CTF解题思路：图片隐写

原创

VIP文章 tiny丶 于 2019-08-03 17:10:58 发布 4380 收藏 9
分类专栏： 渗透&APT 渗透 文章标签： 图片隐写

本文链接：https://blog.csdn.net/vevenlcf/article/details/98350806

一、说明

说道图片隐写，应该算是一种信息隐藏，属于信息保护机制。

二、题目

这是一个利比亚-密码有多简单的题目。

使用的主要工具为： binwalk、foremost、dd

1、首先将图片传至kali。使用binwalk查看文件结构

```
root@kali:~/tmp# binwalk so-easy.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
-
0             0x0             JPEG image data, JFIF standard 1.01
66635         0x1044B         End of Zip archive, footer length: 22
```

【很奇怪- 为什么没有zip的开始位置呢？只有footer？】

这边是一个正常的文件结构 可以看到 zip有起始和结束

```
root@kali:~/tmp2#
root@kali:~/tmp2# binwalk -e sim.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
-
0             0x0             JPEG image data, JFIF standard 1.01

22895         0x596F          Zip archive data, at least v2.0 to extract, compr
essed size: 25, uncompressed size: 23, name: key.txt
23046         0x5A06          End of Zip archive, footer length: 22
```

2、使用foremost进行提取

可以看到只提取了jpg，而zip文件未做提取！！！ 这是一个问题啊 （应该是内部出现了什么错误。）

```
root@kali:~/tmp# foremost  so-easy.jpg
Processing: so-easy.jpg
|*|
root@kali:~/tmp#
root@kali:~/tmp# cd output/
root@kali:~/tmp/output# ll
-bash: ll: 未找到命令
root@kali:~/tmp/output# ls
audit.txt  jpg
```

3、使用dd 进行截断获取 （dd if=so-easy.jpg of=catch