

【CTF题目】01巍然不动 MISC 隐写

原创

铂鄂 于 2022-04-28 00:21:07 发布 8 收藏

分类专栏: [CTF # MISC](#) 文章标签: [网络安全 linux](#)

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/Zhiend/article/details/124462966>

版权



[CTF 同时被 2 个专栏收录](#)

1 篇文章 0 订阅

订阅专栏



[MISC](#)

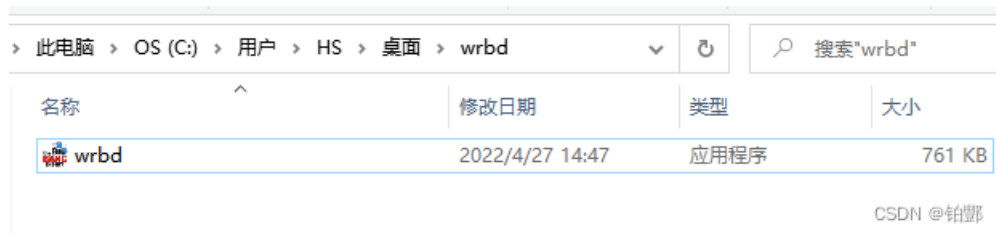
1 篇文章 0 订阅

订阅专栏

MISC 隐写

题目LINK.

【看雪】

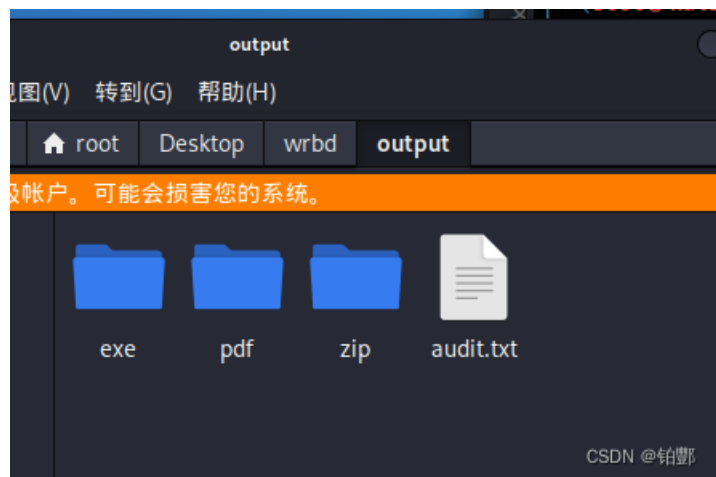


CSDN @铂鄂

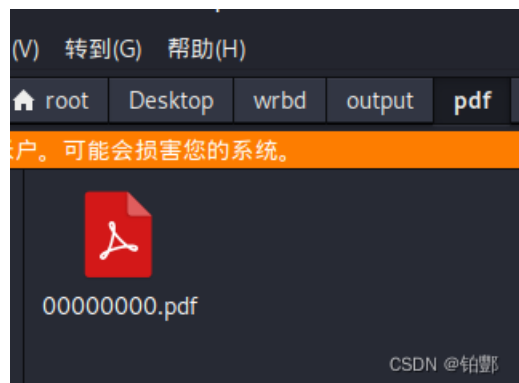
kali linux

正确流程

binwalk 文件分析
foremost 文件分离

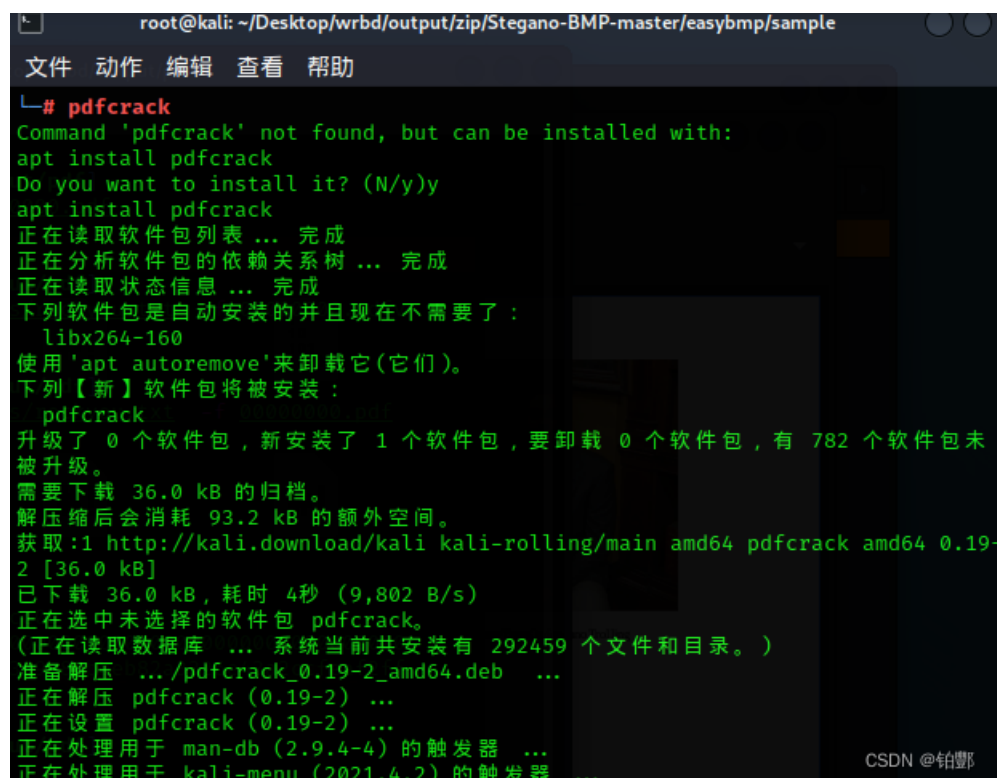


得到一个pdf和一个文件夹



PDF打开需要密码

使用pdfcrack



使用kali自带的字典

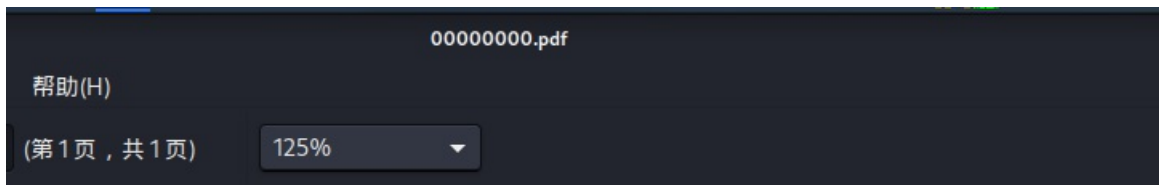
文件目录在/usr/share/wordlists/

进去解压rockyou.txt

```
(root@kali) - [~/Desktop/wrbd/output/pdf]
# pdftocrack -w /usr/share/wordlists/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: fdaee14bbe641f80b7e43e2b1b293587000000000000000000000000000000000000
O: d03d46c7c843771542245350273096ebf319e82bbeb82a3326e43a2ccfeaf2ff
found user-password: 'sheldon'
```

得出密码sheldon

打开pdf 输入密码获得flag StephenHawkingSpentSomeTimeOnSteganoTrolling



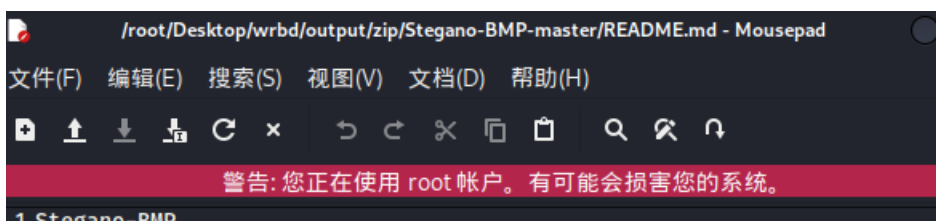
StephenHawkingSpentSomeTimeOnSteganoTrolling

CSDN @铂野

错误的尝试

猜测密码可能在文件夹内，于是打开文件夹

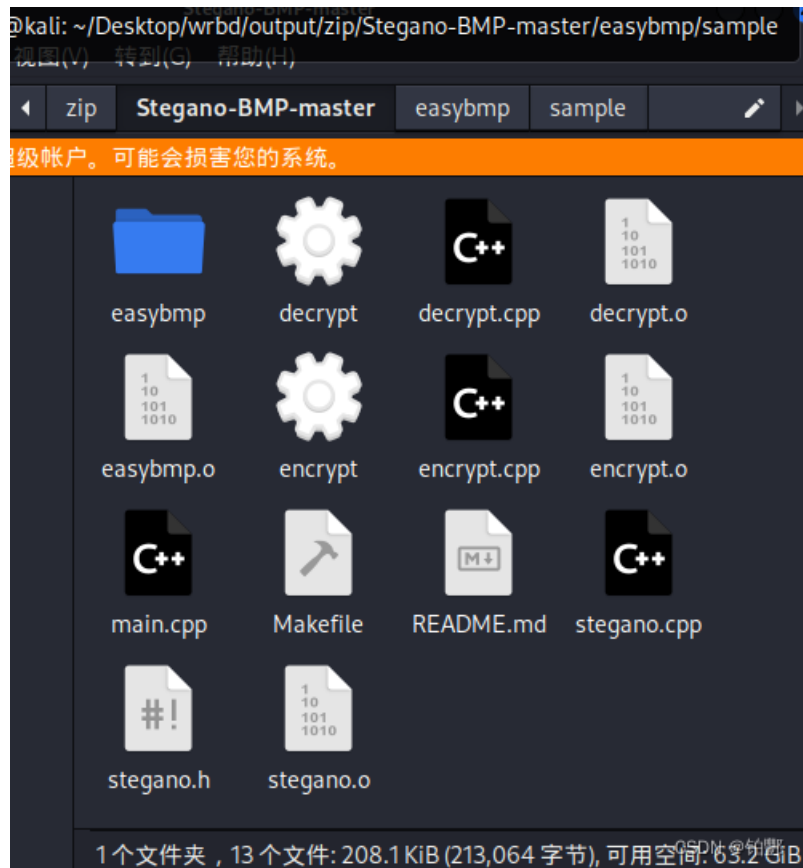
文件夹内readme:



```
1 Stegano-BMP
2 =====
3
4 A Program to hide information in bmp-files
5
6 To build, run `make`
7
8 To install on Linux, run `make install`
9
10 To install on Windows, hahahaha no.
11
12 Use encrypt to hide information, use decrypt to extract information.
13 |
```

CSDN @铂豐

根据以上步骤，获得了加解密



然后进入/root/Desktop/wrbd/output/zip/Stegano-BMP-master/easybmp/sample/
有一个makefile

```
36
37 EasyBMPtest: EasyBMP.o EasyBMPsample.o
38     g++ $(CFLAGS) EasyBMP.o EasyBMPsample.o -o EasyBMPtest
39
40 EasyBMP.o: ../EasyBMP.cpp ../EasyBMP*.h
41     cp ../EasyBMP*.h .
42     cp ../EasyBMP.cpp .
43     g++ $(CFLAGS) -c EasyBMP.cpp
44
45 EasyBMPsample.o: EasyBMPsample.cpp
46     g++ -c EasyBMPsample.cpp
47
48 clean:
49     rm EasyBMP*.h
50     rm EasyBMP.cpp
51     rm EasyBMPtest*
52     rm EasyBMPoutput*.bmp
53     rm -f *.o
54
```

CSDN @铂豐

猜测可能需要，完成EasyBMPoutput*.bmp的输出，然后把输出的图片进行解密得出一个密码
根据以上说明

```
文件 动作 编辑 查看 帮助
(root@kali)-[~/../zip/Stegano-BMP-master/easybmp/sample]
└─# cp ../EasyBMP.cpp .
(root@kali)-[~/../zip/Stegano-BMP-master/easybmp/sample]
└─# cp ../EasyBMP*.h .
(root@kali)-[~/../zip/Stegano-BMP-master/easybmp/sample]
└─# g++ -O3 -pipe -fomit-frame-pointer -funroll-all-loops -s -c EasyBMP.c
(root@kali)-[~/../zip/Stegano-BMP-master/easybmp/sample]
└─# g++ -c
g++: fatal error: no input files
compilation terminated.
(root@kali)-[~/../zip/Stegano-BMP-master/easybmp/sample]
└─# g++ -c EasyBMPsample.cpp
```

CSDN @铂野



得到

后, 运行生成EasyBMPoutput*.bmp, 然后decrypt

```
(root@kali)-[~/.../zip/Stegano-BMP-master/easybmp/sample]
└─# g++ -O3 -pipe -fomit-frame-pointer -funroll-all-loops -s EasyBMP.o EasyBMPsample.o -o EasyBMPtest

(root@kali)-[~/.../zip/Stegano-BMP-master/easybmp/sample]
└─# decrypt /root/Desktop/wrbd/output/zip/Stegano-BMP-master/easybmp/sample/EasyBMPoutput4bpp.bmp

(root@kali)-[~/.../zip/Stegano-BMP-master/easybmp/sample]
└─# decrypt /root/Desktop/wrbd/output/zip/Stegano-BMP-master/easybmp/sample/EasyBMPoutput8bpp.bmp
```

```
(root@kali)-[~/.../zip/Stegano-BMP-master/easybmp/sample]
└─# decrypt /root/Desktop/wrbd/output/zip/Stegano-BMP-master/easybmp/sample/EasyBMPoutput32bpp.bmp
♦

(root@kali)-[~/.../zip/Stegano-BMP-master/easybmp/sample]
└─# decrypt /root/Desktop/wrbd/output/zip/Stegano-BMP-master/easybmp/sample/EasyBMPoutput24bpp_rescaled.bmp
♦

(root@kali)-[~/.../zip/Stegano-BMP-master/easybmp/sample]
└─# decrypt /root/Desktop/wrbd/output/zip/Stegano-BMP-master/easybmp/sample/EasyBMPoutput24bpp.bmp
♦
```

最后三个图片, 解出来乱码

看writeup有解出来3, 搞不出来

难道是有3个?

看了评论 3像耳朵

收敛一下 sheldon =谢耳朵

生活大爆炸, 题目的台词搜了也是

总结

分离文件 foremost好用

对pdf的破解可以使用pdfcrack

pdfcrack

pdfcrack -w 字典文件 -f 破解pdf

kali自带的字典所在/usr/share/wordlists/rockyou.txt

```
(root@kali)-[~]
└─# pdfcrack
Usage: pdfcrack -f filename [OPTIONS]
OPTIONS:
-b, --bench           perform benchmark and exit
-c, --charset=STRING Use the characters in STRING as charset
-w, --wordlist=FILE  Use FILE as source of passwords to try
-n, --minpw=INTEGER  Skip trying passwords shorter than this
-m, --maxpw=INTEGER  Stop when reaching this passwordlength
-l, --loadState=FILE Continue from the state saved in FILENAME
-o, --owner           Work with the ownerpassword
-u, --user           Work with the userpassword (default)
-p, --password=STRING Give userpassword to speed up breaking
                    ownerpassword (implies -o)
-q, --quiet          Run quietly
-s, --permutate      Try permutating the passwords (currently only
                    supports switching first character to uppercase)
-v, --version        Print version and exit
```

CSDN @铂豐