看雪CTF-MISC类型题之巍然不动

原创

李钰铖 于 2021-04-24 11:14:50 发布 230 收藏

分类专栏： 笔记 CTF做题笔记 文章标签： 信息安全 经验分享


笔记 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏


CTF做题笔记

2 篇文章 0 订阅

订阅专栏

题干：

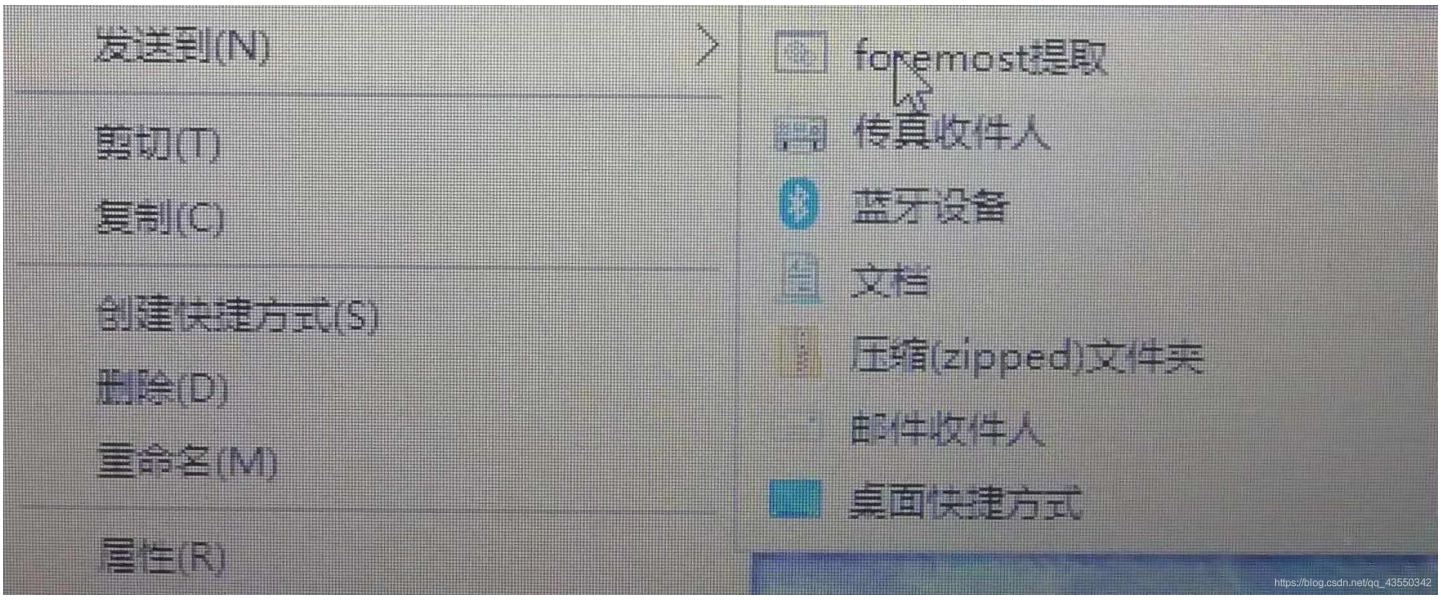
> 隐写题。\"I am not crazy, my mother had me tested.\" (Sheldon) What did Sheldon … huh sorry, Dr. Cooper really mean? 请下载wrbd.zip。

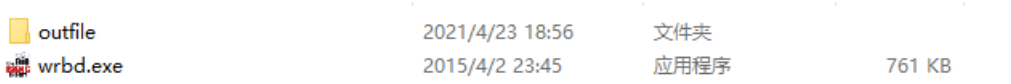
1. 这是一道隐写题，先将wrbd.zip文件解压，解压之后发现有一个exe文件，双击之后会发现只有一张谢耳朵教授的照片，可能有的人会误认为这是道逆向题吧，题干中已经很清楚地描述了这是一道隐写题，所以我们要用到foremost这个工具来找出隐写的文件，foremost的安装教程与下载链接详见下方参考网址。

> 解压之后（杀毒软件会把此文件当作是病毒，需要恢复此文件）

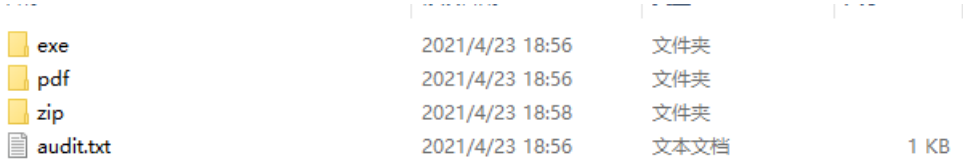
> 双击exe文件

用foremost找出隐写文件



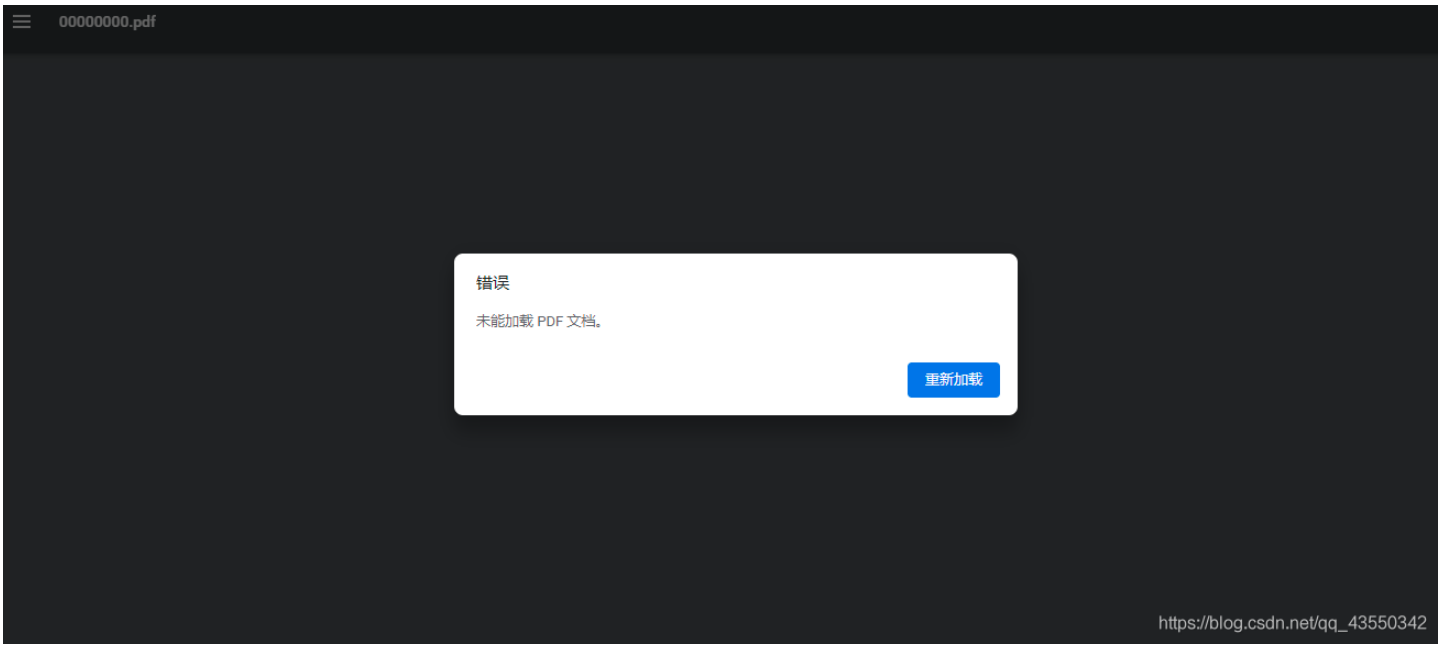


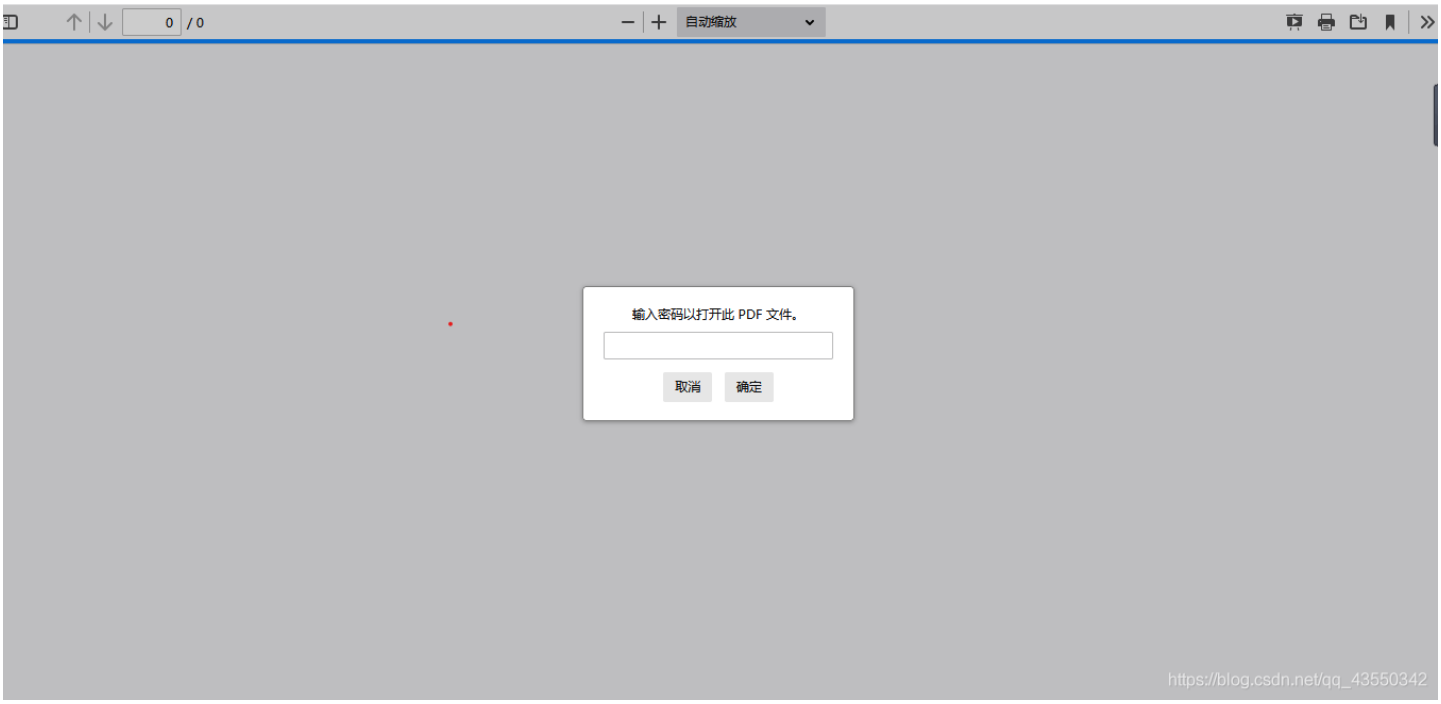
输出文件有三个文件夹与一个文件



打开zip文件夹，解压zip文件，发现是Stegano-BMP的源码，因为是小白所以还不懂什么是Stegano-BMP，随后查看相关的WP发现此文件给出来的信息并不是想要的，所以本小白果断放弃。

双击pdf文件发现，用WPS以及chrome，IE等浏览器都无法打开这个文件，试了一下firefox浏览器打开发现这个pdf文件需要密码





2. 这时想到有款叫pdfcrack的工具可以破解pdf密码，随后用kaliLinux来破解**00000000.pdf**，在kali中自带一本rockyou.txt的字典，用它来爆破这个文件足以。

> 首先pdfcrack不属于kali的默认安装工具，所以需要apt一下

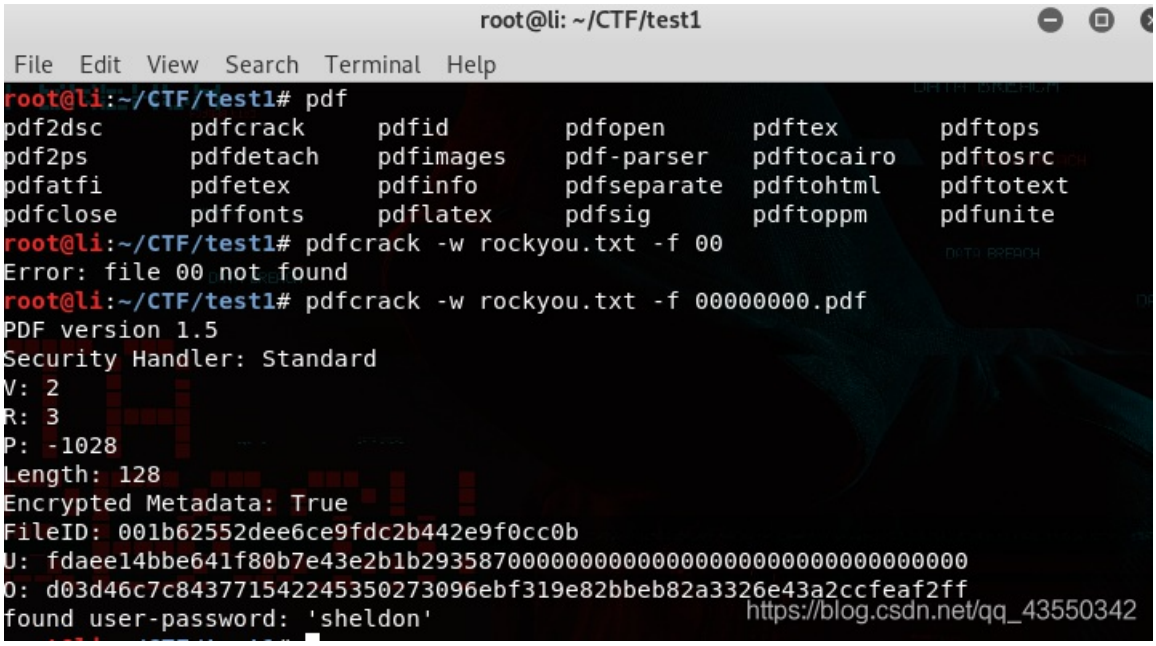
```
apt-get install pdfcrack
```

> rockyou.txt这本字典在 **/usr/share/wordlists** 目录下，最开始默认以.gz的压缩包形式存在，需要gzip解压出**rockyou.txt**文件，再复制到test文件夹下

```
gzip -d rockyou.txt.gz
cp /usr/share/wordlists/rockyou.txt ~/CTF/test1
```

> 将**00000000.pdf**复制到test1文件夹下，使用pdfcrack解密此pdf文件

```
pdfcrack -w rockyou.txt -f 00000000.pdf
```



密码为：sheldon

3. 用这个密码通过firefox浏览器打开pdf文件，可以得到flag以及霍金和谢耳朵的合影

StephenHawkingSpentSomeTimeOnSteganoTrolling

flag为：**StephenHawkingSpentSomeTimeOnSteganoTrolling**

参考：

相关WP:

https://ctf.pediy.com/itembank-writeup_details-31.htm

foremost安装网址与文件包：

https://www.cnblogs.com/cnnnnnn/p/8994362.html

https://github.com/raddyfiy/foremost