CTF杂项题总结（持续更新）

原创

co0ontty 于 2018-12-24 09:35:29 发布 9220 收藏 46

分类专栏： CTF 文章标签： CTF writeup 杂项

本文链接：https://blog.csdn.net/weixin_38830346/article/details/85228832

图片隐写

博客中题目文件下载地址：

https://home.mycloud.com/action/share/db1ed206-5f81-4d3a-b4be-865c5fe78a2c

题目一：图片TIFF

题目文件：ada.jpg

使用binwalk分析图片中的信息如下：

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image directory: 8
5236          0x1474          Copyright string: "Copyright Apple Inc., 2018"
7782          0x1E66          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"/></x:xmpmeta>
218773        0x35695         Zip archive data, encrypted at least v2.0 to extract, compressed size: 34
, uncompressed size: 22, name: flag.txt
218935        0x35737         End of Zip archive
```


发现在图片中有zip，文件和TIFF信息。zip压缩包解压需要密码。查看一下TIFF信息，打开图片的详细信息部分，查看照片的相机信息，发现十六进制字符串，转换为字符串为 sdnisc_2018 即为压缩包密码，解压压缩包得到flag

进制转换工具推荐：co0ontty.github.io/things/cyberchef.htm

题目二：PNG-IHDR隐写

题目文件：2.png
该图片，在windows下面可以正常打开，在LINUX下却无法打开，则判断可能是通过修改PNG的长宽高实现的隐写。
使用工具打开图片，分析文件头种IHDR部分

```
89504E47 0D0A1A0A 0000000D 49484452 | .PNG        IHDR
000001F4 000001A4 08060000 00CBD6DF |    .    .      ...
```

IHDR后的部分，前4 bytes为PNG图像的宽度，接下来的4 bytes为PNG图像的长度
通过windows打开图像可以发现，图片的宽度大于长度，所以将长度修改与宽度相等，得到答案

题目三：grep “flag” -r

题目文件：zip
根据题目文件名字猜测，通过增加后缀变成压缩包来解压。
解压后发现有很多文件，使用查找文件内容命令查找flag

```
grep "flag" -r /Users/co0ontty/Downloads/眼见非实/
```

发现flag在/word/document.xml文件中

```
# co0ontty @ co0ontty-MBP in ~/Downloads/眼见非实 [8:18:41]
$ grep "flag" -r  /Users/co0ontty/Downloads/眼见非实
/Users/co0ontty/Downloads/眼见非实/word/document.xml:<w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wp14="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing" xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/office/word/2010/wordml" xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml" xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordprocessingGroup" xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessingInk" xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordprocessingShape" mc:Ignorable="w14 w15 wp14"><w:body><w:p w:rsidR="002B3D8D" w:rsidRDefault="002B3D8D"><w:r><w:t>Flag</w:t></w:r><w:r><w:t>在这里呦！ </w:t></w:r></w:p><w:p w:rsidR="002B3D8D" w:rsidRPr="002B3D8D" w:rsidRDefault="002B3D8D"><w:pPr><w:rPr><w:rFonts w:hint="eastAsia"/><w:vanish/></w:rPr></w:pPr><w:r w:rsidRPr="002B3D8D"><w:rPr><w:vanish/></w:rPr><w:t>flag{F1@g}</w:t></w:r><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/></w:p><w:sectPr w:rsidR="002B3D8D" w:rsidRPr="002B3D8D"><w:pgSz w:w="11906" w:h="16838"/><w:pgMar w:top="1440" w:right="1800" w:bottom="1440" w:left="1800" w:header="851" w:footer="992" w:gutter="0"/><w:cols w:space="425"/><w:docGrid w:type="lines" w:linePitch="312"/></w:sectPr></w:body></w:document>
```

题目四：路由器配置文件 config.bin

题目文件：config.bin
使用RouterPassView查看config.bin得到答案

题目四：Foremost分离图片

题目文件：foremost.jpg
使用binwalk进行分析，发现图片中隐藏了另一个图片

```
$ binwalk foremost.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0xC             TIFF image data, big-endian, offset of first image
 directory: 8
13017         0x32D9          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
 <rdf:Description rdf:about="" xmlns:photoshop="http://ns.adobe.com/photoshop/1.
0/" xmlns
158792        0x26C48         JPEG image data, JFIF standard 1.02
158822        0x26C66         TIFF image data, big-endian, offset of first image
 directory: 8
159124        0x26D94         JPEG image data, JFIF standard 1.02
162196        0x27994         JPEG image data, JFIF standard 1.02
164186        0x2815A         Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
 <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns
:xap="htt
168370        0x291B2         Copyright string: "Copyright (c) 1998 Hewlett-Pack
ard Company"
```


使用foremost命令进行分离

```
$ foremost foremost.jpg
foremost: /usr/local/etc/foremost.conf: No such file or directory
Processing: foremost.jpg
|*|
```

```
File: foremost.jpg
Start: Wed Dec 19 09:45:56 2018
Length: Unknown

Num      Name (bs=512)         Size      File Offset     Comment

0:      00000000.jpg          155 KB               0
1:      00000310.jpg           27 KB          158792
Finish: Wed Dec 19 09:45:56 2018

2 FILES EXTRACTED
```

```
jpg:= 2
```


成功分离出包含flag的图片