# frackzip暴力破解密码

原创

Sandra_93 于 2018-10-18 22:54:16 发布 3486 收藏 2

分类专栏： BugkuCTF 工具类



本文链接：https://blog.csdn.net/Sandra_93/article/details/83153177



BugkuCTF 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏


工具类

4 篇文章 0 订阅

订阅专栏

## Bugku隐写2

### 第一步

右键文件属性，发现100K+，跟其他后缀名为jpg的文件相比有些大，觉得里面应该有东西，
将图片拖到虚拟机里，用**binwalk**命令：

```
binwalk.Welcome._jpg
```

将里面的东西弄出来，发现是个flag.rar**压缩包**，里面zip文件夹里有00000102.zip压缩包，打开后得到"提示.jpg","flag.rar"两个文件，其中flag **.rar文件被加密**了。将这个00000102.zip压缩包拖到物理机里，右键用记事本的方式打开flag.rar,发现里面有个3.jpg,可以判断里面有张图

### 第二步

linux 下zip文件密码**暴力破解**的工具：frackzip
将00000102.zip先拖到桌面下（也可以放到其他地方，只是放这里便于cd进入flag.rar文件），
然后使用frackzip暴力破解

```
root@kali:~/桌面/zip/00000102# fcrackzip -b -l 3-3 -c1 -v flag.rar
```

### 分析：

对**fcrackzip工具**：

-b表示使用暴力破解算法

-l设置长度，3-3表示最小(3)到最大(3)，也就是限制了密码的长度（从提示.jpg知道密码为3位），

-c 表示使用字符集中的字符

-c1指定密码类型为纯数字型,其他类型看手册

-v 表示更详细些

-u用于显示破解产生的密码

所以也可以：　`frack -b -l 3-3 -c1 -u flag.rar`　这样直接爆出密码

得到密码871

然后到物理机里右键解压，将密码输入进去，得到一张图3.jpg;

然后为3.jpg改下后缀名，改为3.jpg.txt，然后可以用记事本打开，最后一行，得到 f1@g{eTB1lEFyZSBhlGhAY2tlciE=}

将eTB1lEFyZSBhlGhAY2tlciE= 用base64在线解码，得到：y0u Are a h@cker!

补上flag{}，得到完整flag:flag{y0u Are a h@cker!}

windows下的暴力破解软件：ARCHRP

这里是用脚本爆破的writeup

有大佬writeup的用file看看里面的东西是图片还是压缩包

了解下file命令