BUGKU CTF之misc篇(持续更新)

原创

山山得久
● 于 2018-09-23 14:25:08 发布
● 4739 % 收藏 13
分类专栏: CTF学习之路 文章标签: bugku ctf misc
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/drothy_zhang/article/details/82821978

版权

CTF学习之路 专栏收录该内容

4篇文章0订阅

订阅专栏

题库链接: http://ctf.bugku.com/challenges

一.签到题

下载二维码关注bugku得到flag

二.这是一张单纯的图片

图片链接: http://120.24.86.145:8002/misc/1.jpg 下载图片后用winhex或者hexworkshop打开可以看到

1D 64 06 8A 28 03 D0 A8 A2 8A 00 28 A2 8A 00 28 d š(Ш¢Š (¢Š (40 A2 8A 00 FF 26 23 31 30 37 3B 26 23 31 30 31 3B ¢Š ÿke 50 26 23 31 32 31 3B 26 23 31 32 33 3B 26 23 31 32 60 y{ 31 3B 26 23 31 31 31 3B 26 23 31 31 37 3B 26 23 1;ou&# 70 33 32 3B 26 23 39 37 3B 26 23 31 31 34 3B 26 23 32;ar&# 80 90 31 30 31 3B 26 23 33 32 3B 26 23 31 31 34 3B 26 101; r & 23 31 30 35 3B 26 23 31 30 33 3B 26 23 31 30 34 #105;gh A0 3B 26 23 31 31 36 3B 26 23 31 32 35 3B D9 D9 ;t}ÙÙ B0

这明显是一段加密编码:

所以我们直接进行解密,这里给大家提供一下在线解密网址: http://tool.chinaz.com/tools/unicode.aspx。 然后就可以得到flag。

三.隐写

下载解压,得到一张png图片,老规矩,我们放到winhex里面看一下。 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。 PNG图片详解

然后我们再看一下图片的高宽,发现高宽不一样:

2.png																	
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000010	00	00	01	F4	00	00	01	Α4	08	06	00	00	00	CB	D6	DF	ô ¤ ËÖß
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	50	68	t Þf x MiCCPPh
00000040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otoshop ICC prof
00000050	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile xÚ SwX"÷ >ß
00000060	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23	AC	80	÷e VBØð±−1 "#¬
00000070	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	A0	È Ү¢ ′а" @Å^
00000080	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88	E2	A 0	V œHUÄ,ÕH ^â
00000090	28	B8	67	41	8A	88	5A	8B	55	5C	38	EE	1F	DC	A 7	B5	(,gAŠ^Z <u∖8î td="" ܧµ<=""></u∖8î>
0A000000	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9Ć	E7	FC	CE	79	.CF	}ziiiû×û4çœçûÎyÏg
00000080	0.5	80	11	12	26	91	F6	7.2	67	00	20	52	95	30	37	D8	E : 1203 GD / 0

这里我们将A4改成F4,保存,再次查看图片,即可得到flag;

四.telnet

将1.zip下载解压我们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

て件(E)	编辑(<u>E</u>) 视图	(⊻) 跳转(G) 捕获(C) 分析(<u>A)</u> 统计(<u>S</u>) 电	话(Y) 无线(W)	工具(I)	帮助(<u>H</u>)					
	60	🗙 🖸 🤇 🗢 🗢 🗟 👔	۹ 📃 📃 🕭	ର୍ ବ୍ 🎹							
teln	et 🛛	过滤							$\times \rightarrow \cdot$	表达式…	•
·	Time	Source	Destinati	ion		Protocol	Length Info				
	4 0.07800	102 168 221 128	102 169	3.221.164		TELNET	75 Telnet	Data			
	6 4.50840	你吃/蚁洞你吃 方阻(<u>IVI</u>)	Ctri+IVI	.221.128		TELNET	66 Telnet	Data 🧹.			
	7 4.55520	忽略/取消忽略 分组(!)	Ctrl+D	.221.164		TELNET	57 Telnet	Data 🔝			
	8 4.57080	设置/取消设置 时间参考	Ctrl+T	.221.128		TELNET	66 Telnet	Data			
	9 4.64880	时间平移	Ctrl+Shift+T	.221.164		TELNET	63 Telnet	Data			
	10 4.64880	分组注释	Ctrl+Alt+C	.221.128		TELNET	72 Telnet	Data			
	11 4.72680			.221.164		TELNET	71 Telnet	Data			
	12 4.75800	编辑解析的名称		.221.164		TELNET	60 Telnet	Data		点击右	键
	13 4.78920	作为过滤器应用	•	.221.164		TELNET	65 Telnet	Data			
	15 4.83600	准备讨减器	•	.221.128		TELNET	63 Telnet	Data			
	16 4.89840	对活冲海器	•	.221.164		TELNET	57 Telnet	Data			
	17 4.92960	いた主体		.221.164		TELNET	57 Telnet	Data			
	18 4.96080		, i	.221.164		TELNET	57 Telnet	Data			
	20 4.99200	SUIP	,	.221.128		TELNET	74 Telnet	Data			
	22 5.02320	追踪流	•	.221.128		TELNET	90 Telnet	Data			
	24 16.1148	复制	追踪TCP流	.221.164		TELNET	55 Telnet	Data			
	25 16.1304			.221.128		TELNET	60 Telnet	Data			
	27 16.4112	协议首选项	•	.221.164		TELNET	55 Telnet	Data			
	28 16.4112	解码为(<u>A</u>)		.221.128		TELNET	60 Telnet	Data			
	30 16.5048	在新窗口显示分组(<u>W</u>)		.221.164		TELNET	55 Telnet	Data			
	31 16.50482	192.168.221.164	192.168	3.221.128		TELNET	60 Telnet	Data			
	33 16.78562	192.168.221.128	192.168	3.221.164		TELNET	55 Telnet	Data			
	24 46 00422	402 400 224 404	400 400	2 2 2 4 2 0		TELNET	Do . A GHLVB. C		/ uroun)	_21101	15

即可得到flag。

五.眼见非实

下载得到文件zip,无后缀名,我把他放到winhex里面查看,可以看到

zip																					
Offs	et	0	1	2	3	4	5	6	7	8	9	Α	в	С	D	E	F		ANSI	ASCII	~
00000	000	50	4B	03	04	14	00	00	00	08	00	1A	80	87	49	5C	DC	PK		€‡I\Ü	

 \Box \times

0000010	E4	DA	04	28	00	00	AC	36	00	00	0D	00	00	00	D1	DB	äÚ (6 ÑÛ
0000020	BC	FB	B7	C7	CA	B 5	2E	64	6F	63	78	9D	7A	05	40	15	4û Çʵ.docx z @
0000030	DB	F7	F5	25	25	25	25	A 5	BB	Α4	BB	Α5	BB	BB	BB	E1	Ü÷õ%%%%¥»¤»¥»»»á
0000040	22	1D	92	D2	8A	74	09	48	77	4A	77	77	87	74	8A	80	" 'ÒŠt HwJww‡tŠ€
0000050	34	D2	82	C0	87	BE	E7	7B	80	FA	7E	FE	BF	CB	В9	77	4Ò,À‡¾ç{€ú~þ¿Ë¹w
0000060	CF	65	CE	9C	B 3	EE	DA	7B	CF	9C	ЗD	B3	64	25	сó	C0	ÏeΜ³îÚ{Ïœ=³d%ÀÀ
0000070	61	00	DF	5E	1F	FO	11	C4	00	B7	5E	D0	00	34	C0	C8	а ß^ ð Ä ·^Ð 4ÀÈ
0000080	6C	FD	45	55	57	6F	05	AD	03	10	19	00	82	19	9E	D1	lýEUWo – , žÑ
00000090	B2	9E	58	FF	29	DB	7B	23	29	79	B5	28	99	56	F6	9F	"žXÿ)Û{#)yµ(™VöŸ
0A00000C	83	5B	EE	1D	8C	02	C0	FF	F7	60	03	07	ЗB	7B	1B	2B	f[î Œ Àÿ÷` ;{ +
00000B0	55	2B	CB	9B	61	1E	03	40	9E	CF	78	17	DF	19	E6	DF	U+Ë>a @žÏxßæß
00000000	\mathbf{FD}	DF	06	44	BD	39	1C	EA	E6	4D	00	60	36	C2	50	4D	ýß D№9 êæM `6ÂРМ
00000D0	BA	D9	BA	BA	79	ЗF	06	50	FC	6A	40	33	7B	23	2B	FA	°Ù°°y? Püj@3{#+ú
00000E0	27	CE	56	96	0E	40	12	00	48	62	00	13	D2	6F	46	FE	'ÎV- @ Hb ÒoFþ
00000F0	A7	63	E1	90	14	8C	2F	1D	A2	FF	F2	F3	54	27	28	76	§cá Œ∕¢ÿòóT'(v
00000100	AF	F0	27	9A	81	30	4F	E7	27	9E	Α6	E4	5B	47	B0	25	¯ð'š 00ç'ž¦ä[G°%
00000110	FO	79	10	63	F2	DB	2C	E2	67	92	7D	7A	76	86	AB	1D	ðy còÛ,âg′}zvt«
0000120	27	3C	C1	65	29	C7	4F	F8	98	9A	\mathbf{FC}	45	DO	8A	5E	6A	'<Áe)ÇOø∼šüEЊ^j
0000130	ЕG	DE	D5	Β4	5D	59	ЗA	2E	A9	2F	E9	99	6D	F2	(2B)	9F	næ₽Ő′]Y:.©∕é™mò+Ÿng
00000140	11	8D	95	D4	Δ9	C8	CC	8F	2 F	10	96	19	06	63	22	DO	•Ôਫ਼ÈÌ / – c"Đ

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: 眼见非实 。发现文档还是打不开,我们再放进winhex里面查看一下,再次发现了压缩文件的头 50 4B 03 04 。改后缀名 为 zip 可得到文件夹。

_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].xmbs://blog.	.csdn.net/drot	hyXML的文档g

flag路径:word->document.xml。

六.又一张图片,还单纯吗

放进winhex中查看,什么也没有发现,根据图片提示,图片不单纯,猜测图片里面有其他文件在其中,打开 kali->终端->用 binwalk查看。

d	杲	囬	* *	

binwalk 2.jpg

可以看到里面有两张图片

root@bogon:~/Desktop#_binwalk_2.jpg

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, EXIF standard
12 directory: 8	0xC	TIFF image data, big-endian, offset of first image
13017	0x32D9	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:descript< td=""><td>tion rdf:about="'</td><td><pre>xmlns:photoshop="http://ns.adobe.com/photoshop/1.</pre></td></rdf:descript<>	tion rdf:about="'	<pre>xmlns:photoshop="http://ns.adobe.com/photoshop/1.</pre>
0/" xmlns		
158792	0x26C48	JPEG image data, JFIF standard 1.02
158822	0x26C66	TIFF image data, big-endian, offset of first image
directory: 8		
159124	0x26D94	JPEG image data, JFIF standard 1.02
162196	0x27994	JPEG image data, JFIF standard 1.02
164186	0x2815A	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:descript :xap="htt</rdf:descript 	ion rdf:about="'	<pre>xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns</pre>
168370	0x291B2	Copyright string: "Copyright (c) 1998 Hewlett-Pack
ard Company"		https://blog.csdn.net/drothy_zhang

然后输入:

formest 2.jpg

将图片分离,在虚拟机桌面上你可以看到多出一个文件夹,里面有一张图片上面含有flag。

七.猜

直接图片复制,百度识图,发现是神仙姐姐,根据提示: key{liuyifei}

八.宽带信息泄露

可以发现是一个配置文件,使用RouterPassView工具查看。根据flag格式可知需要查找用户名,查找关键字 ctrl+F 输入 username,即可得到。

九.隐写二

得到图片,用winhex没发现什么有用信息,放进kali里面binwalk查看,发现有异样,**查看以及分离见题六**,得到文件夹,里面 有个flag压缩文件,发现打开需要密码,根据提示和人名可以知道密码扑克牌中的KJQ有关,又是三个数字,根据键盘发现字母和 数字之间的关系,k->8,J->7,Q->1,得到密码是871.使用ARCHRP软件暴力破解也可以,解压得到3.jpg,内心无限卧槽,没办法, 继续放到winhex中查看,在最底端发现了一段加密编码,在线base64位解码得到flag。

十.多种方法解决



创作打卡挑战赛 赢取流量/现金/CSDN周边激励大奖