

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](#)

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/qq_43550342/article/details/116069762

版权



[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)

 wrbd.exe

2021/4/24 9:24

应用程序

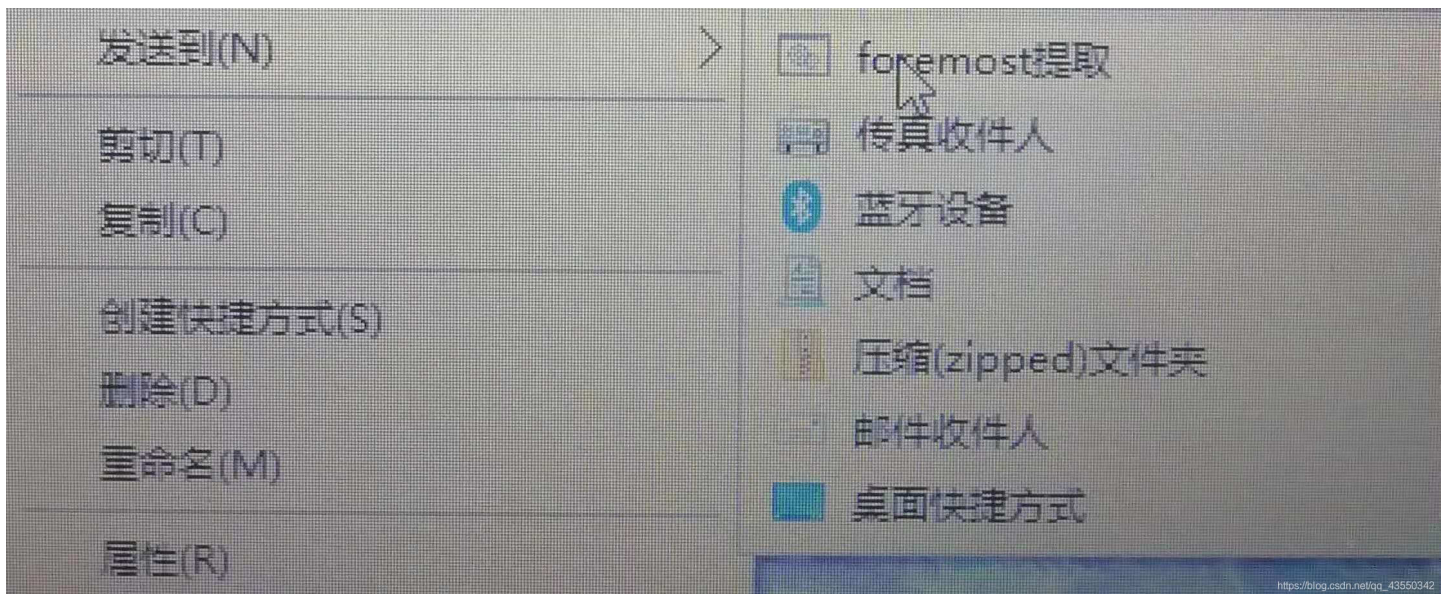
761 KB

https://blog.csdn.net/qq_43550342

双击exe文件



用foremost找出隐写文件



outfile
wrbd.exe

2021/4/23 18:56
2015/4/2 23:45

文件夹
应用程序

761 KB

https://blog.csdn.net/qq_43550342

输出文件有三个文件夹与一个文件

| | | | |
|-----------|-----------------|------|------|
| exe | 2021/4/23 18:56 | 文件夹 | |
| pdf | 2021/4/23 18:56 | 文件夹 | |
| zip | 2021/4/23 18:58 | 文件夹 | |
| audit.txt | 2021/4/23 18:56 | 文本文档 | 1 KB |

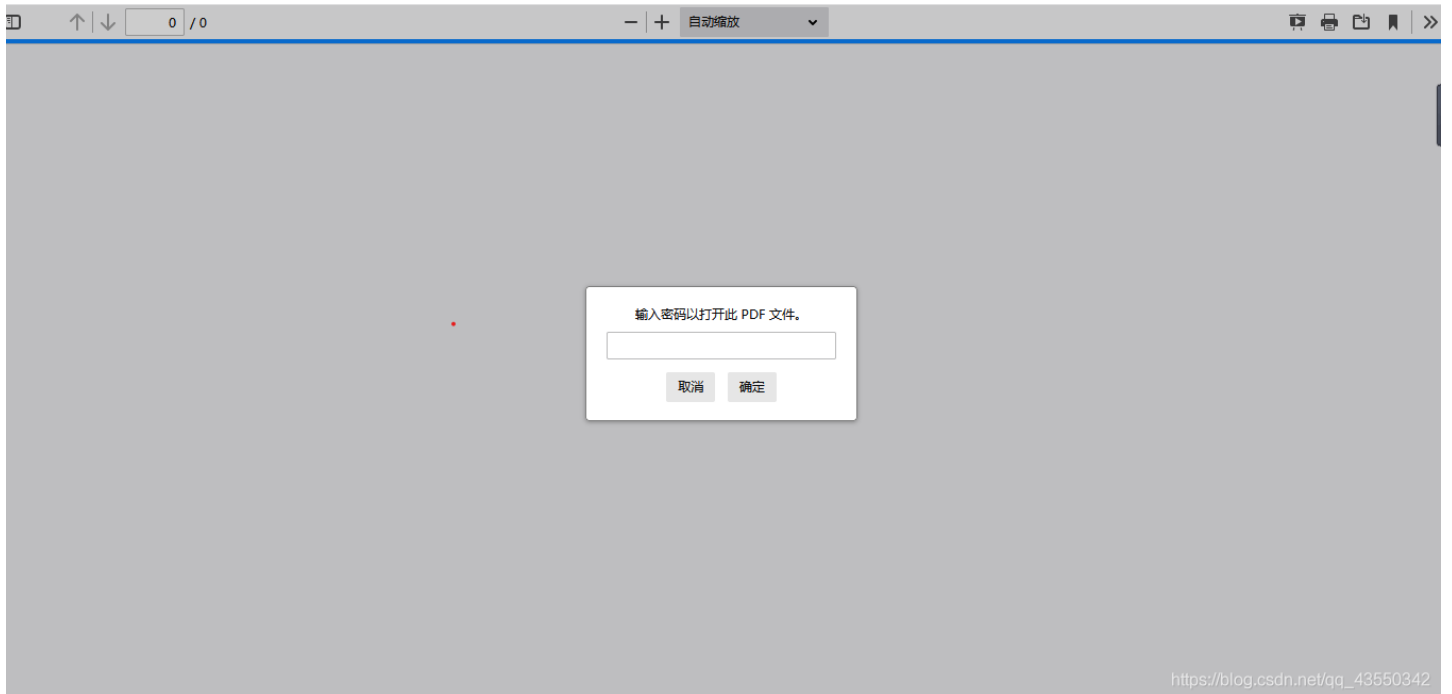
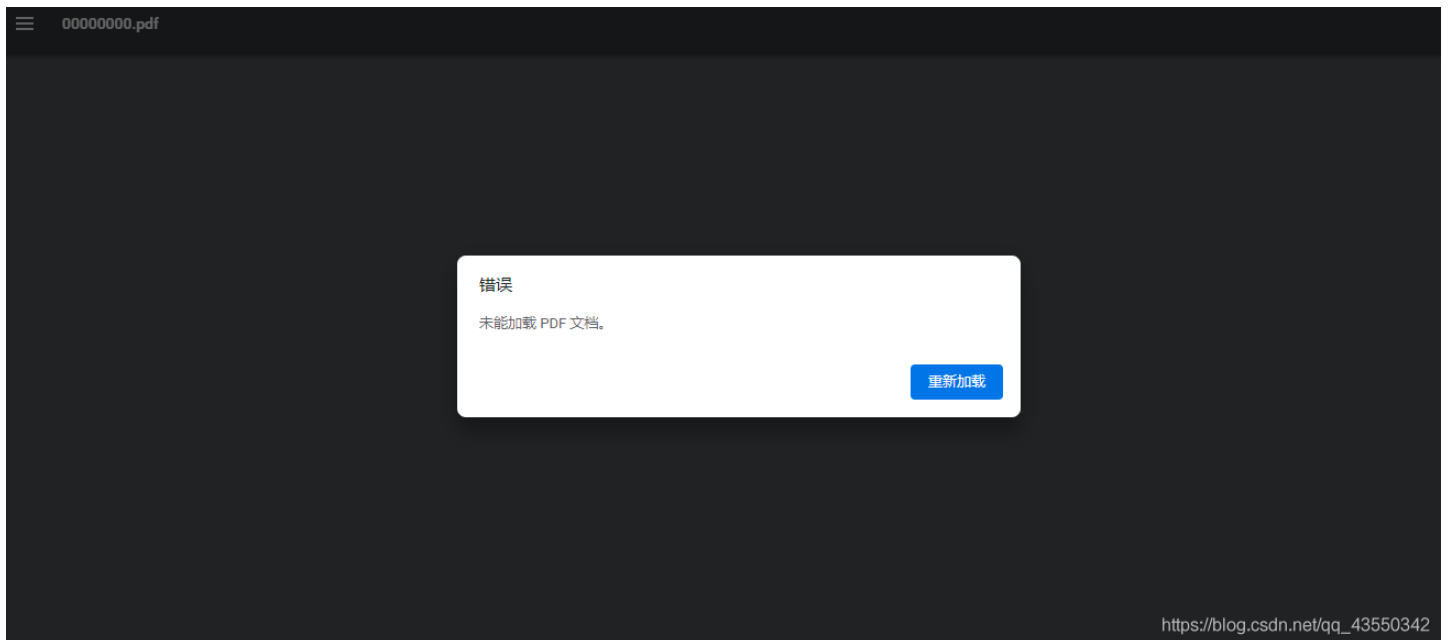
https://blog.csdn.net/qq_43550342

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。



https://blog.csdn.net/qq_43550342

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 0000000.pdf
```

```
root@li: ~/CTF/test1
File Edit View Search Terminal Help
root@li:~/CTF/test1# pdf
pdf2dsc      pdfcrack      pdfid         pdfopen      pdftex      pdftops
pdf2ps      pdfdetach     pdfimages     pdf-parser   pdftocairo  pdftosrc
pdfatfi     pdfetex      pdfinfo      pdfseparate  pdftohtml   pdftotext
pdfclose    pdffonts     pdflatex     pdfsig       pdftoppm    pdfunite
root@li:~/CTF/test1# pdfcrack -w rockyou.txt -f 00
Error: file 00 not found
root@li:~/CTF/test1# pdfcrack -w rockyou.txt -f 00000000.pdf
PDF version 1.5
Security Handler: Standard
V: 2
R: 3
P: -1028
Length: 128
Encrypted Metadata: True
FileID: 001b62552dee6ce9fdc2b442e9f0cc0b
U: fdaee14bbe641f80b7e43e2b1b29358700000000000000000000000000000000
O: d03d46c7c843771542245350273096ebf319e82bbeb82a3326e43a2ccfeaf2ff
found user-password: 'sheldon'
https://blog.csdn.net/qq_43550342
```

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

https://blog.csdn.net/qq_43550342

flag为: StephenHawkingSpentSome TimeOnSteganoTrolling

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/cnnnnn/p/8994362.html>

<https://github.com/raddyfiy/foremost>