Archenemy

发表于 2021-01-08 更新于 2021-01-09 分类于 Challenge， 2020， CSICTF， Forensics
Challenge | 2020 | CSICTF | Forensics | Archenemy

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/forensics/2020/07/19/Archenemy.html

by INXS_JOY

题目描述

John likes Arch Linux. What is he hiding?

题目考点

解题思路

> *Its always a good practice to check the file format of all files while doing Forensics. I used the command `file arched.png` to check the file type. As suspected, I got this,*

```
1 arched.png: JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 1920x1080, components 3
```

So arched.png is a JPEG file. Let's change the extension to .jpeg

Next, I ran the image file through Stego-Toolkit and noticed that steghide found a embedded flag.zip file in the image.

Trying to unzip the flag.zip asks for a password, but we weren't provided with any passwords. So I tried to brute force the password using fcrackzip.

> *Fcrackzip tries all the passwords from any word-list we provide. In this case I used rockyou word-list which is a list of common passwords.*

Using the command, `fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt flag.zip`, we get the following output,

```
1 found file 'meme.jpg', (size cp/uc  27553/ 27752, flags 9, chk 9ed1)
2 PASSWORD FOUND!!!!: pw == kathmandu
```

So, the password for the flag.zip is `kathmandu`. Extracting the contents, we get a file meme.jpg. Opening it, we find the flag at the bottom of the image.

Flag

```
1 csictf{1_h0pe_y0u_don't_s33_m3_here}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/CSICTF/Forensics/7WchqhqZf4FbMxEKzUwznx.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # CSICTF # Forensics
Gradient sky
pydis2ctf