高校战“疫”网络安全分享赛-MISC-武汉加油 writeup

原创

me晴天 于 2020-03-12 22:44:14 发布 349 收藏
分类专栏： CTF

武汉加油！

原本以为是一道逆向题，还有师傅盲猜得到flag，看了出题人的官方wp才知道这真是一道隐写题。

打开题目给的附件，是一张图片

这么大的图片肯定有猫腻

大小:	4.51 MB (4,733,142 字节)
占用空间:	4.51 MB (4,734,976 字节)

binwalk分析一下

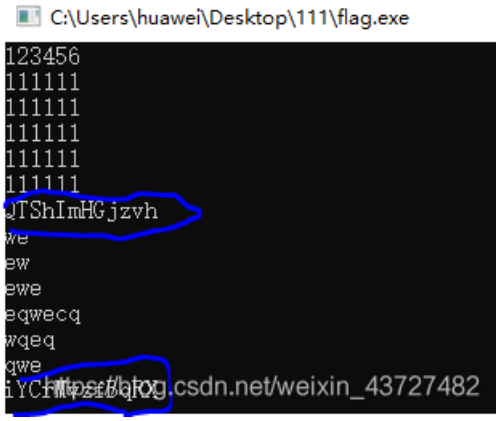
```
root@kali:~/桌面/脚本/Steghide# binwalk 1.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
130228        0x1FCB4         RAR archive data, version 5.x
```

存在图片和一个rar压缩包

提取压缩包，里

面是一个flag.exe的执行文件，打开后尝试输入发现

每输入六行就会返回一串字符串，猜测应该是需要输入特定的六个字符会返回flag；



我们需要找到这六个特殊字符，

使用steghide工具对图片进行分析

```
root@kali:~/桌面/脚本/Steghide# steghide info 2.jpg
"2.jpg":
  format: jpeg
  capacity: 5.9 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
```

发现确实存在隐藏信息，但是需要密码，爆破~！

steghide工具本身不具有爆破功能，这里需要使用的一个shell脚本

```
bruteStegHide.sh



for line in `cat $2`;do

    steghide extract -sf $1 -p $line > /dev/null 2>&1

    if [[ $? -eq 0 ]];then

        echo 'password is: '$line

        exit

    fi

done
```

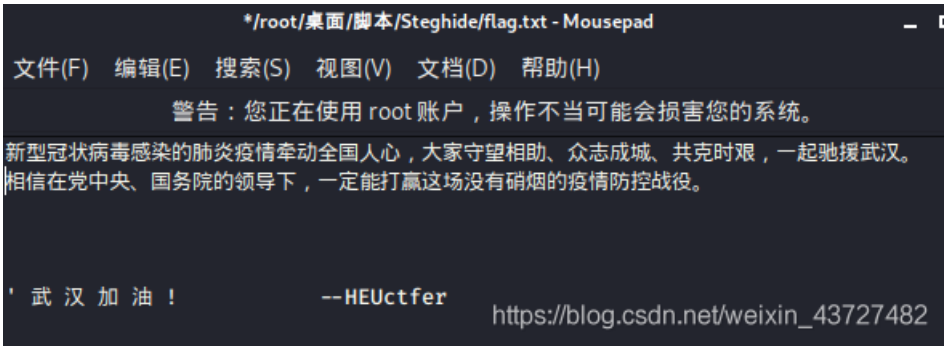
使用方法：

./bruteStegHide.sh 2.jpg passwd.txt

爆了半天没爆出来（字典不够强大（出题人太狗））

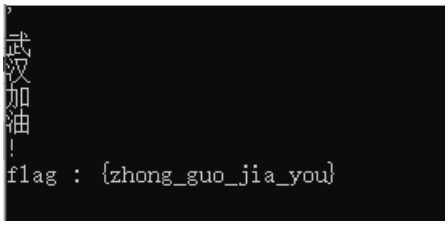
后来才知道密码是“ctf”，我特么心态崩了啊！

得到flag.txt



打开flag.exe

输入“ ' 武 汉 加 油 ！ ”得到flag



中国加油！