bugku隐写2

Lstop. 于 2019-07-18 19:35:18 发布 749 ☆ 收藏 2 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_44813849/article/details/96446860 版权 下载后看到这样一张图片

下软后有到这样一张图片



想拿到flag?心の中ないいくつかB数かの?

然后查看属性没发现啥, 接着用HXD打开,

看到里面有一个压缩包头,然后还有压缩包尾,所以我们把压缩部分复制下来放在一个新建的文件里

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	OD	0E	OF	
00007280	00	0C	FF	00	EO	8A	B0	DD	78	71	6E	9F	4C	OF	18	50	ÿ.àŠ°ÝxqnŸL₽
00007290	4B	79	54	01	F9	OF	FO	DB	E1	56	B1	E3	4D	7D	2D	AD	KyT.ù.ðÛáV±ãM}−.
000072A0	EC	2E	1F	79	EA	16	BD	D7	50	FF	00	82	75	78	DA	6D	ìyê.½×Pÿ.,uxÚm
000072B0	ЗA	39	E0	D2	2F	48	70	0E	E1	15	7E	B6	FE	CA	BF	FO	:9àÒ/Hp.á.~¶þÊ¿ð
000072C0	4C	5F	0C	78	73	C6	Dl	79	E9	6F	13	46	FD	0C	7E	86	LxsÆÑyéo.Fý.~†
000072D0	BF	44	E0	FD	95	BC	33	A7	78	62	08	A3	D3	AD	E6	55	¿Dàý•¼3§xb.£Ó.æU
000072E0	50	38	5E	BC	0A	00	FE	5C	F4	DF	F8	27	DF	8C	AE	AE	P8^¼þ\ôßø'ߌ®®
000072F0	05	B 3	D8	DC	21	63	8E	62	AF	76	F8	33	FF	00	04	5C	.³ØÜ!cŽb vø3ÿ∖
00007300	Fl	37	8C	AD	55	EE	61	62	18	02	14	C4	78	AF	DE	E9	ñ7Œ.UîabÄx Þé
00007310	BF	65	2F	0A	BD	E7	9A	BA	2D	B7	99	9E	B8	AE	FB	C1	¿e/.¾çš°-∵™ž,©ûÁ
00007320	1F	0A	B4	FF	00	0C	5B	62	lD	35	23	DA	38	20	50	07	´ÿ[b.5#Ú8 P.
00007330	E0	CF	88	7F	E0	84	7A	96	8F	E1	B 9	AE	1B	4F	72	CA	àÏ^.à"zá¹⊗.OrÊ
00007340	38	FD	D9	E6	BE	3B	F8	F5	FB	01	F8	9B	E1	54	F7	12	8ýÙæ¾;øõû.ø>áT÷.
00007350	4B	A2	5E	47	6D	09	23	CC	31	E0	57	F5	7F	E2	A5	Dl	K¢^Gm.#ÌlàWõ.â¥Ñ
00007360	74	FD	21	DB	55	9A	28	2D	C0	CB	6F	E9	8A	F8	63	F6	tý!ÛUš(–ÀËoéŠøcö
00007370	F3	F8	E5	FO	2F	50	FO	4D	EE	9B	73	A9	68	DF	68	07	óøåð∕PðMî>s©hßh.
00007380	04	12	73	91	40	1F	CC	C5	E6	97	75	A0	6A	92	23	41	s`@.ÌÅæ—u j′#A

 00007390
 24 7E 5E 49 C8 AD 2F 08 78 D6 EA 2D 4B F7 4E 57
 \$~^IÈ./.xÖê-K÷NW

 000073A0
 76 06 3D 2B EB 3F DA 6B 44 F8 77 A8 DD DF 4D A3
 v.=+ë?ÚkDøw¨ÝßM£

 000073B0
 4F 61 83 B8 A9 8F F1 AF 8A AF EF 6D F4 8F 10 CD
 Oaf,©.ñ¯Š¯imô..Í

 000073C0
 F6 79 94 80 78 02 80 3E FE FD 87 7F 68 BB CF 85
 öy"€x.€>þý‡.h»Ï...

 000073D0
 DE 30 D2 6E 45 E6 0A B8 24 66 BF A2 EF D9 13 E3
 ÞOÒnEæ..\$f¿∘iÙ.ã

 000073E0
 34 7F 15 3E 15 E9 57 46 75 95 DE DD 49 C1 AF E4
 4..>.éWFu•ÞÝIÁ¯ä

 000073F0
 4F E1 9F C5 13 A7 6A 50 BB 4D 86 52 30 33 D2 BF
 OáŸÅ.\$j₽»M†R03Ò¿

 00007400
 A2 DF F8 22 67 C5 D7 F1 CF C3 9D 3A DB 76 E5 48
 c&øø"gÅ×ñĨÃ.:ÛvåH

 00007410
 D1 49 CF B5 00 7E 95 59 4B BE 03 8E 94 D0 B8 04
 ÑIϵ.~•YK¾.Ž″Đ..

 00007420
 D2 69 B1 ED 80 9F 4A 0B 97 FC 28 01 40 CD 2E D3
 Òi±i€ŸJ._ü(.@Í.Ó

 00007430
 49 19 C7 52 73 2F 4D 00 3B 38 27 29 C8 26 54 82
 T C7.s M *8&@FTŠ

打开新建的压缩包发现里面有二个文件

·快 0 ■此	• 66.zip -	2345好压	1	7 除 密码	自解压	」 工具箱		中国。	甲 ₹ 2345以7月 医缩软件知名品》		×
5 3	\leftrightarrow \rightarrow	छ। 🗉 🔹	6 6	i.zip				-	当前目录查找(支持包内	直找) Q	高级
🖪 i	文件夹		×	◆ 名称			大小	压缩后大小	× 类型	安全	修改日
 	> 📙 H1	ML5入门及基础	Щ02 ^	(上层目录)							
a :	ID	M-6.32.6		💼 flag.rar			6.57 KB	6.57 KB	好压 RAR 压缩文件		2017
.	∣ ka ≻ <mark> </mark> Ku	li Gou		National Holes International Holes Internationae Internationae Internationae Internationae Internationae		9	0.22 KB	86.27 KB	JPG 文件		2017
. ,	La	nguages									1813849

查看提示文件知道密码为三位数字。接着我们使用ARCHPR工具暴力破解

文件(F)	恢复(R)	帮助(H)					
8	. 🥬	R	٢	-	2		5
打开	开始 <mark>!</mark>	停止	基准测试	升级	帮助	关于	退出
加密的	ZIP/RAR/A	CE/ARJ 文件		攻击类型	1		
C: User	s\µ	esktop (nag.r	ar	暴刀			~
范围 暴力范	长度 字 1 国选项	典 明文	自动保存	选项	高级		
□所有	1大写拉丁2	र् (A - Z)	Ŧ				
	孙写拉丁3 *教会(0_0)	∑(a - z)	ž	- -			
	1数子(0-9) 1特殊符号(!@)					
		- /		掩印; "	rrunua		ap
□所有	可打印字符	.				用户定义) Č
状态窗							
2019/7	/18 19:30:3	5 - ARCHPR 4	1.54 build 45	已启动			~
							\sim
当前口今				平均速度:			
三用时间 进度指示]: 器			剩余时间			
			09	6			
						ieheksiekeneichi/eiek	المرجع كركم ومحاكركم وكروك

ARCHPR 4.54 Professional Edition		-	_	×				
文件(F) 恢复(R) 帮助(H)								
<mark> - 帰</mark> 🔏 🔇 打开 开始! 停止 基准测试	黎 升级	? 帮助	 (1) (1)	<mark>。</mark> 退出				
加密的 ZIP/RAR/ACE/ARJ 文件	□攻击类型	Ð						
C:\Users'	暴力			~				
范围 长度 字典 明文 自动保存	选项	高级						
品、 (1)2000 晶小口今长度 =	3 =	宝符						
状态窗口								
2019/7/18 19:30:35 - ARCHPR 4.54 build 45	已启动			^				
				~				
当前口令: 2.用时间:	平均速度 剩余时间							
进度指示器								
0'	%	ition (In loc or	nden everilleter - A					

RCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

得到密码817

Advanced Arch	ive Password Recovery 统计信息:	ļ
总计口令	871	
总计时间	15ms	
平均速度(口令/秒)	58,066	
这个文件的口令	871	- C
十六进制口令	38 37 31	- C
保存…	✔ 确定	

然后打开加密文件看到一张图

片,使用HXD打开,发现最后有一个base64,然后解密得到flag

