

BUUCTF：我爱Linux

原创

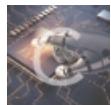
末初 于 2020-08-02 10:31:07 发布 收藏

分类专栏： [CTF_MISC_Writeup](#) 文章标签： [BUUCTF 我爱Linux](#)

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/mochu777777/article/details/107740734>

版权



[CTF_MISC_Writeup 专栏收录该内容](#)

246 篇文章 45 订阅

订阅专栏

题目地址：<https://buujj.cn/challenges/#%E6%88%91%E7%88%B1Linux>

The screenshot shows a challenge interface. At the top, it says "Challenge" and "65 Solves". The title of the challenge is "我爱Linux" with a score of "59". Below the title, there is a question: "你知道Linux下面有哪些好玩的命令吗？比如sl，还有哪些呢？" and a note: "注意：得到的 flag 请包上 flag{} 提交". There is a download button labeled "ba6cbd2f-cf..." and two input fields: "Flag" and "Submit". At the bottom, the URL "https://blog.csdn.net/mochu777777" is visible.

下载下来解压出来的的图片，看不了，用 [010 editor](#) 打开

The screenshot shows the 010 Editor application. The title bar says "010 Editor - C:\Users\Administrator\Downloads\b0d3e5f34e36b189b47a1a57a0a43ba4.png". The main window displays the binary dump of the image file. The left pane shows the hex dump, and the right pane shows the ASCII dump. The ASCII dump contains various characters and some recognizable text like ".fheEq]K;51qq.Ä'." and "j..šEudR..<`çÖ.Öä". A red box highlights the byte sequence FF D9, which is the standard JPEG end-of-file marker.

Name	Value	Start	Size	Color	Comments
struct PNG_SIGNATURE sig		0h	8h	Fg: Bg:	
uint16 btPngSignature[4]		0h	8h	Fg: Bg:	
uint16 btPngSignature[0]	8950h	0h	2h	Fg: Bg:	
uint16 btPngSignature[1]	4E47h	2h	2h	Fg: Bg:	
uint16 btPngSignature[2]	10h	4h	2h	Fg: Bg:	
uint16 btPngSignature[3]	4A46h	6h	2h	Fg: Bg:	

看到 FF D9 明显是 jpg 图片的结尾，而之后的内容不像是图片的内容，右键->Selection->Save Selection 提取出来提取出来的内容如下：

Python Pickle序列化内容 (怎么看出来的我也不知道.....hhh)

使用 `pickle` 脚本 load 出来

```
import pickle

fp = open("123.txt","rb+")
fw = open('pickle.txt', 'w')

a=pickle.load(fp)
pickle=str(a)
fw.write( pickle )
fw.close()
fp.close()
```

得到坐标代码

```
[[3, 'm'), (4, ''), (5, ''), (8, ''), (9, ''), (10, '#'), (31, 'm'), (32, ''), (33, ''), (44, 'm'), (45, 'm'), (46, 'm'), (47, 'm'), (50, 'm'), (51, 'm'), (52, 'm'), (53, 'm'), (54, 'm'), (55, 'm'), (56, 'm'), (57, 'm'), (58, ''), (59, ''), (60, ''), (61, ''), (62, '#'), (66, '#'), (71, '#'), (75, '#)], [(3, '#'), (10, ''), (11, '#'), (12, '#'), (13, '#'), (14, '#'), (15, '#'), (16, '#'), (17, '#'), (18, '#'), (19, '#'), (20, '#'), (21, '#'), (22, '#'), (23, '#'), (24, '#'), (25, '#'), (26, '#'), (27, '#'), (28, '#'), (29, '#'), (30, '#'), (31, '#'), (32, '#'), (33, '#'), (34, '#'), (35, '#'), (36, '#'), (37, '#'), (38, '#'), (39, '#'), (40, '#'), (41, '#'), (42, '#'), (43, '#'), (44, '#'), (45, '#'), (46, '#'), (47, '#'), (48, '#'), (49, '#'), (50, '#'), (51, '#'), (52, '#'), (53, '#'), (54, '#'), (55, '#'), (56, '#'), (57, '#'), (58, '#'), (59, '#'), (60, '#'), (61, '#'), (62, '#'), (63, '#'), (64, '#'), (65, '#'), (66, '#'), (67, '#'), (68, '#'), (69, '#'), (70, '#'), (71, '#'), (72, '#'), (73, '#'), (74, '#')], [(1, ''), (2, '#'), (3, 'm'), (4, 'm'), (5, ''), (8, ''), (9, '#'), (10, 'm'), (11, '#'), (12, '#'), (13, '#'), (14, '#'), (15, '#'), (16, '#'), (17, '#'), (18, '#'), (19, '#'), (20, '#'), (21, '#'), (22, '#'), (23, '#'), (24, '#'), (25, '#'), (26, '#'), (27, '#'), (28, '#'), (29, '#'), (30, '#'), (31, '#'), (32, '#'), (33, '#'), (34, '#'), (35, '#'), (36, '#'), (37, '#'), (38, '#'), (39, '#'), (40, '#'), (41, '#'), (42, '#'), (43, '#'), (44, '#'), (45, '#'), (46, '#'), (47, '#'), (48, '#'), (49, '#'), (50, '#'), (51, '#'), (52, '#'), (53, '#'), (54, '#'), (55, '#'), (56, '#'), (57, '#'), (58, '#'), (59, '#'), (60, '#'), (61, '#'), (62, '#'), (63, '#'), (64, '#'), (65, '#'), (66, '#'), (67, '#'), (68, '#'), (69, '#'), (70, '#'), (71, '#'), (72, '#'), (73, '#'), (74, '#')]]
```

再利用脚本转换

```
fw = open("pickle.txt","r")
text=fw.read( )
i=0
a=0

while i<len(text)+1:
    if(text[i]==']'):
        print('\n')
        a=0
    elif(text[i]==')':
        if(text[i+2]==','):
            b=text[i+1]
            d=text[i+1]
            b=int(b)-int(a)
            c=1
            while c<b:
                print(" ", end="")
                c += 1
            print(text[i+5], end="")
            a=int(d)
        else:
            b=text[i+1]+text[i+2]
            d=text[i+1]+text[i+2]
            b=int(b)-int(a)
            c=1
            while c<b:
                print(" ", end="")
                c += 1
            print(text[i+6], end="")
            a=int(d)
    i +=1
```

转换得到：

flag{a273fdedf3d746e97db9086ebbb195d6}