[BUGKU][CTF][MISC][2020] MISC writeup持续更新中

原创

 CryptWinter
 ● ± 2020-12-30 22:44:13 发布
 ● 2747
 ◆ 收藏 4

 分类专栏:
 CTF 文章标签:
 BUGKU 2020 MISC writeup CTF

 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/dadongwudi/article/details/111998874

 版权



CTF 专栏收录该内容

17 篇文章 2 订阅 订阅专栏 CTF总结 ctf基本操作:https://blog.csdn.net/mafucan/article/details/106886421 zip:https://www.anquanke.com/post/id/86211

找软件推荐网址 1.https://www.52pojie.cn/ 2.没有的话百度一下去找百度云 工具下载:

1. stegSolve 隐写分析 需要配置Java环境 http://www.caesum.com

MISC 1 签到题目 步骤:扫码关注

MISC 2 这是一张单纯的图片 关键字: 信息隐藏 步骤: 1.右键,用记事本或者是用.notepad++打开拉到最下面,看到key{you are right} 2.复制下来HTML实体化转换得出flag

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)

步骤:

1.安装winhex (setup安装在电脑上即可使用) https://www.52pojie.cn/thread-999432-1-1.html

2.修改高度 A4->F4,使图片显示完整

WinHex - [2	.png]																-
Eile Edit	Sea	arch	N	avig	ation	n <u>v</u>	iew	To	ols	Spe	cialis	st 🤇	Optio	ons	Wi	ndov	w <u>H</u> elp	
07.44					5		Đ	6	BB 10	10	1		HE		B HEX		→ + + + ≥	3
2.png																		
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	Е	F	ANSI ASCI	A 1
00000000	89	50	4E	47	0D	0A	1A	0A	E AO	00	00	0D	49	48	44	52	*PNG IHD	R
00000010	00	00	01	F4	00	00	01	Α4	08	06	00	00	00	CB	D6	DF	ô ¤ ËÖ.	в
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	OA	4D	69	43	43	50	50	68	t Pf x MicCPP	h
00000040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otoshop ICC pro	E
00000050	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile xÚ SwX"÷ >	в
00000060	F7	65	OF	56	42	D8	FO	B1	97	6C	81	00	22	23	AC	08	÷e VBØð±−1 "‡¬	
00000070	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	OA	È Y¢ ' a, @Å*	

MISC 4 telent

关键字: winhex winshark

步骤:

4.1 winhex直接打开

4.2 wireshark打开pacp文件一切都是协议 telnet也不例外 通过telnet与服务器主机进行交互 telnet包可以通过追踪tcp流找到

MISC 5 眼见为实

关键字: word zip

知识点: word文档本质上是个压缩包

步骤: 拿到后解压得到docx文档 打开显示内存被占满 无法打开 拖进010etidor瞅瞅是什么牛鬼蛇神 魔数PK开头 猜测是zip文件 将docx后缀改为zip后解压 之后得到一堆文件 全局搜索一些flag

MISC 6 啊哒

关键字: binwalk hex

步骤:

1.1

1.binwalk 查看,是文件包含,该文件包含一个jpg文件和一个zip文件。
 2.foremost分离文件,分离出一个jpg和一个zip文件,
 3.打开zip文件,有flag.txt文件,解压缩提示需要密码。
 4.查看图片详细信息,相机型号为16进制,转字符后得到解压缩密码。

5.打开flag.txt,得到flag。

2.1解压,用hex打开,看到flag.txt,改后缀zip,发现需要解压密码,查看图片详情16进制转字符为密码,解压成功得到一个flag.txt 文件

MISC 7 又一张图片,还单纯吗 关键字: binwalk foremost 步骤: 1.binwalk flle.jpg 2.foremost -T file.jpg MISC 8 猜 步骤: 1.百度识图 2.是刘亦菲liuyifei MISC 9 宽带信息泄露 关键字: RouterPassView 步骤: 1.使用工具查看 RouterPassView (win) 2.搜索username MISC 10 隐写2 关键字: binwalk foremost fcrackzip winhex 步骤: 1.binwalk flle.jpg 2.foremost -T file.jpg 3.解压需要密码根据提示推出和数字有关 fcrackzip 破解zip压缩包密码 fcrackzip -b -l 3-3 -c 1 flag.rar 4.输入密码解压后winhex查看,base64解码 MISC 11 关键字: base64编码转换为图片 知识点: 步骤: 1.winhex打开 发现 data:image/jpg;base64, 2.后缀改为txt,在线base64转图片,扫描二维码得到key MISC 12 闪得好快 关键字: stegSolve 步骤: 1.下载 stegSolve 需要配置Java环境 http://www.caesum.com/handbook/Stegsolve.jar 2.java -jar Stegsolve.jar 打开软件 3.打开gif, Analysis->Frame Browser, 逐个扫描 组合得到答案 SYC{F1aSh_so_f4sT} MISC 13 come game 关键字: hex 步骤: 1. 通关第一关 2.到第二关发现根本过不去,发现exe文件下有个save文件,用hex打开后将数字"2"改到"5"

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



SYC{6E23F259D98DF153}

MISC 14 白哥的鸽子 关键字: hex 栅栏密码 知识点: 图片 FFD8开头, FFD9结尾 步骤: 1.末尾有嫌疑 fg2ivyo}{{2s3_o@aw__rcl@ 2.https://www.qqxiuzi.cn/bianma/zhalanmima.php

FF D9 66 67 32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77 EbEb‰î[ܶs ãÿÙ<mark>f</mark>g2ivyo}l{2s3_o@aw rcl@

MISC 15 linux
关键字: linux cat grep
知识点:
1.cat(英文全拼: concatenate)命令用于连接文件并打印到标准输出设备上。
2.Grep 是 Global Regular Expression Print 的缩写,它搜索指定文件的内容,匹配指定的模式,默认情况下输出匹配内容所在的行。注意,grep 只支持匹配而不能替换匹配到的内容。
步骤:
1.解压缩linux.zip,解压缩1.tar.gz,test目录下有一个flag文件。
2.1cat flag,即可见flag。
2.1grep 'key' -a flag



MISC 16 富强民主 关键字: 在线编码 步骤: http://www.atoolbox.net/Tool.php?ld=850 MISC 17 cisco 为未解决 关键字: cisco 步骤: 1.文件2.txt内容为AES加密,通过解密可知要改1.txt后缀为pka(思科文件后缀) 2.用思科打开,进到交换机CLI的特权执行模式,密码为flag,用show running-config命令查看配置即可找到flag

MISC 18 隐写3
关键字: hex 修改高度
步骤:
1.大白不完整
2.winhex打开 修改高度

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	00	00	02	A7	00	00	01	00	08	06	00	00	00	6D	7C	71
35	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	00	04	67	41	4D	41	49	30	۸B	8F	0B	FC	61	05	00	00
00	09	70	48	59	73	00	00	0E	C4	00	00	0E	C4	01	95	2B	0E	1B	00	00	FF	A	491	H44	41	54	78	5E	EC	BD	07
A0	A5	57	59	EE	FF	EE	BE	4F	9B	DE	93	4C	7A	0F	84	24	24	60	0C	04	A5	2B	20	45	10	10	BB	88	A8	A8	57
BD	FC	EF	BD	7A	F5	5A	AE	7A	BD	5E	CB	BD	2A	62	05	04	69	52	04	E9	01	42	48	48	42	7A	EF	7D	52	Α6	CF

3.出现flag



MISC 19 做个游戏
关键字: jd-gui
步骤:
1.解压后发现是个jar,无法运行
2.使用jd-gui(需要下载),搜索,找到flag后base 64



3.base64解码 flag{DajiDali_JinwanChiji}

MISC 20 想蹭网先解开密码 关键字: crunch https://blog.csdn.net/qq_42025840/article/details/81125584 aircrack-ng

知识点:wireshark查找,发现很多802.11协议,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
:	文件(E) 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(D) 帮助(H)		
4	(II 🖉 🕘 📘 🖎	🗳 ९ 🗢 🗢 🖉 🕭	其 📃 0, 0, 0, म			
	eapol					🛛 🗖 🔻 表达式… 🚽
Ň	o. Time	Source	Destination	Protocol	Length Info	
	3066 45.138762	D-LinkIn_9e:4e:a3	LiteonTe_68:5f:7c	EAPOL	155 Key (Message 1 of 4)	
	3068 45.154148	LiteonTe_68:5f:7c	D-LinkIn_9e:4e:a3	EAPOL	155 Key (Message 2 of 4)	
	3070 45.168458	D-LinkIn_9e:4e:a3	LiteonTe_68:5f:7c	EAPOL	213 Key (Message 3 of 4)	
	3072 45.195620	LiteonTe_68:5f:7c	D-LinkIn_9e:4e:a3	EAPOL	133 Key (Message 4 of 4)	
						the for the set of the

步骤:环境Linux Kali

1.crunch

└─\$ crunch 11 11 -t_1391040%%%% -o dictionsry.txt	
Crunch will now generate the following amount of data: 120000 by	tes
0 MB 最短 最长 margen 論山 文件名	
0 TB	
0 PB	
Crunch will now generate the following number of lines: 10000	
abunt, viingts puse a puse a small, konskmank	
crunch: 100% completed generating output	
https://blog.csd	n.net/dadongwudi

2.aircrack-ng

└─ \$ a Readi Openi Read	ircrack-ng <u>witi.ca</u> ng packets, please ng wifi.cap 4257 packets.	<u>p</u> -w <u>dictionsry.txt</u> wait wait		
#	BSSID Use method r	ESSID (See Delow)	Encryption	
1 2 3	3C:E5:A6:20:91:60 3C:E5:A6:20:91:61 BC:F6:85:9E:4E:A3	CATR CATR-GUEST D-Link_DIR-600A	Unknown Unknown WPA (1 handshake, wit	th PMKID)
Index	number of target n	etwork ? 3		https://blog.csdn.net/dadongwudi

Reading pa Opening wi Read 4257	ckets, ple fi.cap packets.	ase	e wa	ait	• • • •													
1 potentia	l targets																	
t/free zip @goof.com> /					in	Airo	cra	ck-r	ng :	1.6								
[00:	00:01] 948	0/:	1000	90 I	keys	s te	este	ed	(684	42.8	33 I	<td>) s t a</td> <td></td> <td></td> <td></td> <td></td> <td></td>) s t a					
Time	left: 0 s	ec	onds	ce S												Q	94.8	30%
te? [no] acterset]				ΚE	Y F(DUNI	D! S	[1 3	391(9407	7680	5]						
Mast	er Key	e v che ve	CD 09	43 37	57 4F	AD BF	21 03	96 CF	7A 58	F4 06	56 15	C1 62	43 4E	DB CD	56 D2	AF 68	D4 BB	5E 2D
d string Tran	sient Key	Lng ASS Lp Lod	BF F2 8F B4	B0 1B BD BE	E3 50 F7 34	FC FD FF 63	40 C1 50 76	0C 4C 3A C6	81 AC 2D A8	B6 69 CA 9B	08 84 68 99	E7 3B 50 B3	EA 5E 9F E6	AC 31 10 B7	04 48 09 29	BA 72 93 08	A0 97 EC E1	14 95 7D 9D
EAP0	L HMAC	es.	DD	75	EA	С9	CF	F8	13	5B	B0	F9	35	FA	8E	97	52	B3

MISC 21 zip伪加密 关键字: zip伪加密 知识点: zip伪加密是在文件头的加密标志位做修改,进而再打开文件时识被别为加密压缩包 一个 ZIP 文件由三个部分组成: 压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志

压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志

压缩源文件数据区:

50 4B 03 04: 这是头文件标记 (0x04034b50) 14 00: 解压文件所需 pkware 版本 00 00: 全局方式位标记 (有无加密) 08 00: 压缩方式 5A 7E: 最后修改文件时间 F7 46: 最后修改文件时期 16 B5 80 14: CRC-32校验 (1480B516) 19 00 00 00: 压缩后尺寸 (25) 17 00 00 00: 未压缩尺寸 (23) 07 00: 文件名长度 00 00: 扩展记录长度

压缩源文件目录区:

50 4B 01 02: 目录中文件文件头标记(0x02014b50) 3F 00: 压缩使用的 pkware 版本 14 00: 解压文件所需 pkware 版本 00 00: 全局方式位标记 (有无加密,这个更改这里进行伪加密,改为09 00打开就会提示有密码了) 08 00: 压缩方式 5A 7E: 最后修改文件时间 F7 46: 最后修改文件日期 16 B5 80 14: CRC-32校验 (1480B516) 19 00 00 00: 压缩后尺寸 (25) 17 00 00 00: 未压缩尺寸 (23) 07 00: 文件名长度 24 00: 扩展字段长度 00 00: 文件注释长度 00 00: 磁盘开始号 00 00: 内部文件属性 20 00 00 00: 外部文件属性 00 00 00 00: 局部头部偏移量 压缩源文件目录结束标志: 50 4B 05 06: 目录结束标记 00 00: 当前磁盘编号 00 00: 目录区开始磁盘编号 01 00: 本磁盘上纪录总数 01 00: 目录区中纪录总数

步骤:

1.压缩文件结构

59 00 00 00: 目录区尺寸大小

00 00: ZIP 文件注释长度

3E 00 00 00: 目录区对第一张磁盘的偏移量

1.1 查看文件,压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志

	50	4B	0.3	04	14	00	09	00	08	00	50	A3	A5	4A	21	38	76	65	19	00	00	00	17	00	00	00	08	00	00	00	66	6C
	61	67	2E	74	78	74	4B	CB	49	4C	AF	76	4C	C9	35	F4	D3	75	32	72	D7	CD	0E	D5	0D	8E	F2	0C	A8	05	00	50
Ŀ	4B	01	02	1F	00	14	00	09	00	80	00	50	A3	A5	4A	21	38	76	65	19	00	00	00	17	00	00	00	80	00	24	00	00
	00	00	00	00	00	20	00	00	00	00	00	00	00	66	6C	61	67	2E	74	78	74	A0	00	20	00	00	00	00	00	01	00	18
	00	0F	F5	04	D5	9A	C5	D2	01	46	1F	CB	8A	9A	C5	D2	01	46	1F	CB	8A	9A	C5	D2	01	50	4B	05	06	00	00	00
	00	01	00	01	00	5A	00	00	00	3F	00	00	00	00	00											_						

1.2 红色框住的50

4B 是压缩源文件数据区的头文件标记,它对应的红色框柱的 09 00 并不影响加密属性。 绿色框住的50 4B 是压缩源文件目录区,它对应的绿色框柱的 09 00 影响加密属性,当数字为奇数是为加密,为偶数时不加

												一把	煛索	左边	He	x字	符									
/iev	v Tools	Sp	ecialis	t C	Optic	ons	Wii	ndov	v H	Help					_											
	🗋 📑		4	ſ	5		5		Ē	ß		01- 110	ê) (4	HE×		-	- <u>E</u>	- -		3	3	in 🖏	
	flag.zip																									
	Offs	et	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	E	F			ANS	I Z	ASCII			_
	00000	000	50	4B	03	04	14	00	09	00	08	00	50	A3	A 5	4A	21	38	PK			Pf	£¥J!8			
	00000	010	76	65	19	00	00	00	17	00	00	00	08	00	00	00	66	6C	ve				fl			
	00000	020	61	67	2E	74	78	74	4B	CB	49	4C	AF	76	4C	C9	35	F4	ag.	.txt	tKËI	1_1	vLÉ5ô			
	00000	030	D3	75	32	72	D7	CD	0E	D5	0D	8E	F2	0C	A 8	05	00	<mark>5</mark> 0	Óu2	2r×j	ίŐ	Žò	Þ			
	00000	040	4B	01	02	1F	00	14	00	09	00	08	00	50	A3	Α5	4A	21	K			I	₽£¥J!			
	00000	050	38	76	65	19	00	00	00	17	00	00	00	80	00	24	00	00	876	2			Ş			
	00000	060	00	00	00	00	00	20	00	00	00	00	00	00	00	66	6C	61					fla			
	00000	070	67	2E	74	78	74	A0	00	20	00	00	00	00	00	01	00	18	g.t	txt						
	00000	080	00	0F	F5	04	D5	9A	C5	D2	01	46	1F	СВ	8A	9A	C5	D2	6	ŏ Õš	šÅÒ	ΕĖ	ËŠšÅÒ			
	00000	090	01	46	1F	СВ	8A	9A	C5	D2	01	50	4B	05	06	00	00	00	F	ËŠš	ŠÅÒ	ΡK				
	00000	0A0	00	01	00	01	00	5A	00	00	00	ЗF	00	00	00	00	00			2	Z	?				
																								ong		

1.3 更改绿色框中的数字,保存后用压缩软件打开后,即可看到flag

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		Al	NSI AS	SCII
00000000	50	4B	03	04	14	00	09	00	08	00	50	A3	A5	4A	21	38	76	65	19	00	00	00	17	00	00	00	08	00	00	00	66	6C	PK	P£¥J!8ve		fl
00000032	61	67	2E	74	78	74	4B	CB	49	4C	AF	76	4C	C9	35	F4	D3	75	32	72	D7	CD	0E	D5	0D	8E	F2	0C	A8	05	00	50	ag.txtKË]	L vLÉ5ôÓu2r×í (ōžòʻ	. Р
00000064	4B	01	02	1F	00	14	00	0.8	00	80	00	50	A3	A5	4A	21	38	76	65	19	00	00	00	17	00	00	00	80	00	24	00	00	K	P£¥J!8ve		Ş
00000096	00	00	00	00	00	20	00	00	00	00	00	00	00	66	6C	61	67	2E	74	78	74	A0	00	20	00	00	00	00	00	01	00	18		flag.txt		
00000128	00	0F	F5	04	D5	9A	C5	D2	01	46	1F	CB	8A	9A	C5	D2	01	46	1F	CB	8A	9A	C5	D2	01	50	4B	05	06	00	00	00	õ ÕšÅÒ	F ËŠŠÅÒ F ËŠŠÅO) PK	
00000160	00	01	00	01	00	5A	00	00	00	3F	00	00	00	00	00																		Z	?		

名称	^	压缩后大小	Л
flag.txt		25	

flag.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) flag{Adm1N-B2G-kU-SZIP}

flag{Adm1N-B2G-kU-SZIP} 参考链接: https://www.cnblogs.com/0yst3r-2046/p/11890498.html

2 ZipCenOp.jar

2.1 下载flag.zip ZipCenOp.jar文件 放置在同一个文件夹

下载地址: https://pan.baidu.com/s/1GHcUYA36X9reZL7rcmWNfA 提取码: ugyn 2.2 java -jar ZipCenOp.jar r flag.zip ,运行后均能不需要输入密码就能打开文件 正常



我的

D:\CTF\MISC)java -jar ZipCenOp. jar r flag.zip
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by zip.CenOp\$1 (rsrc:./) to method java.nio.DirectByteBuffer.cleaner()
WARNING: Please consider reporting this to the maintainers of zip.CenOp\$1
WARNING: Luse --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
Exception in thread "main" java.lang.reflect.InvocationTargetException
 at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
 at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
 at java.base/jdk.internal.reflect.MativeMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:62)
 at java.base/jdx.internal.reflect.MativeMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
 at java.base/java.lang.reflect.Method.invoke(Method.java:567)
 at org.eclipse.jdt.internal.jarinjarloader.JarRsrcLoader.main(JarRsrcLoader.java:58)
Caused by: java.lang.NoClassDefFoundError: sun/misc/Cleaner
 at zip.CenOp\$1.run(CenOp,java:95)
 at java.base/java.security.AccessController.doPrivileged(AccessController.java:310)
 at zip.CenOp,operate(CenOp,java:89)
 at zip.CenOp.main(CenOp,java:32)
 ... 5 more
Caused by: java.lang.ClassNotFoundException: sun.misc.Cleaner
 at java.base/java.lang.ClassLoader.findClass(URLClassLoader.java:58)
 at java.base/java.lang.ClassLoader.findClass(ClassLoader.java:58)
 at java.base/java.l

参考链接: https://www.pianshen.com/article/3780175978/

MISC 22 linux2 关键字: grep strings 知识点: grep的基本用法 https://blog.csdn.net/successdm/article/details/90145432?utm medium=distribute.pc relevant.none-task-blog-baidujs title-2&spm=1001.2101.3001.4242 步骤: 1.1 实验环境 Kali strings brave |grep 'key' -i -i不区分大小写

(d log kali) - [/mnt/hgfs/share] -<mark>\$</mark> strings <u>flag</u>grep 'KEY' -i -a2 Path=game DeletionDate=2016-06-27T12:27:37 Kev{} key{} key{feb81d3834e2423c9903f4755464060b} game.trashinfo game.trashinfo.OL1PJY -(d�� kali)-[/mnt/hgfs/share] -<mark>\$</mark> strings <u>brave</u>grep 'KEY' -i KEY{24f3627a86fc740a7f36ee2c7a1c124a} KEY{} HuD61KeYH1.JPG HuD61KeYH1.JPG

1.2 实验环境 windows nodepad++ 直接打开 搜索KEY

遹A%汥xCBGSIxE9"綦xE0NAKf2 xCC/hs账蜳t横诘uST INTENTIALITATIKEY(24f3627a86fc740a7f36ee2c7a1c124a https://blog.csdn.net/dadongwudi

MISC 23 细心的大象 关键字: binwalk foremost 知识点: dd命令 https://www.cnblogs.com/ginvip/p/6370836.html 步骤: windows+ kali 1.图片按照以往经验 binwalk查看 2.用dd命令 或 用foremost分解出来得到一个大象的图片及一个压缩包(有密码)



3.查看大象图片的详情,有个备注(经过base64加密的,先解码得到那个压缩包的密码)



4.解压之后得到一张图片,用winhex打开,修改宽和高的值一样,然后保存。再打开图片即可在图片上看到flag.



BUGKU{a1e5aSA}

MISC 24 爆照 关键字: binwalk foremost 知识点: 步骤: windows+kali 1.binwalk分析原文件, foremost分离, 解压后发现多个文件 2.在win下不知道是什么文件 但是在linux下系统会自动辨别 所以我们复制到kali里面



3.binwalk逐个分析文件 发现前三个有修改的痕迹,88,888,8888 88



c2lsaXNpbGk=	1 0000000.jp	og 属性
1	常规 安全	详细信息 以前的版本
	属性 说明 标题	值
	王题 分级	* * * * *
	标记	
L	备注	c2lsaXNpbGk=
	来源	
	作者	
	1日月月月月月月月月月月月月月月月月月月月月月月月月月月月月月月月月月月月月	
编码 base64	在 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	
	版权	
	图像	
	图像 ID	
	分辨率	303 x 299
	宽度	303 像素
	where entry	200 (4)=



MISC 25 猫片

关键字: LSB BGR ntfstreamsedtior StegSolve

知识点:

1.chr() 用一个范围在 range (256) 内的(就是0~255) 整数作参数,返回一个对应的字符。

2.ord() 函数是 chr() 函数(对于8位的ASCII字符串)或 unichr() 函数(对于Unicode对象)的配对函数,它以一个字符(长度为1 的字符串)作为参数,返回对应的 ASCII 数值,或者 Unicode 数值,如果所给的 Unicode 字符超出了你的 Python 定义范围,则 会引发一个 TypeError 的异常

3. uncompyle反编译pyc

pip install uncompyle

uncompyle6 文件名

步骤: windows+java+python

1.hint:LSB BGR 想到信息隐藏, 使用StegSolve提取

Alpha为什么不勾,因为是透明度,如果改为0就变成全透明,图片就什么也看不见,RGB是全为0,让它避免有其他颜色亮度的 干扰,如果RGB任意一个改为不为0,那么这张图片的代码就会出现错误,导致他不是一个图片文件。

当我们改好的时候 可以看见是一个png文件

📓 StegSolve 1.3 by Caesum	-	×		
File Analyse Help				
Norm File Format		 		
Data Extract				
Stereogram Solver				
Frame Browser				
			E 1 (D)	

Image Combiner	E XII dCI PIEVIEW	teres and the second
+ ~	1a0a0000000d4948PNGIF	I 🔺
	444154799ccddd51	
	ff5h761610145020 0 0d [+	2
2	acf1/1000bd/2f7c 7 7 7 3 2	2
	2-56ff-1f2f2f2f27f	
	80d573d8fdb0d3d7 2 ¥ a	
	bfcdeafe7ffee7fb Y W D	
	8404012141404810 ./TH	
	739b95dd39c3f4dc~ s9	
		
		Order settings
Victoria de la companya de la compan	6 5 4 3 2 1 0	Extract Row Column
The second se		
	6 5 4 3 2 1 0	Bit Order O MSB First I I SB First
	6 5 4 3 2 1 0	Rit Diana Ordan
a state of the sta		Bit Plate Order
	6 5 4 3 2 1 0	○ RGB ○ GRB
1 date and the second sec	\smile	⊖ RBG ⊖ BRG
		0.000
	de Hex Dump In Preview 🖌	GBR BGR
	Preview Save Text Save F	3in Cancel
		hilips#d og.csdn.net/dadongwudi

2.打不开图片。winhex打开,选中后右键删除头fffe,保存,发现需要修改高度,发现是一个二维码,扫描是一个百度云链接

89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	00	00	01	18	00	00	01	18	08	02	00	00	00	08	EC	7E	%PNG IHDR 1~
1	0	00	05	9C	49	44	41	54	78	9C	ED	DD	51	6A	1C	3B	14	40	C1	38	64	r r	эв	76	16	10	14	50	38	37	92	Û œIDATxœíÝQj ; @Á8dÿ[v P87'
EC	AA	DF	37	AF	DD	EE	F1	41	90	8B	D4	3F	7E	00	00	00	00	00	00	C0	9F	3E	56	S.F.	E1	F3	F3	F3	7F	DE	C7	ì°₿7 [−] ÝîñA <Ô?~ ÀŸ>Vÿáóóó ÞÇ
3F	FB	F8	58	FE	0A	89	D5	73	D8	FD	B9	D3	D7	59	A9	9E	CF	EE	FD	57	9F	BF	CD	1	FE	7F	FE	E7	FB	80	2F	?ûøXþ ‰ÖsØý¹Ó×Y©žĬîýWŸ;Íêþ þçû€/
49	48	10	10	12	04	84	04	01	21	41	40	48	10	10	12	04	7E	ED	FE	0F	D3	73	9B	95	DD	39	C3	F4	DC	63	FA	IH " !A@H ~ip Ós›•Ý9ÃôÜcú
E7	AE	9C	9A	5F	4D	7F	7E	FA	3A	BB	76	BF	17	2B	12	04	84	04	01	21	41	40	48	10	10	12	04	84	04	01	21	箜š M ~ú:≫v; + " !A@H " !
41	60	7B	8E	В4	52	ED	27	39	35	37	58	99	9E	F3	4C	EF	47	AA	AE	73	6A	7E	B5	7B	FD	5D	D5	FD	58	91	20	A`{Ž´Rí'957X™žóLïG®®sj~µ{ý]ÕýX`
20	24	80	80	09	02	42	82	80	90	20	20	24	08	08	09	02	D9	1C	E9	75	A7	CE	7F	DB	35	BD	AF	69	75	9D	53	\$ B,€ \$ Ù éu§î Û5½ iu S
E7	E9	BD	C2	8A	04	01	21	41	40	48	10	10	12	04	84	04	01	21	41	40	48	10	30	47	8A	9D	7A	5F	D0	6D	D7	çé½ÂŠ !A@H " !A@H OGŠ z_Đm×
99	9E	A7	DD	C6	8A	04	01	21	41	40	48	10	10	12	04	84	04	01	21	41	40	48	10	C8	E6	48	AF	CC	07	5E	39	™ž§ÝÆŠ !A0H " !A0H ÈæH Ì ^9
CF	AD	DA	2F	34	7D	6E	DE	A9	EF	FD	B6	BF	37	2B	12	04	84	04	01	21	41	40	48	10	10	12	04	84	04	01	21	Ï-Ú/4}nÞ©lý¶;7+ " !A@H " !
41	60	7B	8E	54	BD	97	E6	94	53	FB	6D	4E	7D	7E	E5	B6	\mathbf{EB}	EF	5E	E7	36	56	24	08	08	09	02	42	82	80	90	A`{ŽT≒-æ"SûmN}~å¶ëï^ç6V\$ B,€
20	20	24	80	08	09	02	42	82	C0	5D	9B	3A	1E	32	3D	27	99	7E	5F	D3	4A	35	47	DA	BD	FE	EB	AC	48	10	10	\$ B,À]>: 2='™~_ÓJ5GÚ½þë¬H
12	04	84	04	01	21	41	40	48	10	10	12	04	84	04	81	EC	5C	BB	EF	B6	FF	A4	DA	47	54	79	E5	3C	BA	E9	7D	" !A@H " ì\»ï¶ÿ¤ÚGTyå<°é}
50	95	DD	E7	63	45	82	80	90	20	20	24	08	08	09	02	42	82	80	90	20	20	24	08	8C	0F	13	4E	BD	8F	68	D7	P•ÝccE,€ \$ B,€ \$Œ N⁵s h×
EB	FB	7F	6E	9B	D7	9D	DA	D7	34	FD	FC	57	9F	Β7	22	41	40	48	10	10	12	04	84	04	01	21	41	40	48	10	10	eû n>× Ú×4ýuwr . AQH " !AQH
			Sec. 20.	-	-	-		10.000	-	10.00	10.00	1.000	-	-	Sec. 10.	-	Channel and		-	ALC: 100	10.000		-	_								



nttps://blog.csdn.net/dadongwudi

3.NTFS提示要用ntfstreamsedtior 一定要用winrar并且用ntsf导出pyc文件 ntfstreamsedtior下载链接: https://bbs.kafan.cn/thread-460084-1-1.html winrar下载链接: https://www.52pojie.cn/

し 家 約	;果:共9个;用时0.047 s				
*	文件	数据流名称	大小(字节)	可疑度 <mark>(0-5)</mark>	
	D:\CTF\MISC\file.png:Zone.Identifier	Zone.Identifier	158	0	
	D:\CTF\MISC\Stegsolve.jar:Zone.Identifier	Zone.Identifier	118	0	
	D:\CTF\MISC\welcome.jpg:Zone.Identifier	Zone.Identifier	158	0	
	D:\CTF\MISC\Xways Winhex 19.8 Professional License.z	Zone.Identifier	310	1	
	D:\CTF\MISC\ZipCenOp.jar:Zone.Identifier	Zone.Identifier	1299	1	
\checkmark	D:\CTF\MISC\flag\flag.txt:flag.pyc	flag.pyc	755	1	
	D:\CTF\MISC\汇	Zone.Identifier	156	0	
	D:\CTF\MISC\汇总\file(2).zip:Zone.Identifier	Zone.Identifier	156	0	
	D:\CTF\MISC\汇总\file.rar:Zone.Identifier	Zone.Identifier	156	0	
- 8	, 删除 一 🛛 顺 导出 一> 附加 +/ 导八 <	畲⒄ >>	22.原<<		导出列表

4.pyc编译成py

4.1 uncompyle

base) PS D:\CTF\MISC> pip install uncompyle

(base) PS D:\CTF\MISC> uncompyle6 .\D!_CTF_MISC_flag_flag.txt!flag.pyc >flag.py

4.2在线

https://tool.lu/pyc/

```
import base64
```

```
def encode():
    flag = '*********'
    ciphertext = []
    for i in range(len(flag)):
        s = chr(i ^ ord(flag[i]))
        if i % 2 == 0:
            s = ord(s) + 10
        else:
            s = ord(s) - 10
        ciphertext.append(str(s))
```

return ciphertext[::-1]

ciphertext = [

'96',			
'65',			
'93',			
'123',			
'91',			
'97',			
'22',			
'93',			
'70',			
'102',			
'94',			
'132',			
'46',			
'112',			
'64',			
'97',			
'88',			
'80',			
'82',			
'137',			
'90',			
'109',			
'99',			
'112']			

5.根据加密过程写脚本并运行得到flag

```
def decode():
    ciphertext = [
    '96',
    '65',
    '93',
    '22',
    '93',
    '70',
    '102',
    '94',
    '132',
    '46',
    '112',
    '64',
    '88',
    '80',
    '82',
    '90',
    '109',
    '99',
    '112']
    ciphertext.reverse()
    flag = ''
    for i in range(len(ciphertext)):
            s = int(ciphertext[i]) - 10
            s = int(ciphertext[i]) + 10
        s=chr(i^s)
        flag += s
    return flag
def main():
   flag = decode()
    print(flag)
if ___name___ == '___main___':
   main()
```

5.1在线运行 https://c.runoob.com/compile/6 5.2

(base) PS D:\CTF\MISC> python 4.py flag{Y@e_C13veR_C1Ever!}

参考链接: https://www.cnblogs.com/Paranoid-4/p/9502196.html

MISC 26 多彩 超出能力范围 关键字: YSL

步骤:

参考链接: https://blog.csdn.net/carlzj/article/details/82753478

参考链接: https://www.secpulse.com/archives/69465.html

MISC 27 旋转跳跃

关键字: MP3stego

下载地址: https://www.cnblogs.com/yangchas/p/7739874.html

步骤1.下载 MP3stego

2.Decode.exe -X -P syclovergeek sycgeek-mp3.mp3

	Flag Submit	D:/>cd ctf
		D:\CIF>cd MISC
	下载下来是MP3文件,用MP3Sstego分析一下看看	D:\CTF\MISC>1s '1s' 不是内部或外部命令,也不是可运行的程序 或批处理文件。
	首先你得百度下载MP3Sstego,然后安装之后 把题目给的mp3文件复制到安装目录下,打开命令行,cd到	安装 <mark>印:\CTF\MISC>java -jar Stegsolve.jar</mark>
	输入Decode.exe -X -P syclovergeek sycgeek-mp3.mp3	D:\CTF\WISC>cd MP3Stego_1_1_18
	C:\Users\Administrator.PC20140913QRD\Desktop\MP3Stego1116\Development\MP3Stego >Decode.exe -X -P syclovergeek sycgeek-mp3.mp3	D:\CTF\MISC\MP3Stego_1_1_18>cd MP3Stego
	C: Users Administrator.PC201409139RD/Desktop/MP3Stego1116/Development/MP3Stego >Decode.exe -X -P syclovergeek sycgeek-mp3.mp3 MP3StegoEncoder 1.1.16	D:\CTF\MISC\MP3Stego_1_1_18\MP3Stego MP3StegoEncoder l.1.17 See README file for copyright info Input file = 'sycgeek-mp3.mp3' output file = 'sycgeek-mp3.mp3.pcm' Will attempt to extract hidden information. Output: sycgeek-mp3.mp3.txt the bit stream file sycseek-ma3.mp3 is a BINAKY file.
I I I I I I I I I I I I I I I I I I I	go	HDR: s=FFF, id=1, 1=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
文件 主页 共享	查看	alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
← → ~ ↑ ↓ → 此	(电脑 > Data (D:) > CTF > MISC > MP3Stego_1_1_18 > MP3Stego	[Frame 5932]Avg slots/frame = 417.889; b/smp = 2.90; br = 127.979 kbps
	A	Decoding of "sycgeek-mp3.mp3" is finished
E (1)	各称	The decoded Fom output Tile name is sycgeek-mps.mps.pcm
ine(1)	Decoder	D:\CTF\MISC\MP3Stego_1_1_18\MP3Stego>D
MISC	Encoder	2015/12/12 12:16
share	Lables	2015/12/12 12:16
1 工具压缩包	Decode.exe	2006/6/13 7:38 🛛 🕘 sycgeek-mp3.mp3.txt - 记事本
OneDrive	Encode.exe	2006/6/13 7:39 文件(F) 编辑(F) 格式(Q) 音署(V) 帮助(H)
	hidden_text.txt	2000/11/30 12:13
A WPS网盘	MP3Stego.sin	2006/6/13 7:24
▶ 此电脑	README.txt	2015/12/12 12:25
3D 对象	Correspondence in the second s	2016/10/10 12:03
100 × 1046	svcgeek-mp3.mp3.pcm	2021/1/5 20:18
1 1963以	sycgeek-mps.mps.txt	2021/1/5 20:18
▶ 又档		https://blog.csdn.net/dadongwudi
- 1 下載		

MISC 28 普通的二维码 关键字: winhex 八进制转字符串

步骤:

1.winhex打开 拉到尽头

00002032	E E	E E	2.5	E E	2.5	E E	E E	E E	10	00	E E	E E	E E	E E	E E	E E	AAAAAAAAA AAAAAAA
00002848	FF	FF	FF	FF	FF	F0	00	FF	FF	YYYYYYYYYYYY YY							
00002864	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u> 222222222222222222</u>							
00002880	FO	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	8 9999999999999999
00002896	FF	FF	FF	FF	FO	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	99998 9999999999
00002912	FF	FO	00	FF	FF	FF	FF	\mathbf{FF}	FF	999999998 999999							
00002928	FF	FF	FF	FF	FF	F0	00	FF	FF	999999999999998 99							
00002944	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u> </u>							
00002960	FO	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	8 9999999999999999
00002976	FF	FF	FF	FF	F0	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	99998 9999999999
00002992	FF	FO	00	FF	FF	FF	FF	FF	FF	999999998 999999							
00003008	FF	FF	FF	FF	FF	FO	00	31	34	<u> </u>							
00003024	36	31	35	34	31	34	31	31	34	37	31	37	33	31	31	30	6154141147173110
00003040	31	34	31	31	36	36	31	34	35	31	33	37	31	37	31	30	1411661451371710
00003056	36	30	31	32	35	31	33	37	31	32	30	31	37	31	31	33	6012513712017113
00003072	37	31	36	33	31	34	33	31	36	32	31	35	31	31	36	30	7163143162151160
00003088	31	36	34	31	33	37	31	31	37	31	36	34	31	34	33	31	1641371171641431
00003104	33	37	31	32	34	31	35	37	31	33	37	31	32	34	31	34	3712415713712414
00003120	35	31	35	36	31	33	37	31	30	31	31	36	33	31	34	33	5156137101163143
00003136	31	35	31	31	35	31	30	34	31	31	37	35	40	78	6A	73	151151041175@xjs
00003152	65	63	6B	21													eck!

2.八进制转字符串

MISC 29 乌云的邀请码关键字: StegSolve 隐写步骤: windows1.打开 StegSolve java -jar Stegsolve.jar2.提取图片里面的信息

≦ StegSolve 1.3 by Caesum	× 🕨
File Analyse Help	
ormal Image	
您好:	
这是来自于WooYun的一封邀请邮件,非常高兴你通过WooYun发	Evtract Preview
http://www.wooyun.org/user.php?action=register&code=b	0017666c61677b50 6e675f4c73625f59flag{P ng_Lsb_Y 30755f4b306e7721 7dffffffffffffff 0u_K0nw! }
WooYun会给你发送一封确认邮件,可以点击其中的链接完成注册,	ffffffffffffffffffffffffffffffffffffff
漏洞处理流程: <u>http://www.wooyun.org/help#bug</u>	ffffffffffffffffffffffffff
白帽注意事项: <u>http://www.wooyun.org/help#whitehat</u>	IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
	Bit Planes Order settings
本邮件由WooYun自动发送,请勿回复	Alpha 🔄 7 🔄 6 🔄 5 🔄 4 🔄 3 🔄 2 🔄 1 🔄 0 🛛 Extract By 🖲 Row 🔿 Column
WooYun是一个自由平等的漏洞和安全信息报告平台 其他关于WooYun的更多详细信息请访问 <u>http://www.wooyun.or</u>	Red 7 6 5 4 3 2 1 Ø Bit Order MSB First Isse LSB First
谢谢!	Green 7 6 5 4 3 2 1 2 0 Bit Plane Order
	Blue 7 6 5 4 3 2 1 2 0 0 RGB 0 GRB
关键字:	Preview Settings
⊕ 知识点:	Include Hex Dump In Preview 🔽
は、北平・	

MISC 30 神秘的文件

关键字: 明文攻击 ARCHPR

知识点:

步骤: windows+Kali

1.压缩包和png图片,压缩包是加密的,并且那个图片存在于压缩包,于是将logo.png使用winRAR加密成zip,然后对比他们的 CRC32,发现一模一样!考点就是明文攻击。

明文攻击(不懂的参考http://www.cnblogs.com/ECJTUACM-873284962/p/9387711.html)



加密的 ZIP/RAR/ACE/ARJ 文件	攻击类型
C:\Users\hh\Downloads\file\flag.zip	明文
范围 长度 字典 明文 自动倒 明文选项 明文文件路径:	時 选项 高级
C: \Users \hh \Downloads \file \logo.zip	📄 - 开始于: 0 🛛 🍢
	bc1ad2b6 密钥 03bd7740 滑
□ 允许使用二进制文件作为明文 ZIP 相	当案文件
口令已成功恢复!	×
Advanced Archive Pas	sword Recovery 统计信息:
总计口令	n/a
总计时间	18s 415ms
平均速度(口令/秒)	n/a
这个文件的口令	q1w2e3r4
十六进制口令	71 31 77 32 65 33 72 34 🥢

2.binwalk查看,foremos分离后,找到flag.txt,打开得到一串

base64, 解码, ok, 得到flag

🥘 flag.t	xt - 记事本	z			
文件(F)	编辑(E)	格式(O)	查看(V)	帮助(H)	
ZmxhZ3	tkMGNYX	(zFzX3pp	UF 9maWi	1fQ==	

MISC 论剑 关键字: winhex binwalk 知识点: 1.base64, base32, base16 快速判断方法: 大写小写都有是base64,只有大写是base32,只有大写且最大只到F是base16 2.常见的文件头

```
7z
文件头标识: 37 7A BC AF 27 1C
JPEG/JPG
文件头标识:ff, d8(SOI)(JPEG 文件标识)
文件结束标识:ff,d9(EOI)
PNG
文件头标识: 89 50 4E 47 0D 0A 1A 0A
GIF
文件头标识: 47 49 46 38 39(37) 61 GIF89(7)a
BMP
文件头标识: 42 4D--- BM
HTML (html)
文件头标识: 68746D6C3E
ZIP Archive (zip)
文件头标识: 504B0304 PK
RAR Archive (rar)
文件头标识: 52617221
3.jpeg格式详解https://blog.csdn.net/yun_hen/article/details/78135122
```

步骤: win+kali

1.winhex到中部发现一串二进制进行进制转换,发现类似7z文件头37 7A BC AF,修改保存

这个图片中隐藏的不是常见的zip压缩包,是7z压缩包

位置就在二进制码的旁边

00<mark>8 (</mark>-''

标蓝的位置是7z的一个标志,但是这里文件头损坏了,所以binwalk没有分析出来

正常的7z头: <mark>7z≒</mark>-'.

https://blog.csdn.net/dadongwud

— ASCII与	赴制转换 j2进制、10	进制和16进制之间]相互转;2进制、8进制、	10进制、16进制	间及任意进制相互	转换
ASC	淵≓进制	进制转换(常	用) 进制转换(任意	蕉) ●		
	文本	mynameiskey!!	!hhh			Ŀ
	二进制	01101101 011 01101000 0110	(001 01101110 0110000) 1000 01101000	1 01101101 011	100101 0110100	清空 1 01110011 01101011 01100101 01111001 00100001 00100001 00100001
				_	ο×	h.
				1	9.8 x64 - / ×	
4 🕨 🧔						
pq						
15 16 17 6B 60 C5 9D F1 4F	18 19 1A 3E 70 70	1B 1C 1D 1E 11 4C 22 8B C9 31	A B ¤ā JÂAv1 o ËDSÊÂ	file.jpg D:\share		
25 00 4D 08 74 4E	0D 06 30 F1 3A 0B	7A 4C 26 5B 51 92 6E 48 51 D	S ~.Ø ² .<« È{`œ@ÑÔR† 3 ú; # 9\Õ#-07νùÂ	文件大小:	21.5 KB 21,990 字节	l.
C7 E1 07 00 0F DB 2B A0 D1 29 83 6D	40 7C 8C 51 42 00 33 53 9F FB B0 9F 3A D4 30	5 1 5 1 5 2 6 6 5 5 A 3 0 5 7 2 4 4 2 4 9 3 5 5 5 5 5 6 6 7 2 1	A E13 5 5 8 80 μV 3 XB° XN E'R'-ā\æ§> 1 "XyUmê goYJC ŽÜm 1 र±ÛÆkq Êô n@1 C « I@ CAC " €5. å	缺省编辑模式 状态: 撤消级数: 反向撤消:	原始的 0 暂无信息	
DF F9 C3 A0 56 B5 FC 39 7A	4D 46 74 3B CA 06 FA 4A 8B	01 11 FF 00 6 2B E0 71 55 A CE D7 9F 58 92	7 ¾ ů¶ *xOO₩Đ A E ¬}çð ŠÀ‡ Þ\$+Xx* J 2 QU °ÿ ŅŃĖÌ PÒ	创建时间:	2021/01/07 16:28:13	l.
B2 16 93 48 20 2A A8 94 40 30 B4 5F 21 21 21	78 D6 CF 87 CE AB 92 E1 07 70 BF 8F	BC D3 F6 CE 91 F5 88 00 65 E 6F 7F 54 58 20 FD 3A FF D9 30 21 31 30 20 32	 SH šwóö⁻¹GI¹004œ ~ðn,,©ŶùÅmHy qù à -¬0A¹, ùŶ â/ĐNöŸ j³Z,â yÈ ØÙCfó 110010011001 	最后写入时间: 属性: 图标:	2021/01/07 16:27:46 A 0	
31 31 31 30 31 31 31 30 31 30 31 30	30 20 30 30 31 30 20 30 31 30 30 30	30 31 30 30 30 30 31 20 30 31 31 31 31 30 30 31 20 30 31 31	1 01 01101101 0111001 0 110011 01101011 0 1 1 00100001 001000	模式: 偏移地址: 每页字节数:	文本 十六进制 47x32=1504	
30 30 38 15 1F D8	7B BC AF C3 E1 A9	27 1C 00 04 C	01000 01101000 01	当前窗口: 窗口台粉:	11	

2.foremost无法分离出7z,用dd分离

<mark>(d⊛kali</mark>)- _\$ binwalk <u>f</u> :	[/mnt/hgfs/share ile.jpg		
DECIMAL	HEXADECIMAL	DESCRIPTION	
9 9591 17569	0x0 0x2577 0x44A1	JPEG image data, JFIF standard 1.01 7-zip archive data, version 0.4 JPEG image data, JFIF standard 1.01	https://blog.csdn.net/dadongwudi

(d kali) - [/mnt/hgfs/share] \$ dd if=file.jpg of=7.zip skip=9591 bs=1 ^[[A记录了12399+0 的读入 记录了12399+0 的写出 12399字节(12 kB, 12 KiB)已复制, 2.24452 s, 5.5 kB/s (d kali) - [/mnt/hgfs/share] \$ dd if=file.jpg of=1.jpg skip=17569 bs=1 记录了4421+0 的读入 记录了4421+0 的写出 4421字节(4.4 kB, 4.3 KiB)已复制, 0.933102 s 4.7 kB/s

3.用之前的密码修改解密压缩文件得到一张图片



ijcz.jpg i ie.jpg	1.1	og																														
Offset	0	1	2	3	4	5	6	7	8	- 9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
00000000	$\mathbf{F}\mathbf{F}$	D8	$\mathbf{F}\mathbf{F}$	E0	00	10	4A	46	49	46	00	01	01	01	00	60	00	60	00	00	\mathbf{FF}	DB	00	43	00	08	06	06	07	06	05	08
00000032	07	07	07	09	09	80	0A	0C	14	0D	0C	0B	0B	0C	19	12	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20
00000064	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	39	3D	38	32	3C	2E	33	34	32	\mathbf{FF}	DB	00	43	01	09	09
00000096	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
00000128	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	FF	C2
00000160	00	11	08	02	6	02	6E	03	01	22	00	02	11	01	03	11	01	$\mathbf{F}\mathbf{F}$	C4	00	1B	00	01	00	02	03	01	01	00	00	00	00

ljc2.jpg	1.jpg	
Offset	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23	3 24 25 26 27 28 29 30 31 ANSI ASCII 🗚
00000000	FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 00 60 00 00 FF DB 00 43	3 00 08 06 06 07 06 05 08 ÿØÿà JFIF ``ÿÛ C
00000032	07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12 13 0F 14 1D 1A 1F 1E 1D	D 1A 1C 1C 20 24 2E 27 20 \$.'
00000064	22 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27 39 3D 38 32 3C 2E 33 34	4 32 FF DB 00 43 01 09 09 ",∔ (7),01444 '9=82<.342ÿÛ C
00000096	09 OC 0B 0C 18 0D 0D 18 32 21 1C 21 32 32 32 32 32 32 32 32 32 32 32 32 32	2 32 32 32 32 32 32 <u>32 32</u> 2! !222222222222222222
00000128	32 32 32 <u>32 32 3</u> 2 32 32 32 32 32 32 32 32 32 32 32 32 32	2 32 32 32 32 32 32 32 FF C2 22222222222
00000160	00 11 08 <mark>03 00</mark> 03 0D 03 01 22 00 02 11 01 03 11 01 FF C4 00 1B 00 01 00	0 02 03 01 01 00 00 00 00 "ÿÄ
00000192	00 00 00 00 00 00 00 04 05 02 03 06 01 07 FF C4 00 16 01 01 01 01 00 00	0 00 00 00 00 00 00 00 ÿÄ



666C61677B6D795F6E616D655F482121487D 5.base16解密

flag{my_name_H!!H}

快速判断方法:大写小写都有是base64,只有大写是base32,只有大写且最大只到F是base16

MISC Photo自我修养 关键字: 知识点: 步骤: MISC 成果狗成果狗 关键字: 知识点: 步骤: MISC 图穷匕见 关键字: winhex gnuplot 知识点: jpg的文件尾FF D9 步骤: 1.winhex查看, jpg的文件尾FF D9, 将之后的数据保存到txt中,使用的是notepad++中的插件Converter进行解码

File E	dit Search View Encoding Language Settings Tools Macro Run	Plugins Window ?			
B 🚽) 🔚 🖻 🗟 🕼 🌡 🖉 🛅 🗩 C 📾 🏣 🤏 🖷 💁 🖬 📕	MIME Tools	>	77. 	
🔚 ch	ange, log 🗙 🔚 heiheihei, jar 🗙 🔚 bugkul4qiumingshan, pv 🗙 🔚	Converter	>	ASCII -> HEX	
1	28372c37290a28372c38290a28372c39290a28372c3130;	NppExport	>	HEX -> ASCII	283
		Plugins Admin		Conversion Panel	
		Open Plugins Folder		Edit Configuration File	
				About	

2.去除"()," 匹配gnuplot格式

2.1 直接replace

2.2 python脚本



Replace		
Find Replace Find in Files Mark		
Find what :	~	Find Next
Replace with :	~	Replace
		D
	In selection	Replace All
		Replace All in All Opened
Backward direction		Documents
Match whole word only		
Match case		Close
Wrap around		
Search Mode		ransparency
Normal		On losing focus
Extended (\n, \r, \t, \0, \x)		○ Always
Regular expression matches	newline	
Replace All: 35019 occurrences wor	replaced in entire file billered (15)	
Replace Mil. 55019 Occurrences were	replaced in entire me Thtps://b	

gnuplot 使用gnuplot, 扫码得到flag sudo apt-get install gnuplot



MISC convert 关键字: convert 知识点: 步骤: win anaconda 1.脚本2进制分组转换成16进制 f1 = open('1.txt','r') fw = open('2.txt','w') fw.write(hex(int(str(f1.read()),2))) f1.close() fw.close() #2 f1=open('1.txt','r') oct1=int(f1.read(),2) #十进制转16进制 hex1=hex(oct1) #将十六进制文件写入文件 f2=open('out.txt','w') f2.write(hex1) #关闭文件 f1.close() f2.close()

	Users\Administrator\Desktop\out.txt - Notepad++ [Administrator]		4.4		
文件(F)	編辑(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) ?			
6	🗄 🖻 💫 🕼 🏑 🗅 🜔 🤉 🕊 🏙 🍢 🤏 👒 💁 🖼 🚍 1 🏢	DSpellCheck	•	💌 🖬 🛛 🥸	
🔚 1. t	xt 🔀 🔚 out. txt 🔀	MIME Tools	- + _		
1	526172211a0700cf907300000d00000000000000000f7c07420902c000d0900005922000	Converter	+	SCII -> HEX	4a319101
	9a944daa0a0da68b3426cb02cc44d29a1445404474882209a501d06c541151431310: 889aaaf09889c7f463fec0d2adabad2b8036580df85e031fd3a5ac567c6f6dcc2b8b6	NppExport	•	IEX -> ASCII	33c4fb913 2966e1463
	62c5b23eba3e058b64559980e407c03704f4b03c01ec0b806502b0090374599029f9 d692e0ead84053d6c52860a4722f0dee798d696d6052daf2b7d07a4c1bae4814d6d8	Plugin Admin	0	Conversion Panel)4f5d0a7e 287b5ba70
	1bdf494a8c29bdaf3032ecd7062e3aaab63737acbebbb630beee989a9f5c5a939ad18 b24163068b1a352422a92f049ccbf1f124bbd0d085e6822ffe2404ae2bfb01a3e4058b	29690d541f13df1c9 6473fb8d1f202c58b	15c8) 547a: E	dit Configuration File	284e1684a)2a804999
	cf8f852225230a424843cc28fb4d7240cd8ecb2841464e514d1aa09497b21ba16018d3 61758730310e646462621557e0ab80c4e8cb4dacd8aa19e9d7c78842763b1b0315d312	242f6373dd2690f46e 87b6ec77b50c15b7c8	ab0fl A	bout	:0e8307cb
	0f245e9edf093ec1f1212161a1f8bc68b8ce5c6f323b9bcee7c97524e53ab2b2d2f31c 90e7ab9eb1888cac6627bd028745c39eb19e99517c40f76d3a1161277b6cf672434434	19ed4ecf4fd050d1510 1660bed416adcf55130	13f7fcle1a 55e945bfd0	8f178ea6aa c6ffd47f4f1a	237312C1b87c
	92562899a55df576ff9526b3d394b3e1dfa8cb07a5d5e372fc8a74b070b691f71aac3b	099fced19faa473a9	43074532:	one de la serie de la conseil de	inib@accele#10e
	-IUd656cdUc164adeab512456b5da8b1532648cded71312d18c6471491c949c814b28d8	19/1baalafc16e9a9a	12641063c3	59a5ce909a258e0f01b26	e0e2b455576a2

3.转成ASCII码之后,看到开头Rar!,很明显的rar文件头,修改文件后缀为.rar

🔚 1. t	ut. txt 🛛
1	
2	NULNULNULNULNULNULREN XCO+ XEO, NUL
3	NULNULY" NULNULSTX>cp BM
4	YRESJES3 BED NUD NUD NUD key. jpg NUD RF0 DC4 RAS OM DD5 (S R91 NAK (S R91) R90 NAK REA
	x9AP(S)ACK(xC5ANAK(DC4)11SOHEOTM] xC6xC0PxB5DFFDC4xB4DLE; SYNBELD1SO(SIqxBBDC1)
	xF4cxFExC0xxABxAD+x806X
5	xf8^STXIUS%RAGV 0mxCC+X8Bx80:(DC2NUDxF0xCDxE01xG2CENQSTXx97FCAxE0p、xADENQ
) f x21 f 7 \$ Soh x71 0 x31 : > Eng x33 d [x74 VT SYN - x91 xA0 05 xC2 # x32 % h x78 SYN , [# x33 xA3 x20 1
	- 513 22001
6	~cR30\$\$pR39\$00}}RCG.yD\$R39>0830+*1.R30'R330'R38088R3808(`R34r/

4.解压后得到图片key.jpg,属性查看

- base编码

base16, base32, base64



MISC 听首音乐 关键字: audacity 摩斯密码 步骤: 1.下载,解析

····· ···· ····		,					
T) 生成(G) 效果(C)) 分析(A) 工具(O) 帮助(H) -48 -42 -	(卢击开始监视)4	-18 -12 -6	o'	-54 -48 -42	-36
efinition ✓	2 (立体声) 录制声道		● · · · · · · · · · · · · · · · · · · ·	Definition			१.
1:10.0	1:11.0	1:12.0	1:13.0	1:14.0	1:15.0	1:16.0	1:
					https://blog.c	isdene <mark>ct/di</mark> solemig	w4 <u>10</u> i-

.---- ----. .---- -.-.

在线转换一下就是5BC925649CB0188F52E617D70929191C

MISC 好多数值

关键字: PLL RGB

步骤:

1.看到的第一反映就是RGB值,需要通过这些值来重构图片,但是仅有像素的RGB值是不行的,我们还必须要知道此图像的尺 寸,即每行每列各有多少像素

-....-

粗略的研究一下这些数据就能够发现,在其中的某一段呈现出有规律型的变化

计算出行列 3219-3098+1=122 61366/122=502

3094	255,255,255	3216	255,255,255
3095	255,255,255	3217	255,255,255
3096	255,255,255	3218	255,255,255
3097	255,255,255	3219	<u>255,255,255</u> ^尾
3098 <mark>≯</mark>	255,255,253	3220	255,255,248
3099	255,253,251	3221	255,254,235
3100	255,249,235	3222	255,249,211 log.csdn.net/dadongwudi

61365 255, 255, 255 61366 255,255,255 61367



c.show()

flag{ youc@n'tseeme }

MISC 很普通的数独

关键字: 二维码

知识点:常见二维码除了右下角其他角都有框框

步骤:

1.解压观察,换位置调整,第21张换到第1张的位置,第1张换到第5张的位置,第五章换到第21张的位置,还原,脚本还原二维码

•	未	柡	迈- ⁻	1@	66	5.79	% (l	图	쿮 2	5, F	RGE	3/8)*																										Į	_				×	:
	0		_			1				_	2		. 1			3		. 1			4				<u></u>	5		. 1			6		. 1		<u> </u>	7, ,		<u>.</u>			8				
	3		2	7	5	6	4	1	8		9		7		6				3		2						8	3	9	2	7	5				Т	3		7	! !	5		4		T
			8						6	4			3	9	2	5		δ		1			9	2	5		6	4		_		9	2	_	6	ò								6	
			7		4	1	2		3	6	5			4	1	2	9	3		5			4	1	2	9	3	6		7				2	- 0	3	6 5		7 8	3 4	4	1	2		
	5		6		3	9	7		2	5		6	1				4				6		3						8	6	1	3			- 2	2	5						7	2	
	1		9		7	8	6		5		2	9	4			6					9	4	7	8	6		5	1	2	9	4	7	8		3 5	5	1	1	9 4	E i	7		6	5	
1			4						1	7			2							3	4		_		9	_				4	2	6		9			7		4 2	1 1	6		9		
	2		3	5	8	4	1	6	9		7		5		4		6		2		3		8		1		9		7		5		4		6		2	1	3 5	<u>;</u> [8		1		
	9										4	5			3	8		7			5				8	2		9			δ	1			2	7	9						8	7	
				9		7	3	5	4	8			9					4	8	6	1	9	2	7	3			8			9		7				8 8		19) (2	7	3	4	
	3		2			6			8		ô	2	7	5	6	4	1	8	3		2	7	5		4		8		9	2	7	5		4	8	3	3	1	2		1	6	4		
	4						5	7	6	4			3			5						3	9				6	4		8			2	5	E	à	1					2		7	
			7	8				9			5	7		4				3		5			4	1				б							9		6 5				4				
		8		1	3		7		2		8				9	?	4	2	5	8		1				4	2	5		6			ô.	7	4	Т	5	1	6 I			9	7	4 2	
	1				7	8				1				7	8	6			1	2	9		7	8	6		5	1		9	4			6	Ę	5	1	1	9 4	Į :	7	Т		5	
			4	2			9	8		7										3			6					7	3	4	2			9	1	L	7		4	1	6	5		8	
	2		3						9	Γ	7	3		8		1	6	9	2	7			8	4		6	9	2	7	3	5		4		()	2 7	·	5	;		Т		6 9	
	9	4		6	1	3	8	2		9	4	5		1	3			7	9		5	6				2		9					3	В	2				e	i					
	8	6		9		7					6		9		7					6	1	9		7	3		4	8		1	9	2		3	- 4	4	8		1			7	3		
		9			5	ĥ	4	1	8	3	9				6		1		3	9	2		5			_	8					5	6		1 8	3	3		2 7	,	7	6	4		1
		1	8		-	2	-	7	6			8		9		5		6	4				9	2	5	7		4		8			2	5					8	1	9			7	1
		5	-	8	4	1	2	9	3	6	5	7	8		1		9	3	6	5	7	8	4	1	2		3	6		7	8		1	2	9 3	3	6 5		7 8	3 /	4	1	2	-	1
		8	6	1	3	-	-	,	2	5						7					6				7		2				1		1	7		╢	5		+	1	3	9	7	4	1
	1	2	9	4	7	-	6		5	1	2			7	8	6			1	2	9		7		6	3		1			4	7		6			1		9	1	7	T		3	1
	7	3	-	-	6		Ť		1		3	4	2		5		8	1	7		4				9	8	1	7						-	8 :	1	7	+	-	1	6	+	-	-	1
	2	Ť	3		8	4	1	6	9	ſ	7	3	5			1	6	9	2		3	5	8	4	1	6	9	2					4		6	╢	2 7	1	3 5	; ;	8	+		6	1
	9	4	-	6	-	-	-	2	7				6	1	3				9			6	1	3	8		7	9		5	6	1	3	8		7			e	5				2	1
-	8	6	1	9		7	3	5	4	8	6				7			4					2	7		5		8	6				7	3	5 4	1	8 8		ę	1	2	7	3	5	1
	F	9	2			ĥ		1		3		2				4	1			9		7	_			1				2			╡	4	5	2	3		2	1	5	肀	_	8	1
		1	8	3		2	5	7		4		8	3		2	5		6	4			3				-	6	4		8	3		2	-	-	1	4 1		8 3	2	-	2	+	6	
	6	5	0	2	4	-	Ľ	Ľ	3			7	8		1	2			-	5		8		1	2		3	6	5	7	8	4	~	2	-	t	6		7 8	ł	÷	~	2	9	
	Ĕ	- ×			2	9	7	-	-	5	8	6										1	_	-	-	_	2	Ľ	8	÷	1	-	9	7	4 3	2	5	T	Ŧ		3	+	-	4	1
	1	2	9		7	-		3			2	9	4	7			3	5	1		9	4	7			3	-	1	-		-		8	÷	3 5	s II	1 2		a	Ť	7	+	+	3	1
6 -	7	-	4			Б	a	0			3		2	6	5	9	8	1	7	3	-	2	-			-		7					5		8		7		4	1	6	\pm	9	-	
	Ľ.	-	-4		8	0	5	6	9			3			4	1		9	2	7		5		4			9	2	7	3	5		Ť	1	-		2 7		3 5	÷Ť	÷ –	4	1	ç	
					1		8	2	7	9		5	6	1				7	9		5	~	1	3			×	Ľ	-	5	Ű			8		7	9 4		Ĩ	Ť	+	1	8	2	
		6	1	q	2		0	5	4		6		9				5		8		-			-		5	4		6	1						1 I	8 6		Ť	1	2	+	-	-	
	2	0	9	7	5	6	4		0	3			-		6	4		8	3	9	2	7	5	6	4	·	8	3	-	-	7		6	4	1	╞	2 0			ŧ	E	╪	+	1 0	
	4	3	2	1	5	0	14 5		6	4	1	R	3	9		5		6	4		2			Ť	5		6	Ľ	1	8	3		Ť	5	1	╢	4	+			0		+	7 0	
	4		7	0	4	-	2		9	Ť	5	7	8	4	1	Ľ	9	3	-	5	7	-	4		2		3	6	1	7	8	4		~	9 3	2	*	÷	7	\pm	9 1 A	-	-	0	
	5.0		1.1	C2	- T		· ~				100									- N.F																- 11	5.1 L				-	- E	164 L	- A	- 100 P

	5		6	1	3		7	'	2	2	5	8		1		9	?		2	5		6				7	4	2	5	8			3				2	5				3			2	:
	1		9	4	7		6	5		1		2	9	4					5	1	2	9	4	7	8	6		5	1		9			8				1	2	9	4	7	8	:	3 5	
	7						9		1	1	7	3		2	6	5	9		1	7		4						1			4	2		5	9				3	4	2		5	9	1	
	2	7	3	5	8	4	1		ģ	3					8	4	1		9	2					4	1		9		7		5	8			6			7			8			9	, I
		-			-	-						4	5			3		2	7	9	4	5		1	3			7		4	5					2	7		4		6	1				
	8	6			2	7	3	3				6		9		7			4	8	6	1		2	7	3	5	4	8		1	9		7	3	5					9		7	3	4	
66	.67	%			文	[档	:3.	.051	M/1	100).7	М			\rangle																	ш	ιµι	ង្វារ	s LAN	Dβ	μy	505	wir	I₿	iet	φ <u>ia</u>	AU.	ນາຍ	FWC	7 @)

0 - 1 - 2 - 3 - 4 - 5 - 6 - 8 . 9 7 6 - 8 3 9 2 7 5 0 3 2 7 5 0 3 2 7 5 0 3 2 7 5 0 0 2 5 6 4 0 2 5 6 4 0 0 2 5 6 4 0 0 2 5 6 4 1 0 2 5 6 4 1 0 2 5 6 4 1 0 2 5 6 1 0 2 7 5 1 0 2 3 0 1 <th1< th=""> <th1< th=""> <th1< th=""></th1<></th1<></th1<>	4 1 8 6 2 3 7 2 6 5 1 6 9 3 5 4 4 7
3 9 2 7 5 6 4 8 9 7 6 - 8 2 - - 8 8 9 2 7 5 - - 8 8 9 2 7 5 - - 8 8 9 2 7 5 - - 8 8 9 2 7 5 - 8 7 5 - 8 7 5 - 8 7 5 - 8 7 5 - 8 7 5 - 7 5 - 7 5 6 1 7 6 7 5 6 1 1 2 9 3 6 7 8 6 1 3 7 6 6 7 8 6 1 3 7 6 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	4 1 8 6 2 3 7 2 6 5 1 1 6 9 3 5 4 4 7
4 - - 5 - 6 4 - 3 9 2 5 6 4 - 9 2 5 6 4 - 9 2 - 6 - 7 8 4 2 3 6 5 4 1 2 9 3 6 - 7 4 1 1 2 9 3 6 - 7 4 1 1 2 9 3 6 - 7 4 1 1 2 9 3 6 7 8 6 1 3 7 4 1	6 2 3 7 2 6 5 1 1 6 9 3 5 4 4 7 7
6 7 8 4 2 3 6 5 4 1 2 9 3 6 7 4 1 1 2 9 3 6 7 - 2 3 - 7 4 1 1 2 9 3 6 7 - 2 3 - 7 4 1 1 2 9 3 6 7 - 2 3 - 7 4 1 1 1 3 - 2 3 5 1 9 3 6 7 - 4 1 6 - 6 3 4 - 6 5 1 2 9 4 7 8 6 5 1 2 9 4 7 8 6 5 1 2 9 4 7 8 6 5 1 8 7 8 8 1 8 1 8 8 1 9 7 7 8 8	2 3 7 2 6 5 1 1 6 9 3 5 4 4 7
5 6 1 3 7 2 5 6 1 - - 6 3 - - 8 6 1 3 - 2 5 6 3 9 1 9 4 7 6 2 9 4 - 6 3 - 0 4 7 8 6 5 1 2 9 4 7 8 6 5 1 2 9 4 7 8 6 5 1 2 9 4 7 8 6 5 1 2 9 4 7 8 6 5 1 2 9 4 7 8 6 5 1 2 9 7 8 4 4 4 4 4 4 6 4 8 8 8 8 8 8 4 4 4 8 6 1 9 7 8 4 8 6 1 9 7 8	7 2 6 5 1 1 6 9 3 5 4 4 7
1 9 4 7 6 - 2 9 4 6 - 9 4 7 8 5 1 2 9 4 7 8 7 8 5 1 2 9 4 7 8 7 8 6 5 1 2 9 4 7 8 7 8 6 5 1 2 9 4 7 8 8 1 9 7 8 4 7 8 8 1 9 7 5 4 6 2 3 5 8 4 7 8 8 1 9 7 5 4 8 4 1 9 7 5 4 8 4 7 8 7 8 8 1 9 7 7 8 9 7 8 4 8 1 9 7 8 8 1 8 1 8 1 8 1 8 1 8 1	6 5 1 1 6 9 3 5 4 4 7
1 7 2 7 2 7 5 4 6 2 3 4 1 9 7 5 4 6 2 3 5 4 6 2 3 6 9 7 5 6 4 6 2 3 6 1 9 7 5 4 6 2 3 5 6 1 9 7 5 4 6 2 3 5 8 4 9 7 5 4 6 2 3 5 8 4 9 7 5 4 6 2 7 5 8 9 7 5 8 9 7 7 6 9 7 7 6 1 9 7 5 4 8 6 1 9 7 5 4 8 9 7 5 4 8 9 7 6 1 9 7 5 4 8 1 1 1 1 1	1 6 9 3 5 4 4 7
2 7 8 8 4 1 0 4 5 7 6 1 9 1 0 4 0 0 7 0	3 5 4 4 7
2 6 2 7 3 4 8 6 1 9 7 3 4 8 6 1 9 7 3 4 8 6 1 9 7 3 4 8 6 1 9 7 3 4 8 9 2 7 5 4 8 9 7 5 4 8 9 2 7 5 4 8 9 2 7 5 4 8 9 2 7 5 4 8 9 2 7 5 4 8 3 2 6 6 4 8 9 2 7 5 4 8 3 2 6 6 4 8 9 2 7 5 6 1 2 6 6 4 8 3 2 6 6 1 2 3 5	3 5 4 4 7
3 2 - 6 - 8 9 2 7 5 6 4 1 8 3 2 7 5 4 8 3 2 7 5 4 8 9 2 7 5 4 8 3 2 7 5 4 8 3 2 7 5 4 8 3 2 7 5 4 8 3 2 7 5 4 8 3 2 7 5 4 8 3 2 7 5 4 8 3 2 7 5 4 8 3 2 7 5 4 8 3 2 7 5 4 7 8 7 5 5 7 4 7 8 7 4 3 5 4 1 8 7 4 7 8 7 4	4 7
2 4 5 7 6 4 3 5 4 1 6 4 8 2 5 6 1 2 2 7 8 9 5 7 4 3 5 4 1 6 4 8 2 5 6 1 2 2 8 1 3 7 2 8 9 7 4 2 5 8 1 6 9 7 4 5 6 1 9 6 5 4 1 9 1 9 4 5 6 1 9 4 7 4 9 4 6 5 1 9 4 7 4 7 9 1 9 4 7 4 7 4 7 8 6 5 1 9 4 7 4 6 5 1 9 4 7 4 6 5 1 9 1 7 4 6 5 <td>7</td>	7
2 7 8 9 5 7 4 3 5 4 1 5 6 9 6 5 4 4 8 1 3 7 2 8 9 7 4 2 5 8 1 3 5 6 4 2 5 6 9 7 4 5 6 1 9 4 1 9 4 5 6 1 9 4 1 9 4 5 6 1 9 4 7 4 7 8 1 1 1 2 9 7 8 6 1 9 4 7 8 1 9 4 7 8 1 9 1 1 9 4 1 1 9 4 1 9 4 1 9 4 1 9 1 9 4 1 9 4 1 1 9 1 1 9 4 1 1 1	
8 1 3 7 2 8 9 7 4 2 5 8 1 5 6 9 7 4 5 6 1 9 1 7 8 1 7 8 7 8 7 8 1 9 7 8 6 5 1 9 4 7 8 7 8 1 1 2 9 7 8 6 5 1 9 4 7 8 7 4 7 8 7 1 2 9 7 8 6 5 1 9 4 7 8 7 4 7 8 7 1 2 9 7 8 6 5 1 9 4 7 4 7 4 7 4 7 4 7 4 7 4 7 4 7 4 7 4 7 4 7 4 6 5 7 3 4 2	
1 7 8 1 7 8 6 1 2 9 7 8 6 5 1 9 4 6 5 1 9 4 7 9 4 7 9 4 7 9 4 7 9 4 7 9 4 7 9 4 7 9 4 7 9 4 7 4 6 5 1 9 4 7 4 6 5 1 7 4 6 5 1 7 4 6 5 1 7 4 6 5 1 7 4 6 5 1 7 4 6 5 1 7 4 6 5 1 7 4 6 5 1 7 4 6 5 1 7 4 6 5 1 7 4 6 5 1 7 4 6 5 1 7 4 6 5 1 7	7 4 2
4 2 9 8 7 3 6 7 3 4 2 9 1 7 4 6 5	5
	8
2 3 9 7 3 8 1 6 9 2 7 8 4 6 9 2 7 3 5 4 9 2 7 5	6 9
9 4 6 1 3 8 2 9 4 5 1 3 (19 5 6 2 9 3 3 8 2 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	2
	3
9 5 6 4 1 8 0 7 0 4 3 9 2 0 6 6 0 2 5 7 4 0 0 5 0 1 8 3 2 1 0 0	4 7
	2
4 8 6 1 3 2 2 5 7 6 7 2 1 7 7 5 3 9	7 4
1 2 9 4 7 6 5 1 2 7 8 6 1 2 9 7 6 3 1 4 7 6 1 9 7	3
7 3 6 1 3 4 2 5 8 1 7 4 9 8 1 7 8 8 1 7 6	
2 3 8 4 1 6 9 7 3 5 1 6 9 2 3 5 8 4 1 6 9 2 4 6 2 7 3 5 8	6
9 4 6 2 7 6 1 3 9 6 1 3 8 7 9 5 6 1 3 8 7 6	2
5 8 6 1 9 7 3 5 4 8 6 7 4 2 7 5 8 6 7 3 5 4 8 6 9 2 7	3 5
9 2 6 1 3 2 4 1 9 7 1 2 4 8 3 2 5	8
1 8 3 2 5 7 4 8 3 2 5 b 4 3 6 4 8 3 2 4 1 8 3 2	6
	2 9
	2
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	9
	1 9
1 8 2 7 9 5 6 1 7 9 5 1 3 5 8 7 9 4 6	8 2
6 1 9 2 5 4 6 9 5 8 5 4 6 1 4 8 6 2	
3 7 5 4 3 6 4 8 3 9 2 7 5 6 4 8 3 7 6 4 1 3 9 2 7 5	1 8
6 4 1 8 3 9 5 6 4 8 5 6 1 8 5 4 9 2	7
6 5 7 8 4 1 9 3 5 7 4 2 3 6 7 8 4 9 3 6 7 4 1	2 9
5 7 2 5 8 1 9 7 2 5 6 7 4 2 5 8 3 2 5 3	2
1 9 4 7 6 5 2 9 4 5 1 2 9 4 7 8 6 5 1 9 8 1 2 9 4 7 8 6 5 1 9 8 1 2 9 4 7 8	3 5
	9 1
	9
8 6 1 9 2 7 3 4 6 9 7 4 8 6 1 2 7 3 5 4 8 1 9 7 3 5	3 4
66.67% 文档:3.05M/104.0M) 110,05M/104.0M	

```
from PIL import Image
x = 45
y = 45
im = Image.new('RGB', (x, y))
white = (255, 255, 255)
black = (0, 0, 0)
with open('数独.txt') as f:
    for i in range(x):
        ff = f.readline()
        for j in range(y):
            if ff[j] == '1':
                im.putpixel((i, j), black)
            else:
                im.putpixel((i, j), white)
im.save("数独.jpg")
```

2.不断base64 得到二维码,扫描得到 Vm0xd1NtUXIWa1pPVIdoVFIUSINjRIJVVGtOamJGWnIWMjFHVIUxV1ZqTIdNakZIWVcxS1lxTnNhRmhoTVZweVdWUkdXbVZHW khOWGJGcHBWa1paZWxaclpEUmhNVXBYVW14V2FHVnFRVGs9 base64解密一次 Vm1wSmQyVkZOVWhTYTJScFRUTkNjbFZyV21GVU1WVjNWMjFHYW1KR1NsaFhhMVpyWVRGWmVGZHNXbFppVkZZelZrZ DRhMUpXUmxWaGVqQTk= base64解密两次 VmpJd2VFNUhSa2RpTTNCclVrWmFUMVV3V21GamJGSlhXa1ZrYTFZeFdsWlZiVFYzVkd4a1JWRlVhejA9 base64解密三次 VjlweE5HRkdiM3BrUkZaT1UwWmFjbFJXWkVka1YxWlZVbTV3VGxkRVFUaz0= base64解密四次 V20xNGFGb3pkRFZOU0ZaclRWZEdkV1ZVUm5wTldEQTk= base64解密五次 Wm14aFozdDVNSFZrTVdGdWVURnpNWDA9 base64解密六次 ZmxhZ3t5MHVkMWFueTFzMX0= base64解密七次 flag{y0ud1any1s1}

MISC color 关键字: stegsolve hex 步骤: 1.组合起来 Make Me Tall

2.发现提交不了,hex修改高度

自动	1. pn	g ŧ ×														
: 编辑	为: 十	-六进	<u>ŧ</u> 制()	H) ~	运	行脚	本 ~	⁄ 运	行棋	観し、						
	Ò		2		4	5	Ģ	7	8	9	Ä	B	Ċ	Ď	Ę	Ę
000h:	89	50	4E	47	0D	A 0	1A	A 0	00	00	00	0D	49	48	44	52
010h:	00	00	01	90	00	00	01	$\mathbf{F}\mathbf{F}$	80	06	00	00	00	D0	D1	F7
020h:	A 8	00	00	00	04	67	41	4D	41	00	00	D8	EB	F5	1C	14
030h:	AA	00	00	00	20	63	48	52	4 D	00	00	87	0F	00	00	8C
040h:	0D	00	00	F9	93	00	00	84	E5	00	00	7B	82	00	00	EB
050h:	75	00	00	3F	в4	00	00	22	58	75	6B	5E	9C	00	00	04
060h:	18	69	43	43	50	6B	43	47	43	бF	6C	бF	72	53	70	61
070h:	63	65	47	65	6E	65	72	69	63	.52	47	42	00	00	48	.C7.
080h:	8D	55	5D	68	1C	55	14	3E'	BBa	nel Ar	nende:	23	24	ΨĒ.	땡띪	worken

3.最后一行 白0 黑1 转化

1100110 对应 f 102 66 https://011001101n fiet/dadengwudi

c1 = '11111111010111101111'
c2 = '1111101111110111111'
c3 = '0000110010101010001'
c4 = '01001010010000001101'
c5 = '11010011011101010111'
c6 = '10011011011010110'
c7 = '0011100110110111101'
flag = ''
for i in range(0,20):
<pre>c = c1[i]+c2[i]+c3[i]+c4[i]+c5[i]+c6[i]+c7[i] flag += chr(int(c,2))</pre>
print flag

参考链接: https://blog.csdn.net/qq_42777804/article/details/98974287

MISC 怀疑人生

关键字: archpr foremost psytec QR code editor

知识点:

步骤:

1.ctf1 ,使用archpr字典或暴力破解 密码是password,解压后base64,[ascii转unicode],(http://www.jsons.cn/unicode),得到 flag{hacker

2.foremost解压, ook编码, base58转码,得到 misc

	This tool can run programs written in the <u>Brainfuck</u> and <u>Ook!</u> prog	€在线工具 SSL在线工具 SSL漏洞在线检测 工具网 哭证书
■ cf2.8at - 12## - - × 文件() 编辑的 地致(0) 重要(0) 电影(0) - - ×	output. It can also take a plain text and obfuscate it as source code languages. All the hard work (like actually understanding how those languar and his Brainfuck interpreter in PHP	Base58编码 在线base50编码, 在线base50编码, base50编码, base50斜码, base50check 3ob54e
< >>	Test to Oold Test to short Oold Oold to Test Test to Brainflick Brainflick to Test The source can be found at github.	構式 BASE58_STRING (学校 マ 学符集 utf8(unicode编码) マ 編 码 解 码 nisc https://blog.codn.net/tiadongwou

flag{hackermisc12580}

MISC 红绿灯 关键字: Stegsolve PIL 步骤 1.Stegsolve分析发现一共有1168帧图片

2.一帧一帧查看发现多数是红色和绿色,偶尔有黄色且(每8个红绿后跟一个黄),可以推测红色和绿色对应二进制0和1,黄色 作为分隔,这样第一个黄灯之前数值为01100110或10011001,而01100110二进制转成ascii对应字符就是'f',依次可以验证前四 个字符为flag

其中有红色,绿色,还有少部分的黄色,相对应的应该对应1、0、空格,再转换成字符串即可,脚本如下。

用画图定位到红绿灯所在坐标(是一个区域,随便取一个判断颜色值来确定该帧是红灯还是绿灯),红灯为(115,55),绿灯为 (115,150),输出该坐标下的颜色值发现为红灯是颜色值是251,为绿灯时颜色值是186

```
from PIL import Image
im = Image.open("1.gif")
binstr = ""
flag = ""
for i in range(2,1168,2):
    im.seek(i)
    tmp1 = im.getpixel((115,55))
   tmp2 = im.getpixel((115,150))
   if(tmp1 == 251):
        binstr += '1'
   elif(tmp2 == 186):
        binstr += '0'
       binstr += ' '
for i in range(0,len(binstr) - 1,9):
    flag += chr(int(('0b' + binstr[i:i+7]),2))
print(flag)
```

flag{Pl34s3_p4y_4tt3nt10n_t0_tr4ff1c_s4f3ty_wh3n_y0u_4r3_0uts1d3}

MISC 不简单的压缩 关键字: Flash Decompiler winhex foremost 暴力破解 字典爆破

步骤:

1.winhex观察 发现有两个PK头,foremost分离

<pre>(d❀ kali)-[/mnt/hgfs/share]</pre>	▶ 固定到快 速访问	复制	米占贝占	№ 复制路径 記 粘贴快捷方式	移动到 复制
foundat=flag.swf2 0a∏VS00&000:0d0010000j0708i00000lh0s∭0 9∰0 H?30A60AS0000@00U0#0;0000D10+0<700)0cVF00000'K0a^w00 T0070.2.0i0b000c 0LS01000i0\0ip2050(00b00000000000000000000000000000000	$\leftarrow \rightarrow$	· 个	剪贴板	。 此电脑 》 Data (E) > share >
~10070+?u0j0n000<,01&0j000j0)01B20E0/00n00000 0040[0n00 0^c00,g-00000Wv00t0W000 0X 00l/<0 foundat=tingshuo.txt00Q0%0hB000Xc+00 00j0/00`20000p0f00	📌 快速	速访问		▲ 名称	^ 000 zin
* hon-pip-whl (20.1.1-2)	<mark>▶</mark> 桌	面	*	100000	797.zip ^{adongwudi}

archpr自带字典破解小压缩包,得到txt文档,翻译

加密的 ZIP/RAR/ACE/ARJ 文件 D:\share\output_Mon_Jan_11_18_38_	□ 攻击类型 20.
口令已成功恢复!	×
Advanced Archive F	Password Recovery 统计信息:
总计口令	21
总计时间	18ms
平均速度(口令/秒)	1,166
这个文件的口令	0
十六进制口令	30 🕜
	https://blog.c V 确 定ət/dadongwudi

```
パスワードは50桁だそうです
密码是50位数。
```

2.密码是50位,应该就是同样的字符了,50个而已,不然的话基本上是无解的,先生成了一个字母数字的字典,txt文档改后缀 dic,字典破解

3.JPEXS Free Flash Decompiler下载地址: 链接: http://pan.baidu.com/s/1jHOxB2Q 密码: nda5 JPEXS Free Flash Decompiler反编译flash文件 在171中找到base64, 解码

flag{jpexs7reeflash}

MISC 一枝独秀

关键字: stegSolve winhex ARCHRP jphs

知识点:

步骤:

1.winhex查看png 发现PK头 改后缀zip

2.需要密码, ARCHRP字典爆破 解压后发现81张大小不一 查看属性

	公田天王
C:\Users\hh\Downloads\file(4)\一枝独秀.	字典 ~
范围 长度 字典 明文 自动保存 字典选项 字典文件路径:	选项 高级
C: \Program Files (x86) \Ecomsoft Password 智能变化 尝试所有可能的大/小写组合 转换为 OEM 编码	Recove 🎽 · 开始行号 0 😵
状态窗口	
2021/1/11 19:27:47 - 文件"C:\Users\hh\Dov 2021/1/11 19:27:47 - 开始字典攻击 2021/1/11 19:27:47 - 口令已成功恢复!	vnloads\file(4)\一枝独秀.zip"已打开。 ^
2021/1/11 19:27:47 - '12345678' 是这个文作	牛的一个有效口令 🔹
当前口令: 已用时间: 进度指示器	平均速度: [剩余时间:g.csdn.net/dadongwud]

📄 flower (81).jpg 属性													
常规	安全	详细信息	以前的版本										
属性]	值											
标题 主题 分级 标记		$flowers \\ & & & & & \\ \end{pmatrix}$	\checkmark										

3.stegSolve查看 有东西 jphs05提取 填入flowers作为密码,提取后winhex打开,发现PK头,改后缀,解压txt文档,佛说,根据 hint进行栅栏解密,base64解密

http://www.keyfc.net/bbs/tools/tudoucode.aspx

H-hDs	;100ZL31hIZZbeRSbbbVRZNm32₩2X33mGm3Txt999RdV9hx0
每组字 HINT	数 4
	ZmxhZ3tDb29seW91R290SXROb3dZb3VLbm93VGh1RmxhZ30
	清空 加麥 解麥 口解麥结果以16进制显示
	flag {CoolyouGotItNowYouKnowThellag}

MISC 妹子的陌陌

关键字: forewalk 步骤: 1.foremost分解出一个压缩包,但是解压需要密码,图片上写到: 喜欢我吗.

	为加密的文件输入密码 momo.txt 在压缩文件 00000072.rar 里	
输入密码(E)		
喜欢我吗.	· · · · · · · · · · · · · · · · · · ·	2
□ 見示索司(c)		
▶ 38小五时(3)		

2.文本内容 莫斯密码解密,输入网址,二维码(黑白相反或者反色处理)微信 扫码 orQR_Research有自动纠错功能(本人无法使用,打开后点击任务栏在切换大小写)

摩斯电码解密结果: http://encode.chahuo.com/ 是一个解密网站。

下面的是AES解密,U2FsdGVkX18tl8Yi7FaGiv6jK1SBxKD30eYb52onYe0=是密文,@#@#¥%......¥¥%%......&¥是秘钥, 拿去解密得到momoj2j.png,访问http://c.bugku.com/momoj2j.png,得到一个二维码:

KEY{nitmzhen6}

MISC 好多压缩包 知识点: hex base64 crc32 步骤:

1.zip爆破伪加密未果,CRC32爆破脚本(运行时间超级长)

```
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
                   if crc == (binascii.crc32(s.encode())):
                       f.write(s)
                       return
def CrackZip():
       for i in range(0,68):
           file = 'out'+str(i)+'.zip'
           crc = zipfile.ZipFile(file,'r').getinfo('data.txt').CRC
           CrackCrc(crc)
dic = string.ascii_letters + string.digits + '+/='
f = open('out.txt','w')
CrackZip()
print("CRC32碰撞完成")
f.close
```

650000

z5BzAAANAAAAAAAAAAko+egCAIwBJAAAAVAAAAAKGNKv+a2MdSROzAwABAAAAQ01UCRUUy91BT5UkSNPoj5hFEVFBRvefHSBCfGOruGnKnygsMyj8SBaZHxs YHY84LEZ24cXtZ01y3k1K1YJ0vpK9HwqUzb6u9z8igEr3dCCQLQAdAAAAHQAAAAJi0efVT2MdSROwCAAgAAAAZmxhZy50eHQAsDRpZmZpeCB0aGUgZm1sZS BhbmQgZ2V0IHRoZSBmbGFnxD17AEAHAA==

清空 加密 解密 2 解密结果以16进制显示

复制

https://blog.csdn.net/dadongwudi

								- 194						
<		log 🔀	📙 访	包明.tx	:t 🔀 🛛	L,		. txt 🗷	l 🔚 password. py 🔀 🔚 c		py 🔀 🔚 1 🔀 📑 flag. zip 🔀 🛛			- 1
1	cf	90	73	00	00	0d	00	00					^	
2	00	00	00	00	00	aa	3e	7a						
	00	80	23	00	49	00	00	00		Poplar	50 S			
4	54	00	00	00	02	86	34	ab		Replac	ce			<u>^</u>
5	fe	6D	63	10	49	10	33	03		Find	Replace Find in Files Mark			
0	00	16	14	ab	dd	4.5	40. 4 E	54 0E						
8	24	48	43	68	8 f	98	41	11			Find what : 🔯	~	Find Next	
g	51	41	46	f7	9f	1d	20	42						
LO	7c	6d	2b	b8	69	ca	9f	28			Replace with :	~	Replace	
1.1	2c	33	28	fc	48	16	99	1f						
1.2	1b	18	1d	8f	38	2c	46	76				In selection	Replace All	
LЗ	el	с5	ed	67	4d	72	de	4d					Dealers All is All Oncord	
L 4	4a	d5	82	74	be	92	bd	1f		Ba	ackward direction		Replace All in All Opened	
1.5	0a	94	cd	be	ae	£7	3f	22		M	atch whole word only		Documenta	
. 6	80	4a	f7	74	20	90	2d	00		Пм	atch case		Close	
- 7	1d	00	00	00	ld	00	00	100						1
La	102	6Z	30	e/	0.0	41	63	10		⊻ w	rrap around			
20	49	66	60	61	67	20	74	78		Search	n Mode	2	Transparency	
21	74	00	b0	34	69	66	66	69			ormal		On losing focus	
22	78	20	74	68	65	20	66	69			ornia		Off losing focus	
23	6c	65	20	61	6e	64	20	67		ОÐ	xtended (\n, \r, \t, \0, \x)		() Always	
2.4	65	74	20	74	68	65	20	66		OR	egular expression 🗌 . matches newline			
25	6c	61	67	c4	3d	7b	00	40						
2.6	07	00												

3.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"

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

📸 WinHex -	[123.zi	p]															_													
★ 文件(F) 编辑	¥(E) 搜	索(S)	导航	(N)	查看(V)) 工具(T) 专	ШT	具(I)	选项	(0)	窗口(W) 帮	朏(H	ł)															
	e 1	ng	6		100 G	A #	1.46	-04 -04	-+-	₩		34	138	2	RA	0	804		41	•	9									
wn2 123.zip																														
Offset	0	1 2	3	4	5 6	5 7	8	9	10	11 1	2 13	3 14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	ANSI ASCII
00000000	52 6	1 72	21	1A	07 00	F	90	73	00 0	0 00	D 00	00	00	00	00	00	00	AA	3E	7A	00	80	23	00	49	00	00	00	54	Rar! Ïs °>z €‡ I T
00000032	00 0	0 00	υz	00	34 AI	FE	6B	63	1D 4	49 1	D 33	3 03	00	01	00	00	00	43	4D	54	09	15	14	CB	DD	41	4F	95	24	†4«bkc I 3 CMT ËÝAO•\$
00000064	48 D	3 E8	8F	98	45 11	51	41	46	F7 9	9F 1	D 20) 42	7C	6D	2B	B8	69	CA	9F	28	2C	33	28	FC	48	16	99	1F	1B	HÓè ~E QAF÷Ÿ B m+,iÊŸ(,3(üH ™
00000096	18 1	D 8F	38	2C	46 76	5 E1	C5	ED	67	4D 7	2 DF	5 4D	4A	D5	82	74	BE	92	BD	1F	0A	94	CD	BE	AE	F7	3F	22	80	8, FváÅígMrÞMJÖ, t¾'⅔ ";®÷?"€
00000128	4A F	7 74	20	90	2D 00	1D	00	00	00	1D 0	0 00	00	02	62	D1	E7	D5	$4\mathrm{F}$	63	1D	49	1D	30	08	00	20	00	00	00	J÷t - bŇçÕOc I 0
00000160	66 6	C 61	67	2E	74 78	3 74	00	BO	34 1	69 6	6 66	6 6 9	78	20	74	68	65	20	66	69	6C	65	20	61	6E	64	20	67	65	flag.txt °4iffix the file and ge
00000192	14-177-0								-			, 0	07	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	t the flagÄ={ 0
00000224	选择界	财加权	11 AL								>	< 0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000256												0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000288	1100	10.1									_	0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000320	ANS	I-ASC	II								_	0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000352	ASC	II He	х									0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000384											_	0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000416												0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

★ 快速访问 ↓ 桌面	*	123.zip _{美型} : WinRAR ZIP 压缩文件					修改	文日期: 2021/1/13 19:46 N: 1.20 KB	X
123.zip									
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)									
] 🏢 🄇) 🔨	 Image: Image: Image:	E				
添加 解压到	测试 查看	删除 查	1 前导	信息 扫描病毒	注释 化	护 自解压格式			
个 🗱 123.zip - RAR 4.x 压缩文件, 解包大小为 29 字节									
名称	大小	压缩后大小	类型	修改时间	CRC3			flag{nev3r_enc0de_t00_s	m4ll_fil3_w1th_zip}
J			文件夹			1			1 1727 N 1927
flag.txt	29	29 文本文档		2016/8/29 12: D5E7D162		162		https://blog.csdn.net/dadongwudi	

flag{nev3r_enc0de_t00_sm4ll_fil3_w1th_zip}

MISC 关键字:

知识点:

步骤:

杂七杂八:

1.Burpsuite Fiddler Wireshark简单对比

- 1. Burpsuite基于java语言,具有跨平台的优势;
- 2. Fiddler基于.Net,入门简单,功能强大,但是只适用win平台,目前借助mono也无法很好的在mac、 linux平台运行;
- 3. Wireshark各平台都有相应版本,不过入门门槛相对较高。 Burpsuite和Fiddler在抓包上侧重请求和响应的数据,Wireshark侧重于数据帧

2.grep的基本用法

https://blog.csdn.net/successdm/article/details/90145432?utm_medium=distribute.pc_relevant.none-task-blog-baidujs_title-2&spm=1001.2101.3001.4242

3.CTF密码学常见加解密总结

https://blog.csdn.net/qq_40836553/article/details/79383488 https://blog.csdn.net/qq_40837276/article/details/83080460?utm_medium=distribute.pc_relevant.none-task-blog-baidujs_title-2&spm=1001.2101.3001.4242

4.破解ZIP加密文件 https://www.cnblogs.com/ECJTUACM-873284962/p/9387711.html 5.常见的文件头尾 https://blog.csdn.net/qq_29277155/article/details/98060616

```
7z
文件头标识: 37 7A BC AF 27 1C
JPEG/JPG
文件头标识:ff,d8(SOI)(JPEG 文件标识)
文件结束标识:ff ,d9(EOI)
PNG
文件头标识: 89 50 4E 47 0D 0A 1A 0A
GIF
文件头标识: 47 49 46 38 39(37) 61 GIF89(7)a
BMP
文件头标识: 42 4D--- BM
HTML (html)
文件头标识: 68746D6C3E
ZIP Archive (zip)
文件头标识: 504B0304 PK
RAR Archive (rar)
文件头标识: 52617221
```

JPEG (jpg),文件头: FFD8FFE0

PNG (png),文件头: 89504E47

GIF (gif),文件头: 474946383961

ZIP Archive (zip),文件头: <mark>504</mark>B0304

RAR Archive (rar),文件头: 52617221

Wave (wav),文件头: 57415645

AVI (avi),文件头: 41564920

Real Audio (ram),文件头: 2E7261FD

Real Media (rm),文件头: 2E524D46

MPEG (mpg),文件头: 000001BA

MPEG (mpg),文件头: 000001B3

7z文件头: 37 7A BC AF 27 1C

参考链接: https://www.cnblogs.com/cat47/p/11432475.html

参考链接: https://blog.csdn.net/qq_39629343/article/details/80611614

<u>创作打卡挑战赛</u> 赢取流量/现金/CSDN周边激励大奖