Bugku--杂项一(签到题-----猜)

原创

gclome ① 于 2019-11-16 21:26:12 发布 〇 488 🛠 收藏

分类专栏: <u># CTF</u>

版权声明:本文为博主原创文章,遵循<u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/qq_44108455/article/details/103099666</u>





CTF 专栏收录该内容

20 篇文章 0 订阅 订阅专栏

签到题

傻瓜化操作,直接关注微信公众号,就会把flag发过来

这是一张单纯的图片

新于上路 🔄 吊用网址 🖽 设备维护中心

"http://123.206.87.240:8002/misc/1.jpg"因存在错误而无法显示。 图像

点击右键,将图片下载下来,打开



用notepad++打开,最后显示了一串编码,解码后得flag

{W7me6溶携**EEGESG**w**ECKECG**9NUU}整}7D謙龉舘t嫺蒈橅迖顟貎EC3<E8DESOSI5EE4DESEBDEM閣x"鏢裮SUB挑L崶潭b8簚gECDEB秋疽EE4SYN轀瓣EDDES \$*+|瑆2E8CDDBSOH莎汗"x籖駦鈃犄2I\$DDBEE4%SUB(EE201EABUSE99SOHPVTEABNUD笕珀q管电舁eu隒漎/3煜咧'_EEBEE830誌EFX;LEEC1髮s幪E86D

矔 鋹 XA8BEL@SIEM駷)n~*k次 X812 X9B 鲕畚 SOHENO蔊EP抦GSC!} XC4FSDC1苯

9, * 880 ! 茭 8A2 880 830 MULt 評熔 袃 瑟 ST 2 禀 . 颜氏 874 169 琦 拀 驩b SO1 880 8 疑蕿 √ 8A8 00 9 疑 * 874 * 874 * 7 c 嶲 * 酙 507 4 | 873 507 65 15 8 87 4 87

DC3Y蹽ラ騒\莸荸&800畿羖G斾韩*Hv&B7 !BELZE1?BxW&C3SUB7遮鞅痙&9F

ELE90+殆兞|UEFIBELEC6?SIu4夫I]W骂ECDDDE础Q庩廣搗艮檻

闡#eR缳r}蛔兵 ^GS博i5M=~咱O起a)N9] 腊家和OSII 60舣US駸煜g 十结家部 畸HEON晚菜929日72X状窝和NUUA珼VAX持bhE722级拯国的第2C演 SYN拐螽SU 9 20774 扽 1 柃 尕 10 g- 瑸 爭 J E92 ACK W #8 ES 28 2 SOLIES Mg 玧 SUBUS 桂 秸 銤 K 裰 枆 m IM M o 釱 - 胰眊 NUL 200 鷄GSIXFFNUL) 纀 XAA SOH 鬍 NAKKF 原 5 X 9 D. 浴 X

2017 婼镖 V11 [鳨至22) 锚 藂 NUD 矦0-鉾 88CB31 葱 薇`Mr? 8226 炡 0883<Ck 贪 k20 鍬w\$Q 183 PB31 钝0 吨鹆 184 MikHég b NUD 芳 DC2 I <u\$ 揝 QENUD NAR 髼 鞲 叉 畔 &

Z.,

BSE9BEMA、注意E008是E5EM集份EF1技?NW薩爾24/凸跿E5EFA持e对 E5E9 AN合T?ES彩HES凯E31EEDE4PEBAL姆垫落張wG2DG1j疠芩ES2EM菌8没、箕~陆;噫攖y<qn]dDC2x奫怳vE30%贩E3DE7{n轻^M鷓蜡 M)CAN傿GE37?啕t`咖 峽應T0鑠魚 簄焔へce 彩gESEDEES0FDENDE3CEOEDI疠SE0jEDDDC4NUDQEDC4NSD比PFB至D5]ESC转低S达娩FE33GS>IEAN2清 - Z 襤m | ACK 鱳< 舘wn NEC 2G 蔰

诏G[**x9DSUBXC2XFENUL**蕭IFFr啬DLEXE339GM躵65 ZE3BEL 尠飱網

配)斜口器D3:梶晴程DC3崜:673蜥器B3NDD) 壇&/鳥寝器A7A>嬬器D9:7褫器D8C07控器970夏∞VWVnACKL2等器9CNUUNUD膳8.NDD器7AACK88A(%A0S7X88A(%A0S7X8 銱云97'2槓!K 浦云F5+云BBETXpNAK云E85聃蠄/云FEGSx驩評VT

齊裓剖EMIXA3BELIDC2E版紙縊IXA3#IX9ANUL 堍IX8A (NUL) (NUL) 錠蠅>

)卤 \$1 鼕 \$6\$31 & \$77\$1 & \$75 (娒K 鸶 暺 D \$2977 鸶 3 嶱 ! 蟐 烶 歸 1573 閂 胙 { 1779 n " 兜 塊 I , \$770 NARP 2 抶 \$773 / @ \$720 \$689 ACR 煠 师 マ \$

ECCAN" 嗖[哥@]抬忰刹丽#8痋劓餲Z储ETB5}^Y轴d+END展徭遍孤STAX随 ES杜荜2Y展FNUTH叼HECH3k識 殖gCB2] 壑Z`NAR 8骎NUTHERDICHSYNOEDB:E 鉴忊GAN"V图D#貘oj需TGSTEP试)越云BS蠓奻呧汞EBIETB啥DCHseqUS1轿斗餲EPEMTECHDC2魔 S苦遌[xGTB醚N撥EDBhAEDD]+艹阹届坿T蔥omTCBDTM

隐写

打开图片

https://blog.csdn.net/qq_44108455

把图片放到HxD里,根据图片格式,我们发现图片的宽与高有矛盾,更改不合尺寸,把此处的A4改为F4,将图片保存,

Ľ	e z.png																	
	Offset(h)	00	01	02	03	04	05	06	07	9 8	09	OA	ов	oc	OD	OE	OF	对应文本
	00000000	89	50	4E	47	OD	OA	1Å	OA	bo	00	00	OD	49	48	44	52	‰PNGIHDR
	00000010	00	00	01	F4	00	00	01	F4	08	06	00	00	00	СВ	D6	DF	ô <mark>ô</mark> ËÖß
	00000020	88	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	ŠpHYst
	00000030	74	01	DE	66	1F	78	00	00	OA	4D	69	43	43	50	50	68	t.bf.xMiCCPPh
	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	ЗE	DF	ileür≲xÚ₀S⊚X ñ÷e⊯§_44108455

然后打开图片,得到flag

BL

BUGKU{a1e5aSA}

telnet

打开链接,下载了一个流量包

		, 🔳 🖉 🞯 🖡 🗟 🙆 9, 🗢 🛸 🖀 🕭 👱 🔜 🗐 9, 9, 9, 14, 12											
	te	lnet										X	
N	io.		Time	Source	Destination	Protocol	Length	Info					
AL OL		7	4.555208	192.168.221.128	192.168.221.164	TELNET	57	Telnet Da	ta				
		8	4.570808	192.168.221.164	192.168.221.128	TELNET	66	Telnet Da	ta				
		9	4.648808	192.168.221.128	192.168.221.164	TELNET	63	Telnet Da	ta				
		10	4.648808	192.168.221.164	192.168.221.128	TELNET	72	Telnet Da	ta				
		11	4.726808	192.168.221.128	192.168.221.164	TELNET	71	Telnet Da	ta				
	>	[TCF Sequ [Ne> Ackr 0101 Flag Wind [Cal	Segment Len: uence number: xt sequence nu nowledgment nu 1 = Heade gs: 0x018 (PSH dow size value lculated windo	38] 83 (relative seque mber: 121 (relativ mber: 124 (relativ rr Length: 20 bytes (S I, ACK) :: 256 ww size: 65536] in Content 256	ence number) ve sequence number)] ve ack number) ;)								

查找flag

2										
		🖹 🏹 🍳 🔶 🚔	🛃 📃 🔳 🔍 Q	€. ₩						
	tcp.stream eq 0 📘						X		表达式…	+
4	分组列表	宽窄、	~ □区分大小写 字符	串 🗸 🗸 flag	1			查找	取消	
No	o. Time ^	Source	Destination	Protocol	Length Info			1		1
	1 0.000000	192.168.221.128	192.168.221.16	4 TCP	66 1146 → 23 [S	YN] Seq=0 Win=8192 Len=0 MSS=1	.460 WS=256 SACK_PER	M=1		
	2 0.000000	192.168.221.164	192.168.221.12	тср	66 23 → 1146 [S	YN, ACK] Seq=0 Ack=1 Win=14600	Len=0 MSS=1460 SAC	K_PERM	=1 WS	
	3 0.046800	192.168.221.128	192.168.221.16	4 TCP	54 1146 → 23 [A	CK] Seq=1 Ack=1 Win=65536 Len=	:0			
	4 0.078000	192.168.221.128	192.168.221.16	4 TELNET	75 Telnet Data	•••				
	5 0.093600	192.168.221.164	192.168.221.12	B TCP	60 23 → 1146 [A	CK] Seq=1 Ack=22 Win=14624 Len	1=0			<u> </u>
1100	Sequence number	r: 83 (relative s	sequence number)							1
	[Next sequence	number: 121 (re:	lative sequence numbe	er)]						
	Acknowledgment	number: 124 (re:	lative ack number)							
1	0101 = Hea	der Length: 20 byte	es (5)							
	> Flags: 0x018 (P	SH, ACK)								
	Window size val	ue: 256								
	[Calculated win	ndow size: 65536]								
1	[Window size sc	aling factor: 256]								
	Checksum: 0x3cb	7 [unverified]								
		· ·								_

找到之后,追踪tcp流,然后找到了flag

🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · networking.pcap

眼见非实(ISCCCTF)

下载下来是一个zip文件,解压得到一个word文档,但是并打不开,尝试修改后缀为txt,png,依旧无果。

看了别人的writeup,发现别人在这里打开了文档,但是乱码,下面出现了FK,然后猜测这是一个压缩包,于是将其后缀改为zip

		大王
📙 眼见非实	2019/11/16 17:21	文件夹
🚔 眼见非实.zip	2016/12/7 16:00	好压 ZIP

解压缩之后里面

有个document.xml文件,用记事本打开,然后"ctrl+F",查找flag,就找到flag了。

	> zip∼	> 眼见非实 > 眼见非实 :	> word	~ ひ 搜索
	^	名称	~ 修改日期	类型
		📜 _rels	2016/8/15 4:06	文件
		📜 theme 🔪 🏉	2016/8/15 4:06	文作
	*	📄 document.xml 🧲		XM
	*	📄 fontTable.xml	•	XM
	*	📄 settings.xml		XM
		styles.xml		XM
		webSettings.xml		XM
库				
i				

with the second se

啊哒

下载下来是一张图





查看图片属性,有一串编码(后面有用),然后再无其他发现,

属性压缩	值	^
分辨率单位		
颜色表示		
压缩的位/像素		
照相机		
照相机制造商		
照相机型号	73646E6973635F32303138	
光圈值		
曝光时间		
ISO 速度		
曝光补偿		
焦距		
最大光圈		
测光模式		
目标距离		
闪光灯模式		
闪光灯能量		
35mm 焦距		
高级照片——		
镜头制造商		455

把图片放到notepad++里,这里看见大佬

们的writeup里说是这是个压缩文件,(也不知道怎么看出来的),然后修改后缀为ada.zip,不过是加密的,输入 上面那串编码ascll hex的 sdnisc_2018 成功打开得到flag





又一张图片,还单纯吗

初练杂项,真的好多不会,看了别人的writeup,知道这道题要用binwalk(第一次用binwalk------瑟瑟发抖.jpg)。 写下我的笔记,打开链接一张程序猿



然后j将图片下载下来放到binwalk里 运行 binwalk -e /root/2.jpg 发现捆绑了好几张图片 运行 dd if=/root/2.jpg of=/root/1.jpg skip=158792 bs=1 查看其中一张图片

root@kali:~#	binwalk -e /root,	/2.jpg							
DECIMAL	HEXADECIMAL	DESCRIPTION	警告,您正在使用超级帐户						
0 12 rectory: 8	0x0 0xC	JPEG image data, EXIF standard TIFF image data, big-endian, offset	of first image di						
158792 158822 rectory: 8	0x26C48 0x26C66	JPEG image data, JFIF standard 1.02 TIFF image data, big-endian, offset	of first image di Desktop						
159124 162196 168370	0x26D94 0x27994 0x291B2	JPEG image data, JFIF standard 1.02 JPEG image data, JFIF standard 1.02 Copyright string: "Copyright (c) 19	同题站 98 <mark>m H</mark> ewlett-Packard						
Company" File File Number of a state of the									
记录了27689+0 27689 bytes (的写出 <u>2</u> 8 kB, 27 KiB) cd	opied, 0.128218 s, 216 kB/s https://blo	g.csdn.net/qq_44108455						

打开这张图片,

出现flag(真是学到了!!!),把flag一个个字母敲上去。。



猜

打开图片,是一个明星,只是不知道是谁,而flag就是这个人的名字全拼 于是百度识图哈哈哈,识别出来是刘亦菲,然后成功了。。哈哈哈