2017年全国大学生信息安全竞赛 misc warmup



mrwangtw 于 2021-10-22 16:34:46 发布 ○ 2978 ☆ 收藏 1 分类专栏: ctf misc 文章标签: 安全 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/mrwangtw/article/details/120906297 版权

 ctf同时被2个专栏收录

 3 篇文章 0 订阅

 订阅专栏



2篇文章0订阅

订阅专栏

这题之前做过一次没做出来,就是因为后面的盲水印得到的图片看不出来。

进入题目,下载文件,一个图片和一个压缩包,点开压缩包看到三个图片,但是需要密码,最最最重要的是压缩包里最后一张图片和下载的那个图片是一样的名字,基本可以猜到是明文攻击。

压缩下载的那个图片, 放入winrar,

📕 ••			又14关	
open_forum.png	42,196	41,512	PNG 文件	202759941&mr83822658

再同样查看下载的压缩包

			文件夹		
🔳 fuli.png *	3,869,944 3,8	851,145	PNG 文件	2017/6/19 17:	40056D15
🔳 fuli2.png *	4,551,642 4,	513,642	PNG 文件	2017/6/19 17:	02EB038D
open_forum.p	42,196	41,524	PNG 文件	2017/7/5 13:03 CSDN (83E22C5E @mrwangtw
 full2.png ^ open_forum.p 	4,551,642 4,3 42,196	41,524	PNG 文件 PNG 文件	2017/6/19 17: 2017/7/5 13:03 CSDN (83E22C @mrwa

最后面的crc校验码一样的

用ARCHPR进行明文攻击

ARCI	HPR 4.54 Pro	fessiona	l Edition				×
文件(F)	恢复(R) 專	§助(H)					
2	. 🙉	P	(S)	-	2		
打开	开始!	停止	基准测试	升级	帮助	关于	退出
加密的 ZIP/RAR/ACE/ARJ 文件 攻击类					<u>1</u>		
C:\Users\18240\Desktop\warmup_3D8711			明文			~	
范围 明文递 明文文	长度 字典 硕 件路径:	明文	自动保存	选项	高级		
C:\Use	rs\18240\Desk	top\open_	forum.zip	- · •	· 开始于:		
2	密钥 e43	a642a	密钥	3e424cdb	密钥	eb7c633	1 🔚
☑ 允许使用二进制文件作为明文 ZIP 档案文件							
状态窗							
2021/1	0/22 15:12:55	- ARCHPR	4.54 build 45	已启动			^
							~
当前口令 已用时间 进度指示	; 器			平均速度: 剩余时间:			
			09	6	CCD		
ARCHPR v	ersion 4.54 (c)	1997-201	2 ElcomSoft (Co. Ltd.	CSD	M @mrv	vangtw

上面放加密的文件(下载的压缩包),下面放明文文件(压缩的文件),选择明文攻击,开始。

这里需要爆破很长时间,爆破了几分钟就可以停止,得到一个文件,这个就是解密后的文件,可以正常打开

名称	大小	压缩后大小	类型	修改时间	CRC32
			文件夹		
🔳 fuli.png	3,869,944	3,851,133	PNG 文件	2017/6/19 17:	40056D15
🔳 fuli2.png	4,551,642	4,513,630	PNG 文件	2017/6/19 17:	02EB038D
open_forum.png	42,196	41,512	PNG 文件	2017/7/5 13:03	83E22C5E
				CSDN @	emrwangtw

打开发现上面的两张图片肉眼看起来都一样,这里把图片放在010里也没看到什么信息,放在stegsolve里面查 看也是一样没什么信息,怀疑可能是盲水印,百度下看了大佬的wp,确实盲水印,本题在我看来最大的难点就 是在这。

这里解密采用BlindWaterMark,下载下来,运行脚本需要安装numpy,opencv-python,matplotlib,这里安装opencv时不知道为什么总是错误,其实可以 在https://download.lfd.uci.edu/pythonlibs/w6tyco5e/cp27/opencv_python-2.4.13.7-cp27-cp27m-win_amd64.whl

上面的网站里下载,cp后面就是对应的python的版本,下载下来之后,cd到下载目录,pip install opencv_python-2.4.13.7-cp27-cp27m-win_amd64.whl,然后就可以运行bwm.py,这里有个bwmforpy3的脚本,就是针对python3的,我用的是python2。

python27 bwm.py decode fuli.png fuli2.png shuiyin.png

预先把图片放在盲水印脚本里运行,即可得到



总结:自我感觉解密不难,难的是安装这些脚本,工具或者其他东西,如果不会安装,有教程还好,难的就是 发生的错误,百度不出来。本人安装opencv,装了半天,百度到的教程看了很多,很多照着做也没成功,所以 任重而道远啊