark>SC =)5(NUBI)</mark> UBA(NUB(=NO)C(NU		ULINULINUL			ULINULINUL

顺着玩是保存通关记录,而逆着玩,则是在读取通关记录,则会发现flag。



然后提交flag即可。

但是这里有一个坑需要注意就是这里并不是flag的格式而是SYC{6E23F259D98DF153}这种格式。

14、白哥的鸽子

图片隐写,套路化,notepad++、winhex、010edit、右键属性、binwalk、foremost打一遍 拿到文件binwalk,一切正常

root@kali:~/	氟面# binwalk jp	g\(白哥的鸽子\)
DECIMAL	HEXADECIMAL	DESCRIPTION
0 30 directory: 8	0x0pg 0x1E 3	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of

丢进010editor和winhex(后者不清晰)

並 栅栏密码加密解密	—	×					
文字 flag{w22_is_v3rj	/_cool}@@						
栏数 3	栏 数 3						
加密	解 密	7	LELESI [0%s ayorg 2ivyc}l{2s3_c@aw				
关于: MV STUDIO:出品	Copyleft 2011-2014		rcl@				

发现文件末位有fg2ivyo}l{2s3_o@aw__rcl@字符串(含flag字样,推断出是栅栏密码,栅栏密码:就是把要加密的明文分成N个一组,形成一段无规律的话)

🏦 栅栏密码加密解密	- 🗆 X
文字 flag{w22_is_v3ry	_cool}@@
栏数 3	
加密	解 密

关干: MV STUDIO出品 Copyleft 2011-2014

尝试栅栏密码得出flag{w22_is_v3ry_cool}@@,栏数为3

flag{w22_is_v3ry_cool}

15、linux

提示: linux基础问题

放在linux下解压(或者Windows下解压),然后得到一个flag二进制文件,使用linux命令查找关键字grep 'key' – a flag



key{feb81d3834e2423c9903f4755464060b}

16、隐写3



Windows下打开正常(感觉高度少了),kaili下打开报错,IHDR:CRC error

← ŵ	主文件夹	桌面	output	png	output	png	•	۹ ::
使用的				c	labai.png		× ⁿ =	: • • ×
ne I	9	E法载入 atal error re	图像"daba sading PNG in	ii.png"。 mage file	IHDR: CRC	error		取消(C)

IHDR后的4字节是宽,再后4字节是高,00改成FF

Ŧ	Edit	As:	Hex	Ψ	Run	Scri	ipt	▼ R	lun 1	Cemp.	late								
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	Е	F	0123456789ABCDEF	
000	0h:	89	50	4 E	47	0D	0A	1A	0A	0	00	00	0D	49	48	44	52	%PNGIHDR	
001	0h:	00	00	02	A 7	00	00	01	00	08	06	00	00	00	6D	7C	71	§m q	
002	0h:	35	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	5sRGB.®Î.é	
	. Y	- ÷	4	<u> </u>	-	<u> </u>	. Y	1	Y	1	-		¥.	1	10	-			
0h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%F		
0h:	00	00	02	Α7	00	00	01	FF	08	06	00	00	00	6D	7C	71			
1	25	00	00	00	01	70	50	477	40	00		077	10	-	00	00	-		



flag{He1I0_d4_ba1}

17、做个游戏(08067CTF)

坚持60秒,Java程序heiheihei.jar



拿到题目,下载jar。直接解压,然后Java反编译.class文件

白柳	
📜 cn	
📕 images	
META-INF	





flag{RGFqaURhbGlfSmlud2FuQ2hpamk=} base64解密



18、想蹭网先解开密码

提示: flag格式: flag{你破解的WiFi密码}

tips: 密码为手机号,为了不为难你,大佬特地让我悄悄地把前七位告诉你 1391040** Goodluck!!

下载cap包,WIFI连接认证的重点在WPA的四次握手包,也就是eapol协议的包,过滤一下

	101	S	-	0111	1111	×	-	-	10	1	_	-	1	1	~	

📕 eapol			
No.	Time	Source Destination Protoc. I	Len
306	6 45.138762	D-Li LiteonTe_68:5f:7c EAPOL	
306	8 45.154148	Lite… D-LinkIn_9e:4e:a3 EAPOL	
307	0 45.168458	D-Li… LiteonTe_68:5f:7c EAPOL	
307	2 45.195620	Lite… D-LinkIn_9e:4e:a3 EAPOL	

使用crunch生成密码字典

crunch 11 11 -t 1391040%%%% >>wifipass.txt

或者: crunch 11 11 -t 1391040%%%% -o password.txt

root@kali:~/桌面# crunch 11 11 -t 1391040%%%% >>wifipass.txt
Crunch will now generate the following amount of data: 120000 bytes
0 MB
0 GB
0 zTB ip_
0 PB gL
Crunch will now generate the following number of lines: 10000

利用aircrack 进行爆破

aircrack-ng w wifipass.txt wifi.cap

或者aircrack-ng -a2 wifi.cap -w wifipass.txt

root@kali: ~/桌面# aircrack-ng -a2 wifi.cap -w wifipass.txt Opening wifi.cap Read 4257 packets.										
#	BSSID	ESSID		Encryp	tion					
1 2 3	3C:E5:A6:20:91:60 3C:E5:A6:20:91:61 BC:F6:85:9E:4E:A3	CATR CATR-GUEST D-Link_DIR-60	9A	WPA (0 WPA (0 WPA (1	handshake) handshake) handshake)					
Index	Index number of target network ? 3									
Openi Readi	Opening wifi.cap Reading packets, please wait https://blog.csdn.net/zsw15841822890									

第三个存在握手包,就是他。

秒出答案



flag{13910407686}

19、Linux2

给你点提示吧: key的格式是KEY{}

压缩包brave.zip 解压,产生brave文件,固定的binwalk 和foremost执行



产生图片文件

面	output	jpg	•	
		000	0267	782.jpg
	f	ag{f	Or	ensics scools
	https://	blog.c	sdn	.net/zsw15841822890

???出错???

flag格式是"KEY{}"

尝试直接搜索brave文件!

grep 'KEY' -a brave



KEY{24f3627a86fc740a7f36ee2c7a1c124a}

20、BUGku账号被盗了

http://123.206.87.240:9001/cookieflag.php

$\ \ \leftarrow \ \ \rightarrow \ \ G$	① 不安全 123.206.87.240:9001/cookieflag.php	* 🚳
🔢 应用 🍸		 📄 🚡 Chrome 🕅

You are not an admin!

文字说我们不是管理员

没什么提示,抓个包看看;

Intercept HTTP history WebSockets history Options					
Request to http://123.206.87.240:9001					
Forward Drop Intercept is on Action					
Raw Params Headers Hex					
POST /cookieflag.php HTTP/1.1					
Host: 123.206.87.240:9001					
Content-Length: 0					
Pragma: no-cache					
Cache-Control: no-cache					
Upgrade-Insecure-Requests: 1					
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36					
Origin: http://123.206.87.240:9001					
Content-Type: application/x-www-form-urlencoded					
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3					
Referer: http://123.206.87.240:9001/					
Accept-Encoding: gzip, deflate					
Accept-Language: zh-CN,zh;q=0.9					
Cookie: isadmin=false					
Connection: close https://blog.csdn.net/zsw15841822890					

显示false, 改成true, 然后repeater下试试看



发现出来个网页,打开后自动下载一个叫123.exe的文件

跟游戏有关的,利用wireshark分析一下;

找到User和pass

471 21.085779 14.17.57.241	192.168.43.224	SMTP	72 S: 334 VXNlcm5hbWU6
472 21.085999 192.168.43	14.17.57.241	SMTP	80 C: User: YmtjdGZ0ZXN0QDE2My5jb20=
473 21.151023 14.17.57.241	192.168.43.224	SMTP	72 S: 334 UGFzc3dvcmQ6
474 21.151170 192.168.43	14.17.57.241	SMTP	68 C: Pass: YTEyMzQ1Ng==
175 21 270562 11 17 57 241	103 160 13 334	TCD	54 35 . 10726 [ACK] Son-311 Ack-75 Win-14464 Lon-0

选一个右键点击追踪流就行了,这两行用base64解密就是163邮箱的账号和密码。登陆之后找flag。

YmtjdGZØZXNØQDE2My5jb2Ø= 334 UGFzc3dvcmQ6 YTEyMzQ1Ng==

里面有人把flag修改了,不过我发了一份真flag上去了,去收件箱找就行了!

真flag! flag{182100518+725593795416}

flag{182100518+725593795416}

【注】未完待续