## 2017信息安全大赛 MISC warm up 解题详解





CTF 专栏收录该内容

4 篇文章 0 订阅 订阅专栏

## 2017信息安全大赛 MISC warm up 解题详解

首先下载题目链接得到两个文件,如图所示。

TF⇒



https://blog.csdn.net/qq\_43165101

具体的题目链接可以查看爱春秋,https://www.ichunqiu.com/battalion?t=1&r=58837。 拿到题目,发现有一个图片和一个压缩包,尝试打开压缩包发现需要密码,因此猜测图片即为压缩包的明文。 首先,将图片压缩为zip文件,因为此处要使用ARCHPR进行压缩包的破解工作,所以要使文件的类型相同。 关于ARCHPR工具的下载可以参考csdn上的教程,https://blog.csdn.net/weixin 40270867/article/details/83062134

## 使用该工具破解,选择明文,然后选择对应文件,发现提示如下错误。

	阳, 反现1	月一个图片	和—1	门圡缩	包, 罢武	打开压缩	祖友圳	需要密始	3, 因此	猜》
	将图片日	ARCHPR 4.	.54 Prof	essiona	l Edition		_	- 🗌	×	所
	RCHPR 3	文件(F) 恢复	(R) 帮助	助(H)						02
			R	R	S	- 🍫	2			
HPR 错误		×	始!	停止	基准测试	升级	帮助	关于	退出	
			R/ACE/A	RJ文件		攻击类型				Th
🔒 在选定的档案中没有匹配的文件。如果您想要	仅使用文件的一音	粉分执行	istrator \Downloads \warmu			明文	$\sim$	TX		
	一个文件。		字典	明文	自动保存	选项 「幕	訯			
		确定	nistrator	r\Docume	ents\CTF\oper	n_fo 📄 ·	开始于:	:	•	
=== <b>E</b>	开始!	📑 密钥		-	密钥	-	密钥		- 温	
加密的	] ZIP/RAR/ACE	☑ 允许使用□	二进制文	件作为明	刖文 ZIP 档案	文件				
C:\Use	ers (Administrati	状态窗口								
范围 长度 字曲 明文选项 明文文件路径:									< >	
C:\Us	ers\Administrat	当前口令:				平均速度:				
🗎 🗎 🗎	密钥 1	3月时间: 进度指示器				剩余时间:				
☑	并使用二进制:				03	(ttps://blo	og.csdn.	net/qq_	431651	01

分析是压缩包的格式不一致,采用winrar再次压缩得到zip文件。再次尝试,发现开始破解。

ARCHPR 4.54 Professional Edition – 🗆 🗙									
<b>Հ件(F)</b>	恢复(R) 🕴	帮助(H)							
<mark>≗</mark> ≇⊺#	- <i>帰</i>	<b>船</b> 停止	(S) 基准测试	<b>黎</b> 升级	<b>?</b> 郪助	① ¥∓	退出		
加密的	ZIP/RAR/ACE	/AR1文件	HALL AND A	- 改击迷刑			~~~		
C:\Users\Administrator\Downloads\warmu 明文									
范围 长度 字典 明文 自动保存 选项 高级 明文选项 明文选项 明文注码									
C:\Users\Administrator\Documents\CTF\open_fo 📄 🕌 开始于: 🔤 🧐									
📄 ङञ्च - ङञ्च - 😭 -									
☑ 允许使用二进制文件作为明文 ZIP 档案文件									
状态窗口									
2019/7/24 13:49:35 - ARCHPR 4.54 build 45 已启动									
~									
前口令: 平均速度: 引用时间: 剩余时间: 使指示器									
	0%								
CHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd. 00,0500, 09/00 45165101									

刚开始以为破解时间很久,其实只需要几秒就可以破解,后面应该是在计算具体的密码可以忽略,直接另存为就可以得到破解的 文件。

		(前口令: 3月时间: 封度指示器	ARCHPR 4	54 - (	平均速度 到公司為 0%					×	]
9nLm	加密密钥已成功恢复! Advanced Archive Pa	assword Recovery 统计信息:	×	(R)	帮助(H)	3	-	?		5	
	总计口令	n/a		F始!	停止	基准测试	升级	帮助	关于	退出	
	总计时间	14s 638ms		nistrat	tor\Downloa	ads\warmu	- 攻击突型 - 阳立			~	句家和可以勿暇



猜测采用的是盲水印算法,根据github上的py脚本,可以直接破

解, https://github.com/chishaxie/BlindWaterMark/blob/master/README.md

注意这里采用的是python2编写的脚本,所以运行时也要用python2不然会报错。另外因为调用了opencv的库所以需要安装python 对应的opencv库。具体脚本运行时还需要一些其他的库再自行安装。 破解的结果如图

PS C:\Users\Administrator\Downloads\warmup\_3D87119B1FD69603E77BA1292A007C4B (2)\_decrypted> python2 bwm.py decode fuli.pn g fuli2.png watermark.png image<fuli.png> + image(encoded)<fuli2.png> -> watermark<watermark.png>

-2001112011002002010H1222H0010H0 (2)\_0003ptc0











open\_forum.pn g



