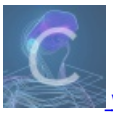
# Bugku CTF 杂项（1-12） Writeup

原创

KRDecad3 于 2018-06-09 19:53:50 发布 2124 收藏 6

分类专栏： writeup 文章标签： writeup Bugku CTF







# Bugku CTF 杂项（1-12） Writeup

## 0x01签到

扫描二维码，关注Bugku微信公众号，在公众号里输入“flag”即得到flag。

---

## 0x02这是一张单纯的图片

```
 d S( Ð¨¢S (¢S (
¢Š ÿ&#107;&#101;
&#121;&#123;&#12
1;&#111;&#117;&#
32;&#97;&#114;&#
101;&#32;&#114;&
#105;&#103;&#104
;&#116;&#125;ÙÙ
```

从winhex中打开图片，在底部发现一串HTML实体编码，解码得到flag。

---

## 0x03隐写

原图片的高度被更改了，IHDR文件头数据块，更改高度，把“A4”改成“F4”，保存，就可以看到被隐藏的flag（注意：图片是透明的）。

```
00 00 01 F4 00 00 01 F4
8A 00 00 00 09 70 48 59
```

---

## 0x04telnet

解压文件夹中有个pcap的文件，用wireshark打开，右键点击任一个消息追踪流，追踪TCP流，就可以看到flag。

| No. | Time | Source | Destination | P |
|---|---|---|---|---|
| 29 | 16.458029 | 192.168.221.128 | 192.168.221.164 | T |
| 30 | 16.504829 | 192.168.221.128 | 192.168.221.164 | T |
| 31 | 16.504829 | 192.168.221.164 | 192.168.221.128 | T |
| 32 | 16.754429 | 192.168.221.128 | 192.168.221.164 | T |

---

## 0x05眼见非实(ISCCCTF)

下载下来是一个zip文件，那就先解压，里面有个docx文件，拖进winhex发现文件头标识是504B0304，则推断这个docx文件是被改了后缀名的zip文件，更改后缀名后再打开，在word文件夹中的document.xml文件中发现flag。

---

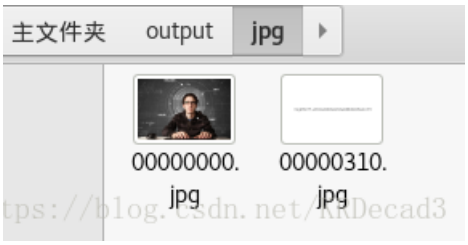
## 0x06又一张图片，还单纯吗

放入winhex看不出什么，放到kali里，通过终端用binwalk查看，在终端输入：
binwalk /root/桌面/2.jpg

```
root@kali:~# binwalk /root/桌面/2.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"
```

发现里面包含两个图片，一个jpg格式，一个tiff格式；
使用foremost分离文件，输入：foremost /root/桌面/2.jpg
在output文件夹中可以找到分离的图片，得到flag。




Binwalk：后门（固件）分析利器
CTF中图片隐藏文件分离方法总结

---

## 0x07猜

给了一张某女星的图片，放到百度识图或谷歌图片里搜一下，然后此女星的名字的拼音就是flag的内容/xyx。

---

## 0x08宽带信息泄露

下载得到一个二进制文件，放入RoutePassView查看，题目提示flag为宽带用户名，则在里面查找user，找到username。

---

## 0x09隐写2

下载得到一个图片，拖到Kali里用binwalk分析，终端输入：binwalk /root/桌面/Welcome_.jpg

```
root@kali:~/output/zip/00000102# binwalk /root/桌面/Welcome_.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
4444          0x115C          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc=
"http://p
4900          0x1324          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:li xml:lang="x-default">hint:</rdf:li></rdf:Alt>
52516         0xCD24          Zip archive data, at least v1.0 to extract, compre
ssed size: 6732, uncompressed size: 6732, name: flag.rar
59264         0xE780          End of Zip archive
147852        0x2418C         End of Zip archive
```



发现里面有zip文件，再用foremost分离，终端输入：foremost /root/桌面/Welcome_.jpg
解压里面的00000102.zip文件，发现里面还有flag.rar和一个图片提示，提示说密码是三个数，那么就暴破吧；
利用fcrackzip进行暴破，路径移动到flag.rar所在文件夹，终端输入：fcrackzip -b -l 3 -c '1' -u flag.rar

```
root@kali:~/output/zip/00000102# fcrackzip -b -l 3 -c '1' -u flag.rar

PASSWORD FOUND!!!!: pw == 871
```



得到密码，再解压又出现一张图片，winhex打开，在底部发现base64编码的flag。

---

## 0x10多种方法解决

下载解压里面是个无法打开的exe文件，用文本编辑器打开，里面写着jpg和base64编码，利用解码工具解开是个二维码，扫描得到flag。

```

ARnQU1BAACxjwv8YQUAAAAJcEh
Kq19hwPCDcrMJ9m7/7n45zfdxe
```



在线图片base64编码
在线二维码解码器

---

## 0x11linux

解压得到一个名为flag的二进制文件，使用grep命令（使用正则表达式搜索文本），转换到flag所在文件路径，终端输入：grep ‘key’ -a flag
搜索到flag。

---

## 0x12中国菜刀

解压得到一个pcapng文件，用wireshark打开追踪TCP流，发现里面有flag.tar.gz
用binwalk提取，输入binwalk -e /root/桌面/caidao.pcapng
再解压，得到flag的文本。