whaleCTF-30days-隐写【第二期】-SECCON大战-writeup

原创

sec小玖 于 2018-07-23 22:49:02 发布 1565 收藏 1
分类专栏： CTF 隐写 文章标签： CTF 隐写 视频隐写 ffmpeg ImageMagic

本文链接：https://blog.csdn.net/afuzong4267/article/details/81176108


CTF 同时被 2 个专栏收录
6 篇文章 0 订阅
订阅专栏


隐写
3 篇文章 0 订阅
订阅专栏

题目：

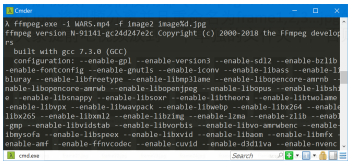
> 这次的大电影演员整容十分强大哦！可以我们还有一位隐藏嘉宾，不知道你能不能找到。

打开压缩包，获取视频后打开观看，发现是一个SEECON做的类似星球大战的开头片。

观看一段时间不难发现在黑色背景中隐藏的二维码，可是这个二维码只有在黄色字体扫过的时候才能够看到。这道题的解法是将这些图像（每一帧）重合恢复二维码。

按照帧来分解视频，我们使用ffmpeg工具，ffmpeg可以运行音频和视频多种格式的录影、转换、流功能。

我们使用命令ffmpeg -i WARS.mp4 -f image2 image%d.jpg,将视频分离并且重命名为image1,2,3…jpg的图片文件

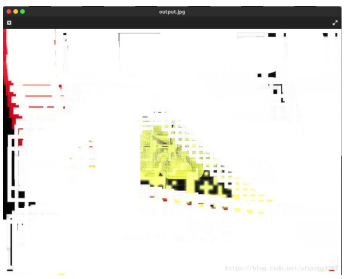


得到大量的jpg文件：

接下来我们还需要使用一个linux下的工具ImageMagic，我们安装在了ubuntu中，使用ImageMagic中的convert工具，将土图片进行重合覆盖。

```
sec@sec-pc:~/1$ convert image???.jpg -background none -compose lighten -flatten output.jpg
```

需要较长时间，运行结束后得到output.jpg，但是并没有发现二维码：

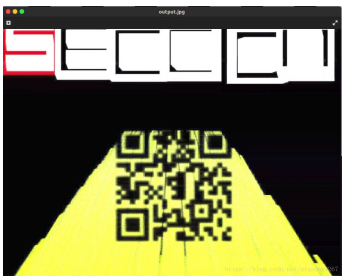


重新分析影片，发现应该是片头的SECCONWARS字符在覆盖时，造成了图片的错误，于是删除带有SECCONWARS字样的帧：

于是把前面部分的图片删除即可：

```
sec@sec-pc:~/1$ for i in {700..1200}; do mv image$i.jpg new/; done;
sec@sec-pc:~/1$ cd new
sec@sec-pc:~/1/new$ convert image???.jpg -background none -compose lighten -flatten output.jpg
```

重新查看output.jpg



得到了正确的二维码，使用QR_Research，识别二维码，得到flag：