BUUCTF~Misc~Test5



 kvmbox
 于 2021-02-14 14:09:26 发布
 178 % 收藏 1

 分类专栏:
 <u>笔记</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/m0_47643893/article/details/113573548</u>



笔记 专栏收录该内容

1篇文章 0 订阅 订阅专栏

目录

前言

前言

又是全新的一篇.....

黄金6年

视频中满放帧看发现有4张二维码扫出来拼接一下然后得到完整的key: iwantplayctf 然后视频在010最后发现了base64,然后解码一下。用脚本将base64以字节流数据写入成Rar文件然后密码就上上面的key

#base64以字节流数据写入成Rar文件 import base64

b64_str = "UmFyIRoHAQAzkrXlCgEFBgAFAQGAgADh7ek5VQIDPLAABKEAIEvsUpGAAwAIZmxhZy50eHQwAQADDx43HyOdLMGWfCE9WEsBZprAJ QoBSVlWkJNS9TP5du2kyJ275JzsNo29BnSZCgMC3h+UFV9p1QEfJkBPPR6MrYwXmsMCMz67DN/k5u1NYw9ga53a83/B/t2G9FkG/IITuR+9gIvr/ LEdd1ZRAwUEAA=="

byte_stream = base64.b64decode(b64_str)
open('flag.rar','wb').write(byte_stream)

就得到了flag flag{CTF-from-RuMen-to-RuYuan}



C4:BC20h:	00	00	00	00	00	00	00	00	01	F5	55	6D	46	79	49	52	ÕUmFyIR
C4:BC30h:	бF	48	41	51	41	7A	6B	72	58	6C	43	67	45	46	42	67	oHAQAzkrXlCgEFBg
C4:BC40h:	41	46	41	51	47	41	67	41	44	68	37	65	6B	35	56	51	AFAQGAgADh7ek5VQ
C4:BC50h:	49	44	50	4C	41	41	42	4B	45	41	49	45	76	73	55	70	IDPLAABKEAIEvsUp
C4:BC60h:	47	41	41	77	41	49	5A	6D	78	68	5A	79	35	30	65	48	GAAwAIZmxhZy50eH
C4:BC70h:	51	77	41	51	41	44	A0	44	78	34	33	48	79	4F	64	4C	QwAQAD.Dx43HyOdL
C4:BC80h:	4D	47	57	66	43	45	39	57	45	73	42	5A	70	72	41	4A	MGWfCE9WEsBZprAJ
C4:BC90h:	51	6F	42	53	56	6C	57	6B	4A	4E	53	39	54	50	35	64	QoBSV1WkJNS9TP5d
C4:BCA0h:	75	32	6B	79	4A	32	37	35	4A	7A	73	4E	6F	32	39	42	u2kyJ275JzsNo29B
C4:BCB0h:	6E	53	5A	43	67	4D	43	33	68	2B	55	46	56	39	70	31	nSZCgMC3h+UFV9p1
C4:BCC0h:	51	45	66	A0	4A	6B	42	50	50	52	36	4D	72	59	77	58	QEf.JkBPPR6MrYwX
C4:BCD0h:	6D	73	4D	43	4D	7A	36	37	44	4E	2F	6B	35	75	31	4E	msMCMz67DN/k5u1N
C4:BCE0h:	59	77	39	67	61	35	33	61	38	33	2F	42	2F	74	32	47	Yw9ga53a83/B/t2G
C4:BCF0h:	39	46	6B	47	2F	49	49	54	75	52	2B	39	67	49	76	72	9FkG/IITuR+9gIvr
C4:BD00h:	2F	4C	45	64	64	31	5A	52	41	77	55	45	41	41	3D	3D	/LEddlZBAMUEAA===t/m0_47643893
C4:BD10h:	A0																

Base64 在线解码、编码

□ 点击关闭

常规Base64 CSS Base64

DES加密/解密

解密 3DES加密/解密

AES加密/解密 RSA加密/解密

 $\label{eq:constraint} UmFyIRoHAQAzkrXICgEFBgAFAQGAgADh7ek5VQIDPLAABKEAIEvsUpGAAwAIZmxhZy50eHQwAQAD$

Dx43HyOdLMGWfCE9WEsBZp JkBPPR6MrYwXmsMCMz67DN	AJQoBSVIWkJNS9TP5du2kyJ275JzsNo29BnSZCgMC3h+UFV9p1QEf <5u1NYw9ga53a83/B/t2G9FkG/IITuR+9glvr/LEdd1ZRAwUEAA==	
	编码源格式: ○文本 ●Hex 解码结果: 自动检测 · 中	≝ 文编码:UTF-8 ∨ 编码 解码
00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	^
52 61 72 21 1A 07 01 00	33 92 B5 E5 0A 01 05 06 Rar!3	
00 05 01 01 80 80 00 E1	ED E9 39 55 02 03 3C B0 9U<.	
00 04 A1 00 20 4B EC 52	91 80 03 00 08 66 6C 61 K.Rfla	未能识别的数据
67 2E 74 78 74 30 01 00	03 OF 1E 37 1F 23 9D 2C g.txt07.#.,	当前编码:[Hex + Ascii]
C1 96 7C 21 3D 58 4B 01	66 9A CO 25 0A 01 49 59 !=XK.f%IY	数据长度 · 169 Bytes
56 90 93 52 F5 33 F9 76	ED A4 C8 9D BB E4 9C EC VR.3.v	truck of the
36 8D BD 06 74 99 0A 03	02 DE 1F 94 15 5F 69 D5 6ti.	插件致:16, 耗时:1ms

间谍启示录

一开始是iso文件

不解压问价直接打开可以获得flag解压之后打开程序直接自动删除,不会生成flag

这个文件用binwalk看不到rar文件,直接用foremost分离然和看到有rar文件,一开始解压发现打开没有东西弹出,然和以为就是 这样的题目,又放到虚拟机中泡ios镜像然后无果。后面才知道不解压的时候时直接打开会生成文件。 flag{379:7b758:g7dfe7f19:9464f:4g9231}

🛢 00000517.ra	ar - WinRAR (评估版本)										
文件(F) 命令(C)	工具(S) 收藏夹(O)	选项(N) 帮助	(H)									
(第111) (111) ((1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	重找 向										
0000 1	2 3 00000517.rar - RAR 压缩文件, 解包大小为 356,660 字节											
名称	大小 压缩后.	. 类型 ; 7	下面的注释包含自解压脚本命令									
 ■. ■ flag.exe 副 机密文件.txt ■ 文件已被销 □ 文件已被销 	180,263 33,844 38 34 172,073 31,074 4,286 2,267	文件夹 2	ith=D:\机密文件 itup=文件已被销毁.exe itle=身份识别 ixt 份识别似乎有误,正在销毁文件。 .cense=获取机密 i在解压机密文件,请点击继续									
			不解压可以在软件里生成文件解压反而不能生成文件									
<		> <										

1	添加解压到测试 查看	删除	查找	向导	信息	扫描病毒
1	🗈 📓 00000517.rar - RAR	压缩文件	‡,解包大	小为 350	5,660字	τ ι
1	名称		^	;下面	前的注釈	译包含自解
L(i	 ■ flag.exe ■ 机密文件.txt ■ 文件已被销毁.exe □ 文件已被销毁.ico 			Path Setu Titl Text {	=D:\机 p=文件 e=身份	密文件 己被销毁. 识别
				身份	识别似	乎有误,〕
ıli	文件(F) 编辑(E) 格式(O) 查	看(V) 精	^殷 助(H)			
,	Flag{3/9:7b758:g7dfe	/19:9	94641:4	.g923	1}	
6						

我吃三明治

在kali中看到两张图片,在010中两张图片的连接处,有base32弄出来解密一下就是flag flag{6f1797d4080b29b64da5897780463e30}



拉胯的三条命令

Tcpdump使用命令:

tcpdump -n -r nmapll.pcapng 'tcp[13] = 18' | awk '{print \$3}' | sort -u

-n网络地址转化

-r 从指定文件中读取包

tcp[13] = 18代表只抓取synACK标志位(代表服务器和客户端连接)

Awk'{print\$3}' 取第三为字符串

Sort -u 拒绝重复

Tcpdump使用详解:

https://www.cnblogs.com/lvdongjie/p/10911564.html

Tcpdump常用抓包教程:

https://blog.csdn.net/shun smile/article/details/80261335

在看了wp之后有两种方法第一种就是用wireshark手工修改port来找开放的端口

在编辑->首选项->外观->列添加一个Port类型选择Dest port(unresolved)

以port列降序排序,查找每个端口是否有[ACK]响应标志,众所周知在TCP三次握手中,[SYN]标志表示建立连接,[ACK]表示响应,查看开放端口,肯定会返回[ACK]标志

找端口因该是题目的本意。

我们也也可以在kali中使用Tcpdump工具

使用这段命名即可

tcpdump -n -r nmapll.pcapng 'tcp[13] = 18' | awk '{print \$3}' | sort -u

即可得到开放端口:

flag{21226318013306}



在参加网络安全大赛第二届世界巡回赛新加坡站一场与SP战队的比赛时,作为K&K战队主防手的你使用经典的"三条命令"检查端口封闭: ^ 请将开放端口按由小到大顺序写入flag中如:开放1、22、234端口,flag{122234}

https://blog.csdn.net/m0_4764389

吹着贝斯扫二维码

这题的拼二维码太难了吧,非常考验耐心。



扫码是编码过程要我们解码,在压缩包备注中发现base32->16->13->85>64>85

按照二维码依次解码

	★ BROWSE THE FULL DCODE TOOLS' LIST	or En
	Results	ASCII85 DECODER
	ThisIsSecret!233	ASCII85 CIPHERTEXT <
		dCode decodes ASCII85 https://blog.csdn.nel/m0_47643893
相因应		

得到密码,打开压缩包即可看到flag flag{Qr_ls_MeAn1nGfuL}

🔨 🌌 flag.zip - ZIP 压缩文件, 解包大小为 22 字节				
名称 ^	大小	压缩后大小	类型	IMRRGNBDEQZWGI3DKMSFGNCDMRJTII3TMNBQGM4TERRTGEZTOMRXGQYDGO
📕			文件夹	
flag.txt *	22	34	文本文档	
[
📗 🗐 flag.txt - 记事本				-
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)				
flag{Qr_ls_MeAn1nGfuL}				

https://blog.csdn.net/m0_47643893

从娃娃抓起

打开是数字和字母的编码方式,数字的是中文电码字母是五笔编码

分别看对照表找到。

人工智能也要从娃娃抓起

惹1931 热3583							
ren							
壬1103 仁0088 人0086 忍1804 韧7282 任0117 认6126 刃0432							
妊1175 纫4771							
reng							
🥘 *从娃娃抓起.txt - 记事本							
文件(E) 编辑(E) 格式(<u>O</u>) 查看(⊻) 帮助(<u>H</u>)							
 文件(E) 编辑(E) 格式(O) 查看(Ⅴ) 帮助(H)							
文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H) 0086 1562 2535 5174							
文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H) 0086 1562 2535 5174 人工智能							
文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H) 0086 1562 2535 5174 人工智能 bnhn s wwy vffg vffg rrhy fhnv							
文件(E) 编辑(E) 格式(Q) 查看(⊻) 帮助(且) 0086 1562 2535 5174 人工智能 bnhn s wwy vffg vffg rrhy fhnv 从娃娃抓起							
 文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H) 0086 1562 2535 5174 人工智能 bnhn s wwy vffg vffg rrhy fhnv 从娃娃抓起 请将你得到的这句话转为md5提交, md5统一为32位小写。 							

https://blog.csdn.net/m0_47643893

转md5,32位小写。



小易的U盘

是一个镜像文件,我们用010打开发现是rar改下后缀,解压出来。



一个个试发现在autorun.inf里提示32这个程序,我们用IDA打开,找到flag flag{29a0vkrlek3eu10ue89yug9y4r0wdu10}

	.text:00401010				
4	.text:00401010	push ebp			
1	.text:00401011	mov ebp	, esp		
	.text:00401013	sub esp	, 44h		
	.text:00401016	push ebx			
	.text:00401017	push esi			
	.text:00401018	push edi			
	.text:00401019	lea edi	, [ebp+var_44]		
	.text:0040101C	mov ecx	, 11h		
	.text:00401021	mov eax	, ØCCCCCCCCh		
	.text:00401026	rep stosd			
	.text:00401028	push off	set aW ; "w+"		
	.text:0040102D	push off:	set aDProgramFlagTx ; '	"D:/Program/flag.txt"	
	.text:00401032	call fo	pen		
	.text:00401037	add esp	, 8		
	.text:0040103A	mov [eb	p+var_4], eax		
	.text:0040103D	mov eax	, [ebp+var_4]		
	.text:00401040	push eax	; FILE *		
	.text:00401041	push off:	set aFlag29a0vkrlek ; '	"flag{29a0vkrlek3eu10ue	89yug9y4r0wdu10}"
	.text:00401046	call _fp	uts		
	.text:0040104B	add esp	, 8		
	.text:0040104E	mov ecx	, [ebp+var_4]		
	.text:00401051	push ecx	; FILE *		
	.text:00401052	call _fc	lose		
	-				

截取两位转16进制转成10进制,都大于128,然后所有-128,在转ASCII。最后脚本

```
def hex_str(str):#对字符串进行切片操作,每两位截取
   hex_str_list=[]
   for i in range(0,len(str)-1,2):
       hex_str=str[i:i+2]
       hex_str_list.append(hex_str)
   print("hex列表: %s\n"%hex_str_list)
   hex_to_str(hex_str_list)
def hex_to_str(hex_str_list):
   int_list=[]
   dec_list=[]
   for i in range(0,len(hex_str_list)):#把16进制转化为10进制
       int_str=int('0x%s'%hex_str_list[i],16)
       int_list.append(int_str)
       dec_list.append(int_str-128)#-128得到正确的ascii码
   for i in range(0,len(dec_list)):#ascii码转化为字符串
       flag += chr(dec_list[i])
   print("转化为十进制int列表: %s\n"%int_list)
   print("-128得到ASCII十进制dec列表: %s\n"%dec_list)
   print('最终答案: %s'%flag)
if ___name__=='___main___':
  str='d4e8e1f4a0f7e1f3a0e6e1f3f4a1a0d4e8e5a0e6ece1e7a0e9f3baa0c4c4c3d4c6fbb9b2b2e1e2b9b9b7b4e1b4b7e3e4b3b2b2e3
e6b4b3e2b5b0b6b1b0e6e1e5e1b5fd'
   print("字符串长度: %s"%len(str))
   hex_str(str)
```

得到flag{922ab9974a47cd322cf43b50610faea5}

[ACTF新生赛2020]swp

数据流导出http文件中有个压缩包然后需要密码7z提取文件,是伪加密然后就的到了flag文件 ELF文件用ida64打开找到flag,也可以直接010搜索ctf找到 flag{c5558bcf-26da-4f8b-b181-b61f3850b9e5}

Э	F6	4C	29	E5	48	83	EC	08	48	C1	FD	03	E8	57	FE	Н
F	FF	48	85	ED	74	20	31	DB	ØF	1F	84	00	00	00	00	H1
9	4C	89	FA	4C	89	F6	44	89	EF	41	FF	14	DC	48	83	.LLA
3	01	48	39	DD	75	ΕA	48	83	C4	08	5B	5D	41	5C	41	H9[]A\A
)	41	5E	41	5F	С3	90	66	2E	ØF	1F	84	00	00	00	00]A^A_Ð.f
9	F3	С3	00	00	48	83	EC	08	48	83	C4	08	С3	00	00	Н
9	01	00	02	00	00	00	00	00	61	63	74	66	7B	63	35	actf{c5
5	35	38	62	63	66	2D	32	36	64	61	2D	34	66	38	62	558bcf-26da-4f8b
)	62	31	38	31	2D	62	36	31	66	33	38	35	30	62	39	-b181-b61f3850b9
5	35	7D	00	00	01	1B	03	3B	38	00	00	00	06	00	00	e5};8
9	EC	FD	FF	FF	84	00	00	00	0C	FE	FF	FF	AC	00	00	https://blog.csdp.pet/m0_47643893
9	10	FF	FF	FF	54	00	00	00	26	FF	FF	FF	C4	00	00	T&

百里挑一

exiftool安装: apt-get install exiftool

运行命令:

Exiftool *| grep flag

题目: 好多漂亮的壁纸,赶快挑一张吧! 题目说有很多图片直接在图片的关键字

直接导出http有很多的图片,不可能我自己一个个看吧,发现一个新的工具exiftool可以找到flag flag{ae58d0408e26e8f26a3c0589d23edeec}

 TCP
 66 80→9744 [SYN, ACK] Seq=0 Ack=1 Win=8192 L

 TCP
 54 9744→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0

 HTTP
 447 GET /image/image1.html HTTP/1.1

 TCP
 1514 [TCP segment of a reassembled PDU]

找到了一般的flag还有一般应该就在数据流中

找不到看了wp在114tcp中,太难了。

root@kali: ~/kali/111 🛛 🛛	
<mark>xootakali:-/kali/111#</mark> exiftool * grep flag XP Comment :恭喜你!找到一半了,还有另一半哦!flag{ae 58d0408e26e8f rootakali:-/kali/111# ■	U`O~b0R.NJS.N g.S.NJS.T2.6.a.3.c.0.5.8.9.d.2.3.e.d.e.e.c.}. begin='' id='WSM0MpCehiHzreSzNTczkc9d'?> <x:xmpmeta xmlns:x="adobe:ns:meta/"><rdf:RDF xmlns:rdf="http://www.w3.c</td></x:xmpmeta>

alison_likes_jojo

outguess解密命令

Outguess -k 密码 文件 -r输出文件

第一张图片010看里面有zip文件,直接foremost分离,然后的到zip爆破得到密码解压

一串字符base32解密不是base64解密解三次得到killerqueen

一串字符串以为是flag拿去尝试发现不对,还有一张图片没有文件隐写色道也不是,还有两种加密的方式一个个尝试先用 steghide尝试不是,然后就是用outguess密码一开始没用压缩文件的密码,解不出来,然后尝试压缩文件密码,成功解除flag flag{pretty_girl_alison_likes_jojo}

Πουγκαιη		M/V/DK = 2N/t+ (Club)M/th max a) /07= =1 deV/=DOUT00
		killerqueen
11.txt jl	y.j; /root/kali/11.txt - Mousepad	
	文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)	
	警告:您正在使用 root 账户,操作不当可能会损害您的系统	
	<pre>wctf2020{pretty_girl_alison_likes_jojo}</pre>	
	root@kali: ~/kali	
	文件(E) 动作(A) 编辑(E) 查看(V) 帮助(H)	
	root@kali: ~/kali 🛛	
	<pre>root@kali:~/kali# outguess -k killerqueen jljy.jpg -r 11.txt Reading jljy.jpg Extracting usable bits: 5580 bits Steg retrieve: seed: 127, len: 40 root@kali:~/kali#</pre>	
2 个项目: 6.2		https://blog.csdn.net/m0_47643893

Zips

解压zip里面发现密码数字爆破解开密码,然后里面还有压缩包,可以看到是两个文件的,有密码,用7z解压可以解压但是另一个文件打开没有东西。后来才发现这个伪加密用7z解压不出来,然后用010打开找到09改成00然后就可以解压出来,里面是提示密码=printf是flag.zip的密码

注意:这是python2。然后得到当前系统时间的编码,出题时间和我现在的时间肯定不一样,然后试下15掩码爆破得到密码得到 flag{fkjabPqnLawhvuikfhgzyff}



注意伪加密不要直接用7z提取,可能会出错



Attack

安装mimikatz文件,在kali中"/usr/share/windows-resources/"文件夹下把文件直接复制到windows中然后要以管理员模式运行不然 会因为权限的原因无法运行 运行指令:

privilege::debug#获取权限

看别人的wp还要访问要解密的dmp文件(我是直接把文件放在64文件夹里)命令: sekurlsa::minidump lsass.dmp

sekurlsa::logonpasswords full#查看密码

查看数据流里面有zip文件,分离之后需要密码提示"这可是administrator的秘密,怎么能随便给人看呢?",回到数据流,导出 http看到有个dmp文件

使用mimikatz解析一下这个文件,找到win密码passwd就是压缩文件的密码

 	flag.txt	x	▼	
52				base64 - Switch file input/output base64 version - Display some version informations
53				cd - Change or display current directory
55				hostname - Displays system local date and time (of command)
56				
57				mimikatz # privilege::debug
58				Privilege 20 OK
59				mimikatz
60				Switch to MINIDUMP : 'lsass.dmp'
61				and a start and a start of the second statement of the
62				mimikatz # sekurisa::minidump isass.dmp Switch to MINIDIMP : 'lsass.dmp'
64				
65				mimikatz
66				ERROR mimikatz_doLocal ; "" command of "standard" module not found !
67				Module : standard
68	D0g3{3466b11de8	894198af3636c5bd1efce2}		Full name : Standard module Description : Basic commands (does not require module pame) 47642903

Game

打开压缩包是一张图片一个压缩包,首先我们来看下文件,初步没有看出什么问题,在后压缩包里是网页源码,在html文件中发现flag,是base32解码之后以为就是flag然而并不是,再回到图片lsb一看有一段

U2FsdGVkX1+zHjSBeYPtWQVSwXzcVFZLu6Qm0To/KeuHg8vKAxFrVQ==

结合上面的假flag然后 [在线网站上去解码]AES之类的(https://www.sojson.com/encrypt_rabbit.html)全部试了一遍才找到TripsDes 加密

然后就得到了flag flag{U_F0und_1t}

加密/解密	AES加密/解密	DES加密/解密	RC4加密/解密	Rabbit加密/解密	TripleDes加密/解密	MD5加/解密	Base64加/解密	Hash加/解密	JS 加密	JS 解密	
suctf{U_F0und_1t}					suctf{hAHaha_Fak3_F1ag} U2FsdGVkX1+zHjSBeYPtWQVSwXzcVFZLu6Qm0To/KeuHg8v			Hg8vKAxFrVQ==			
				1	密码是可选项,也就是可以	以不填。					
					く解密加密ン	>					