BUU隐写



BL_zshaom ① 于 2022-03-14 20:33:59 发布 ② 3398 ☆ 收藏

文章标签: 安全

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/BL_zshaom/article/details/123462265</u>

版权



下载压缩包后,打开扫码,没有发现flag



就算加上flag{}也是错的,那拉进010看看。



这里面有个txt文本,这让我想起来了

1,图种(利用Linux下的foremost工具可以将output.png里隐藏的zip文件分离出来,在kali linux命令行里输入foremost,然后将output.png 拖入命令窗口回车执行即可分离,默认的输出文件夹为output,在这个文件夹中可以找到分离出的zip)

但是我没有,我只能把图片的后缀改为zip,然后用Ziperello进行爆破

S	zíperello zip password recovery tool	tanl	× T	18.44							
		帮助									
	当前密码长度 4	<u> </u>									
	当前密码										
	当前速度 恋母・7639	■注急:後系进度宋(つ)及 ■前的密码效验长度相关。 ■ 耗时较长。	动解 AES 算法力	111111月18日日 111211日11日日 11121日日							
独主	0% U u	*UH 34X IV *									
<u>)177</u> Z4											
	开始										
17:06:	i5: 密码 : "7639" .时间: 0 s										
	BACK 步骤 4 / 4: 破解密码.Go										
Ziperell	o ver. 2.1 版权所有 (C) 2008 FDRLab		CSDI	N@BL_zshaom							
用脱壳 m Exe	工具一看:发现不是exe文件 einfo PE - ver.0.0.4.3 by A.S.L - 960+49 sign 2016.07.29 File: KEY.exe Entry Point:? oo < EP Section:? File Offset:? First Bytes: 64.61.74.6										
Co	Linker Info : ? SubSystem : ?	the second is the	Ē.								
ha	File Size : 00000F1Eh < № Overlay : ?										
in	Diagnose:	💈									
2	NOT EXEbase64/32 encoded file data (Lame Generic detector)		1								
S	Lamer Info - Help Hint - Unpack info	Dth@BL zshaom	7								
	try base64 decoder by Fatin Kodak - www.t2ko.de	T V F									
后缀改	为txt后:										
dat	a:image/jpg;base64,iVBORw0KGgoAAAAN	SUhEL									
用notep	pad打开,复制打开网址得到二维码										
扫码得											

打开压缩包得到一张图片:查看属性、转为txt,放到010都没发现什么有用的东西。 用stegsolve打开图片,分别在red plane、bule plane、green plane能够发现图片的上方有异样:



我们用analyse >> data extract:

Bit Planes										
Alpha	7	6	5	4	3	2	1	0		
Red	7	6	<u> </u>	4	3	2	1	▶ 0		
Green	7	6	5	4	3	2	1	₽ 0		
Blue	7	6	5	4	3	2	1	▶ 0		
Proview Settings										

preview,能够看见16进制代码,我们save bin为png,打开是一个二维码,扫码得到flag。