

CTF-隐写术（二）

原创

红烧兔纸 于 2020-09-14 16:42:53 发布 521 收藏 2

分类专栏: [CTF-隐写术](#)

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/weixin_39934520/article/details/108580998

版权



[CTF-隐写术](#) 专栏收录该内容

14 篇文章 2 订阅

订阅专栏

声明: 以下CTF题均来自网上收集, 在这里主要是给新手们涨涨见识, 仅供参考而已。需要题目数据包的请私信或在下方留言。

3.黑与白（来源：实验吧）

1.关卡描述

黑与白 分值: 20

来源: pcat 难度: 中 参与人数: 4014人 Get Flag: 783人 答题人数: 902人 解题通过率: 87%

flag格式: CTF{}

解题链接: <http://ctf5.shiyanbar.com/stega/Pcat.jpg>

https://blog.csdn.net/weixin_39934520

2.解题步骤

分析:

二维码直接上QR扫描工具, 得到[Http://pcat.cnblogs.cOM?Hh](http://pcat.cnblogs.cOM?Hh)

(注: 图片要与QR扫描工具在同一目录下)



打开网址以后是作者的个人博客, 里面并没有任何信息

百度了下writeup~~发现网址居然是培根密码

这里没有用A B~~网址的大小写即是 A B, 要么大写是A 小写是B, 要么大写是B 小写是A 写出来试一下把

HttpPp ABBAB OR BAABA ---> o 或 t

catcn BBBBB AAAAA ---> *或a ok只能是后一种, 前面的没有答案

bloGs BBBAB AAABA---> c

cOMHh BAAAB ABBBA---> p

密码: tacp (已验证)



附上培根密码表

- a AAAAA g AABBA n ABBA t BAABA
- b AAAAB h AABBB o ABBAB u-v BAABB
- c AAABA i-j ABAAA p ABBBA w BABAA
- d AAABB k ABAAB q ABBBB x BABAB

e AABAA l ABABA r BAAAA y BABBA

f AABAB m ABABB s BAAAB z BABBB

上 Stegdetect

Stegdetect的参数：**Stegdetect**通过统计测试来分析图像文件中是否包含隐藏内容。它运行静态测试以判断隐藏的内容是否存在。此外，它还会尝试识别隐藏内容是通过哪个隐写工具嵌入的。

Stegdetect的主要选项如下：

q – 仅显示可能包含隐藏内容的图像

n – 启用检查JPEG文件头功能，以降低误报率。如果启用，所有带有批注区域的文件将被视为没有被嵌入信息。如果JPEG文件的JFIF标识符中的版本号不是1.1，则禁用**OutGuess**检测。

s – 修改检测算法的敏感度，该值的默认值为1。检测结果的匹配度与检测算法的敏感度成正比，算法敏感度的值越大，检测出的可疑文件包含敏感信息的可能性越大。

d – 打印带行号的调试信息。

t – 设置要检测哪些隐写工具（默认检测jopi），可设置的选项如下：

j – 检测图像中的信息是否是用jsteg嵌入的。

o – 检测图像中的信息是否是用outguess嵌入的。

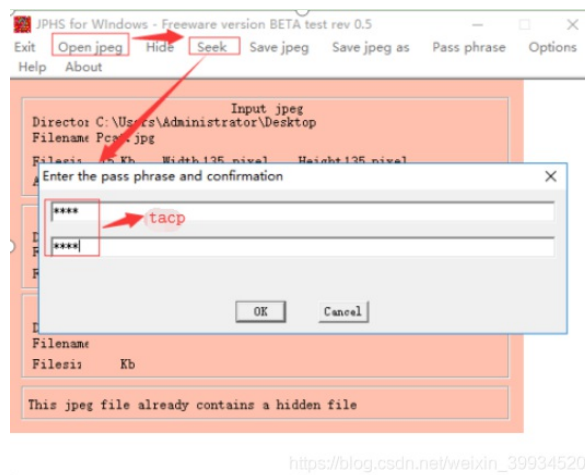
p – 检测图像中的信息是否是用jphide嵌入的。

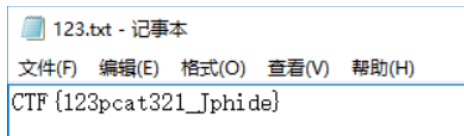
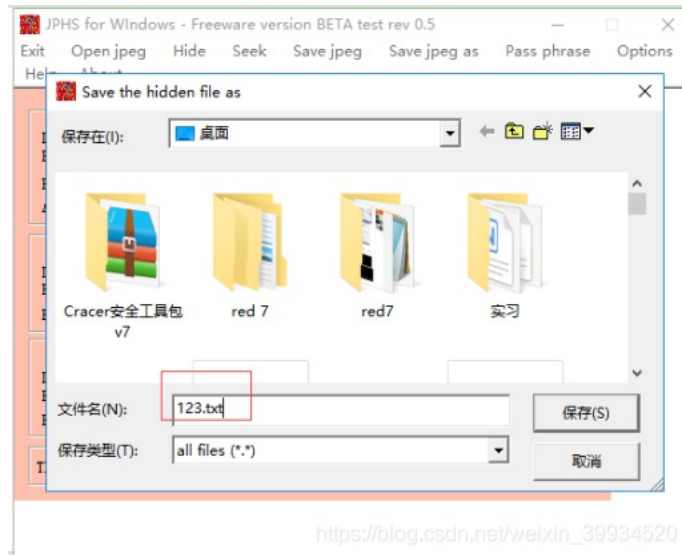
i – 检测图像中的信息是否是用invisible secrets嵌入的。

stegdetect.exe -t jopi -s 1000 C:\Users\Administrator\Desktop\Pcat.jpg

```
D:\各种工具\CTF工具合集\隐写\图像隐写\stegdetect-0.4-windows>stegdetect.exe -t jopi -s 1000 C:\Users\Administrator\Desktop\Pcat.jpg
C:\Users\Administrator\Desktop\Pcat.jpg : jphide(***)
```

打开JPHswin





CTF{123pcat321_Jphide}

知识扩充:

深入理解JPEG图像格式Jphide隐写

4.九连环(伪加密) (来源: 实验吧)

1.关卡描述

九连环 分值: 20

来源: [实验吧](#) 难度: 易 参与人数: 3638人 Get Flag: 770人 答题人数: 857人 解题通过率: 90%

flag格式: flag{xxx}

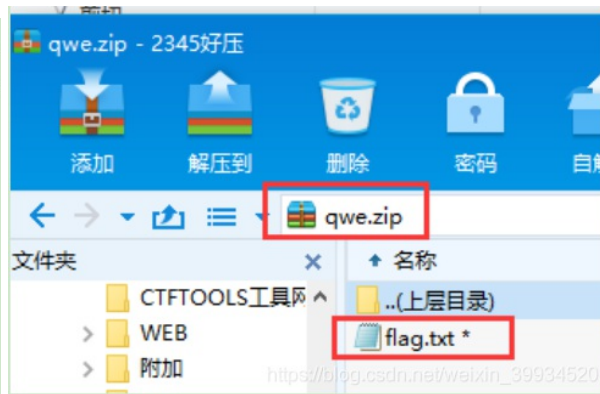
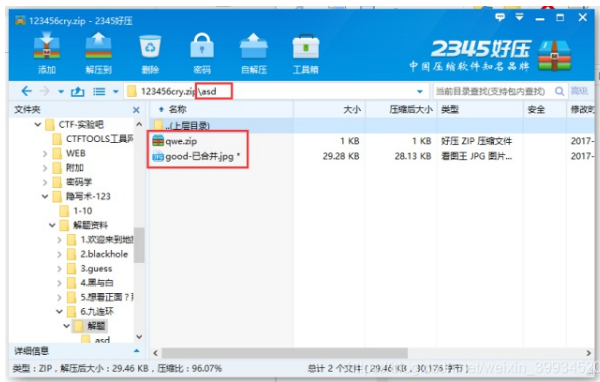
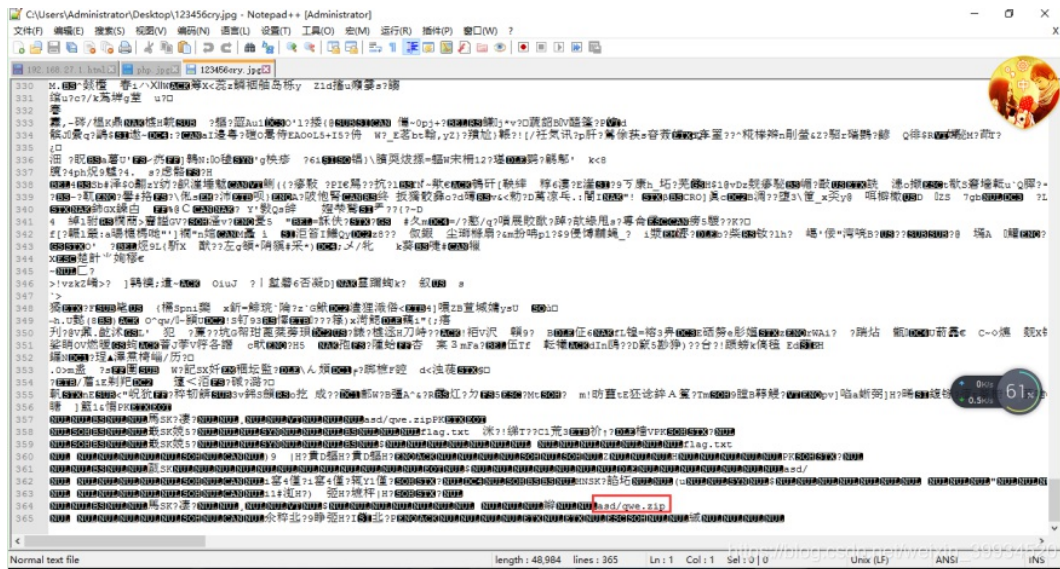
解题链接: <http://ctf5.shiyanbar.com/stega/huan/123456cry.jpg>

https://blog.csdn.net/weixin_39934520

2.解题步骤

分析:

打开链接, 是一张图片, 下载到本地。一般情况下要改后缀名为.zip, 用notepad打开验证一下, 果然在最后看到.zip。然后改后缀, 打开看一下里面都有什么, 先不解压。



将提取的压缩包解压后可以得到一张图片和一个被加密的压缩包, 因为有除开压缩包以外的信息, 所以猜测不是暴力破解弱口令。

要密码,

解答:

[Binwalk:后门\(固件\)分析利器 - FreeBuf网络安全行业门户](#)

[Steghide使用教程及其密码爆破](#)

使用工具: binwalk, steghide (可以把信息隐藏在AU, BMP, JPEG 或 WAV格式的文件中)

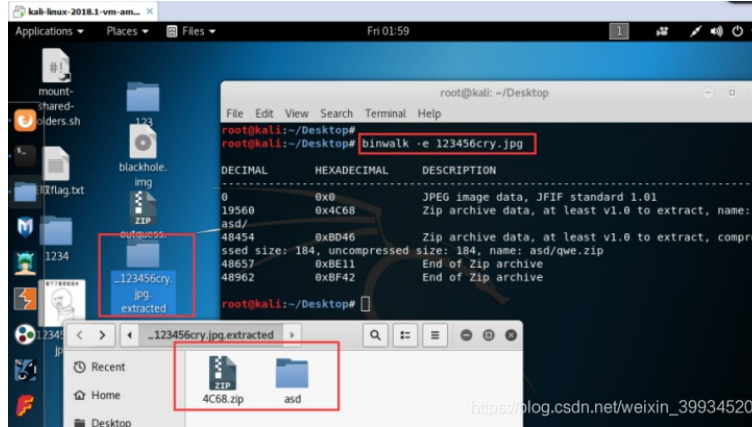
题目是一张图片, 首先使用binwalk查看, 果然其内部隐藏了压缩包, 使用命令binwalk -e 123456cry.jpg 提取内容


```

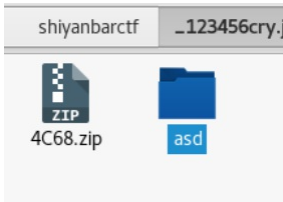
root@kali:~/Desktop# binwalk 123456cry.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
19560       0x4C68      Zip archive data, at least v1.0 to extract, name:
asd/
48454       0xBD46      Zip archive data, at least v1.0 to extract, compressed size: 184, uncompressed size: 184, name: asd/qwe.zip
48657       0xBE11      End of Zip archive
48962       0xBF42      End of Zip archive

```

如果用binwalk什么都没查看到，用命令apt-get update更新下软件。



binwalk -e分解，分成一个zip和那个asd文件夹。（4C64的压缩包里的内容和asd文件夹中的一致，无视掉）



直接打开asd，里面同样有一张图片和一个压缩包，good-已合并.jpg，qwe直接提取，发现里面有一个flag.txt，但是需要密码，应该需要这张图片上找密码了。用stegsolve也没看到啥。用steghide试试

```

root@kali: ~/Desktop/_123456cry.jpg.extracted/asd
File Edit View Search Terminal Help
root@kali:~/Desktop# cd _123456cry.jpg.extracted/
root@kali:~/Desktop/_123456cry.jpg.extracted# ls
4C68.zip asd
root@kali:~/Desktop/_123456cry.jpg.extracted# cd asd/
root@kali:~/Desktop/_123456cry.jpg.extracted/asd# steghide extract -sf good-已合并.jpg
Enter passphrase:
wrote extracted data to "ko.txt".
root@kali:~/桌面/shiyanbarctf/_123456cry.jpg.extracted/asd#

```

出来一个ko.txt，里面是打开压缩包的密码。然后提取出flag.txt，就得到flag了。

apt-get install steghide在kali上安装不成功什么鬼？

算了，用windows版的steghide

```
D:\各种工具\CTF工具合集\隐写\图像隐写\steghide>steghide extract -sf C:\Users\Administrator\Desktop\good-已合并.jpg
Enter passphrase:
```

密码为空.

```
ko.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
看到这个图片就是压缩包的密码:
bV1g6t5wZDJif^J7
```

bV1g6t5wZDJif^J7

```
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag {1RTo8w@&4nK@z*XL}
```

flag{1RTo8w@&4nK@z*XL}

注:这里提供windows安装binwalk, 不过感觉好麻烦就没装, 用kali里binwalk就好, 前提你kali里的binwalk正常。

<http://www.cnblogs.com/pcat/p/5256288.html>

拓展:

把一个文件或者图片藏到另一张图片里:

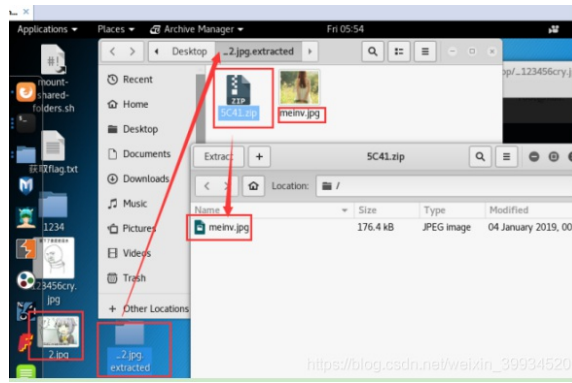
```
C:\Users\Administrator>cd Desktop
C:\Users\Administrator\Desktop>copy /b hack.jpg+meinv.zip 2.jpg
hack.jpg
meinv.zip
已复制 1 个文件。
C:\Users\Administrator\Desktop>
```

copy /b hack.jpg+meinv.zip 2.jpg

meinv文件可以是文本文档或者图片, 但都要压缩成zip, rar等格式, 然后找张图片如(hack.jpg)合成类似名如2.jpg的图片。

```
root@kali:~/Desktop# binwalk 2.jpg
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
4370         0x1112      Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>
<rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:MicrosoftPho
4886         0x1316      Unix path: /purl.org/dc/elements/1.1/"><rdf:Description
rd:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc="http://pu
rl.org/dc
23617        0x5C41      Zip archive data, at least v2.0 to extract, compressed size: 168795, uncompressed size: 176449, name: meinv.jpg
192542       0x2F01E     End of Zip archivehttps://blog.csdn.net/weixin_39934520
```

```
root@kali:~/Desktop# binwalk -e 2.jpg
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
4370         0x1112      Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>
<rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:MicrosoftPho
4886         0x1316      Unix path: /purl.org/dc/elements/1.1/"><rdf:Description
rd:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc="http://pu
rl.org/dc
23617        0x5C41      Zip archive data, at least v2.0 to extract, compressed size: 168795, uncompressed size: 176449, name: meinv.jpg
192542       0x2F01E     End of Zip archivehttps://blog.csdn.net/weixin_39934520
```



解压后有两个meiniv图片，只不过一个在文件夹里另一个在压缩包里。