网络安全CTF夺旗赛入门到入狱-杂项（文件隐写篇）

原创

菜鸡林某 于 2021-12-09 21:25:51 发布 161 收藏 3

分类专栏： CTF新手入门篇 文章标签： 安全 网络安全 密码学

本文链接：https://blog.csdn.net/qq_45149716/article/details/121843123

哈喽大家好，我是菜鸡林某。

今天给大家带来CTF夺旗赛入门的第一步杂项篇

本篇预计也是分为好几个个部分因为他比较多

往期传送门：

网络安全CTF夺旗赛入门到入狱-入门介绍篇

网络安全CTF夺旗赛入门到入狱-密码学上篇

网络安全CTF夺旗赛入门到入狱-密码学下篇

今天主要就讲一个内容

- 文件操作与隐写

文件操作与隐写

1. 文件类型识别

文件无后缀 ：

File命令

当文件没有后缀名或者有后缀名而无法正常打开时，根 据识别出的文件类型来修改后缀名即可正常打开文件。

使用场景：不知道后缀名，无法打开文件。

格式：file filename

```
root@kali2:~/ctf# file myheart
myheart: pcap-ng capture file - version 1.0
```

Winhex

通过winhex程序中可以查看文件头类型，根据文件头类型判断出文件类型

使用场景：windows下通过文件头信息判断文件类型

常见的文件头类型如图所示

文件类型	文件头
JPEG (jpg)	FFD8FFE1
PNG (png)	89504E47
GIF (gif)	47494638
TIFF (tif)	49492A00
Windows Bitmap (bmp)	424DC001
ZIP Archive (zip)	504B0304
RAR Archive (rar)	52617221
Adobe Photoshop (psd)	38425053
Rich Text Format (rtf)	7B5C727466
XML (xml)	3C3F786D6C
HTML (html)	68746D6C3E
Adobe Acrobat (pdf)	255044462D312E
Wave (wav)	57415645
pcap (pcap)	4D3C2B1A

文件头残缺/错误：

通常文件无法正常打开有两种情况，一种是文件头部残缺，另一种是文件头部字段错误。针对文件 头部残缺的情况，使用winhex程序添加相应的文件头，针对头部字段错误，可以找一个相同类型的文 件进行替换。

使用场景：文件头部残缺或文件头部字段错误无法打开正常文件。

格式：file 文件名!

2.文件分离操作

Binwalk 工具

Binwalk是Linux下用来分析和分离文件的工具，可以快速分辨文件 是否由多个文件合并而成，并将文件进行分离。如果分离

成功会在目标文 件的目录。同目录下生成一个形如_文件名_extracted的文件目录，目录中有 分离后的文件。

用法： 分析文件：binwalk filename 分离文件：binwalk –e filename

```
root@kali2:~/ctf# binwalk ans.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
8232          0x2028          TIFF image data, big-endian
19610         0x4C9A          Copyright string: " (c) 1998 Hewlett-Packard Companyny"
```

`foremost`

如果binwalk无法正确分离出文件，可以使用foremost，将目标文件复制 到kali中，成功执行后，会在目标文件的文件目录下生成我们设置的目录，目录 中会按文件类型分离出文件。

用法： foremost 文件名 –o 输出目录名

```
root@kali2:~/ctf# foremost oddpic.jpg -o oddpic
Processing: oddpic.jpg
|*|
```

`dd`

当文件自动分离出错或者因为其他原因无法自动分离时，可以使用dd实现文件手动分离。

格式： dd if=源文件 of=目标文件名 bs=1 skip=开始分离的字节数

参数说明：

if=file #输入文件名，缺省为标准输入。

of=file #输出文件名，缺省为标准输出。

bs=bytes #同时设置读写块的大小为 bytes ， 可代替 ibs 和 obs 。

skip=blocks #从输入文件开头跳过 blocks 个块后再开始复制。

1.txt
1234567890abcdefg

dd if=1.txt of=2.txt bs=5 count=1

dd if=1.txt of=3.txt bs=5 count=2

2.txt:
12345

3.txt:
1234567890

dd if=1.txt of=4.txt bs=5 count=3 skip=1

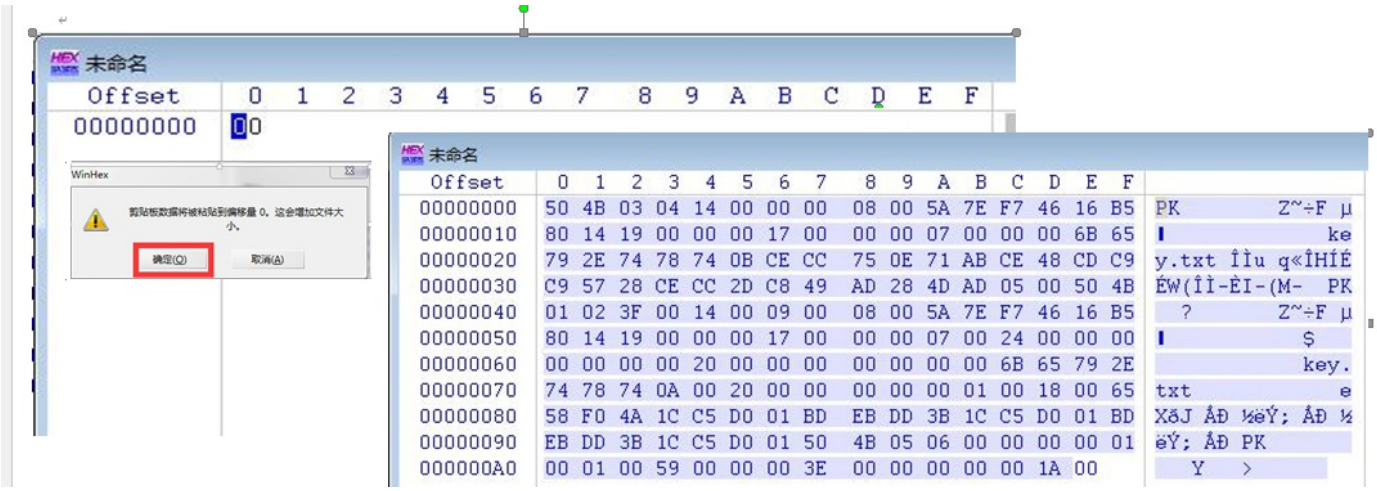
4.txt:
67890abcdefg

`winhex`

除了使用dd外，还可以使用winhex实现文件手动分离，将目标文件拖入winhex中，找到 要分离的部分，点击复制即可。 除了使用dd外，还可以使用winhex实现文件手动分离，将目标文 件拖入winhex中，找到要分离的部分，点击复制即可。

使用场景：windows下利用winhex程序对文件进行手动分离

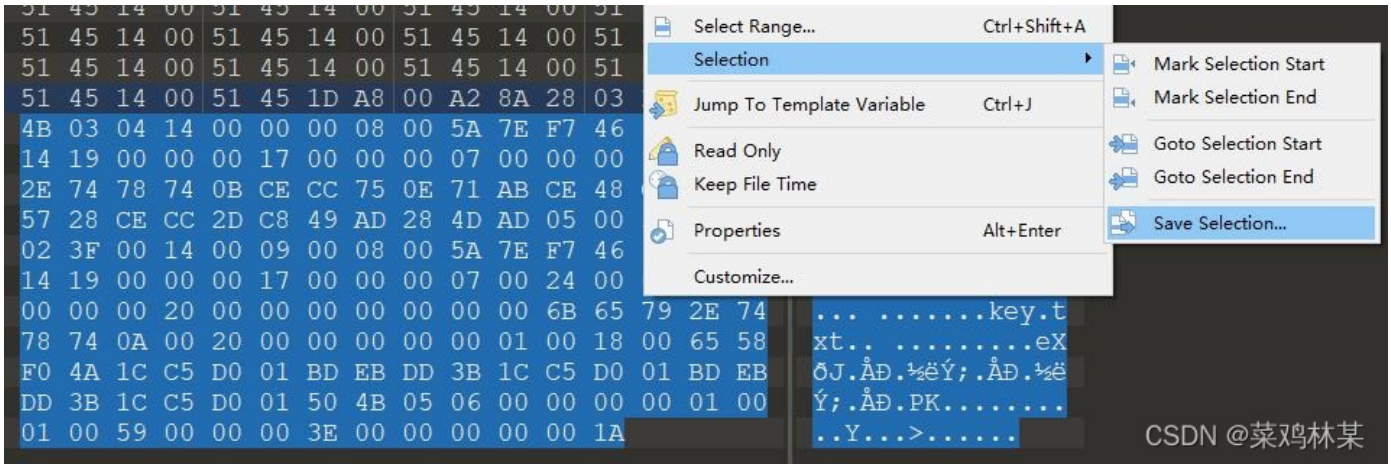
例：新建一个文件，文件大小1byte，在文件开头位置点击粘贴，弹出提示框选否、确定，将文件 保存为想要的后缀即可



`010Editor`

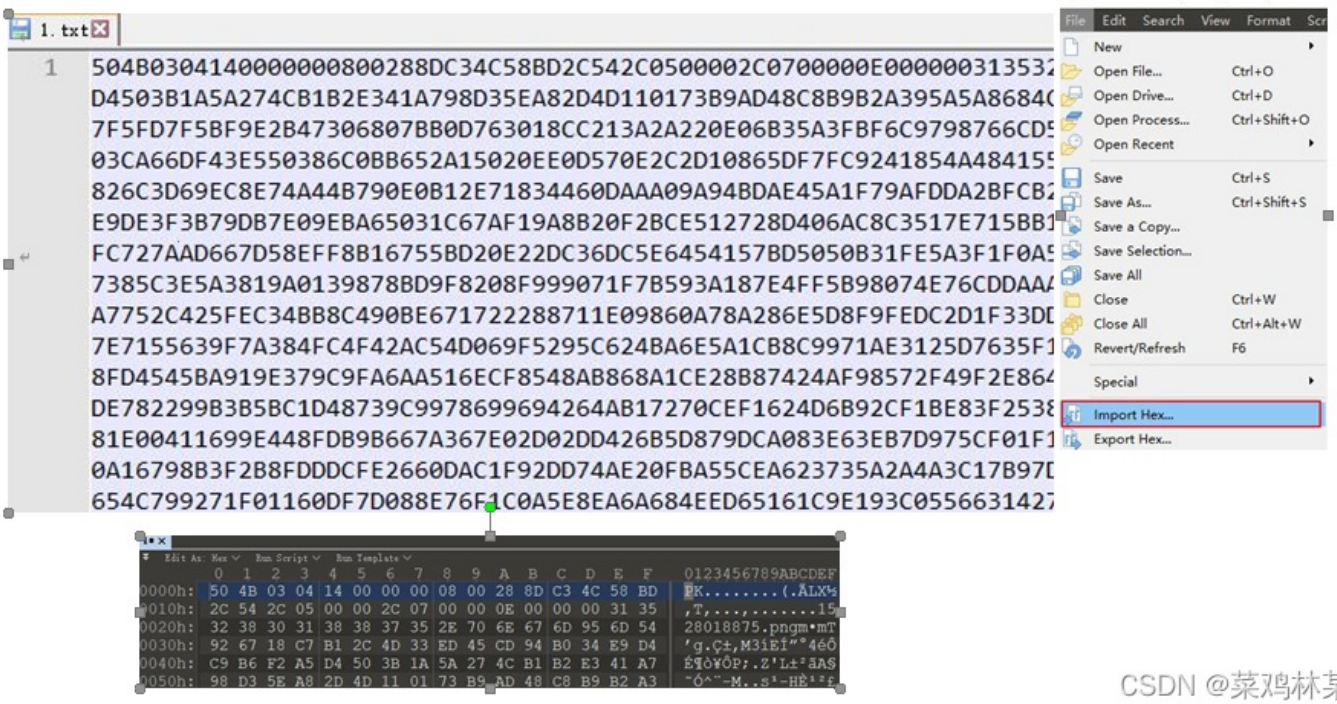
将某块区域文件保存的方式如下：

- 010Editor打开文件
- 选中右键
- Selection
- Save Selection



将16进制字符文件导入保存操作方法如下：

- 将16进制字符文件保存在一个文件
- 打开010Editor import Hex



文件合并

1. Linux下的文件合并

   使用场景：linux下,通常对文件名相似的文件要进行批量合并

   格式： cat 合并的文件 > 输出的文件

```
root@kali2:~/ctf/cat# cat chapter01 chapter02 chapter03 > book
root@kali2:~/ctf/cat# cat chapter* > book1
```

   •完整性检测：linux 下计算文件md5：

   md5sum 文件名

```
reborn@Oooo:/mnt/d/forkali$ md5sum sim.jpg
d09e8a07b6dedb0633aa3c432f931362  sim.jpg
```

2. Windows下的文件合并

   使用场景：windows下，通常要对文件名相似的文件进行批量合并

   格式： copy /B 合并的文件 输出的文件命令

```
D:\CTF\copy>copy /B chapter01+chapter02+chapter03 book
chapter01
chapter02
chapter03
已复制         1 个文件。

D:\CTF\copy>copy /B chapter* book1
chapter01
chapter02
chapter03
已复制         1 个文件。
```


   •完整性检测：windows下计算文件md5：

   certutil -hashfile 文件名 md5

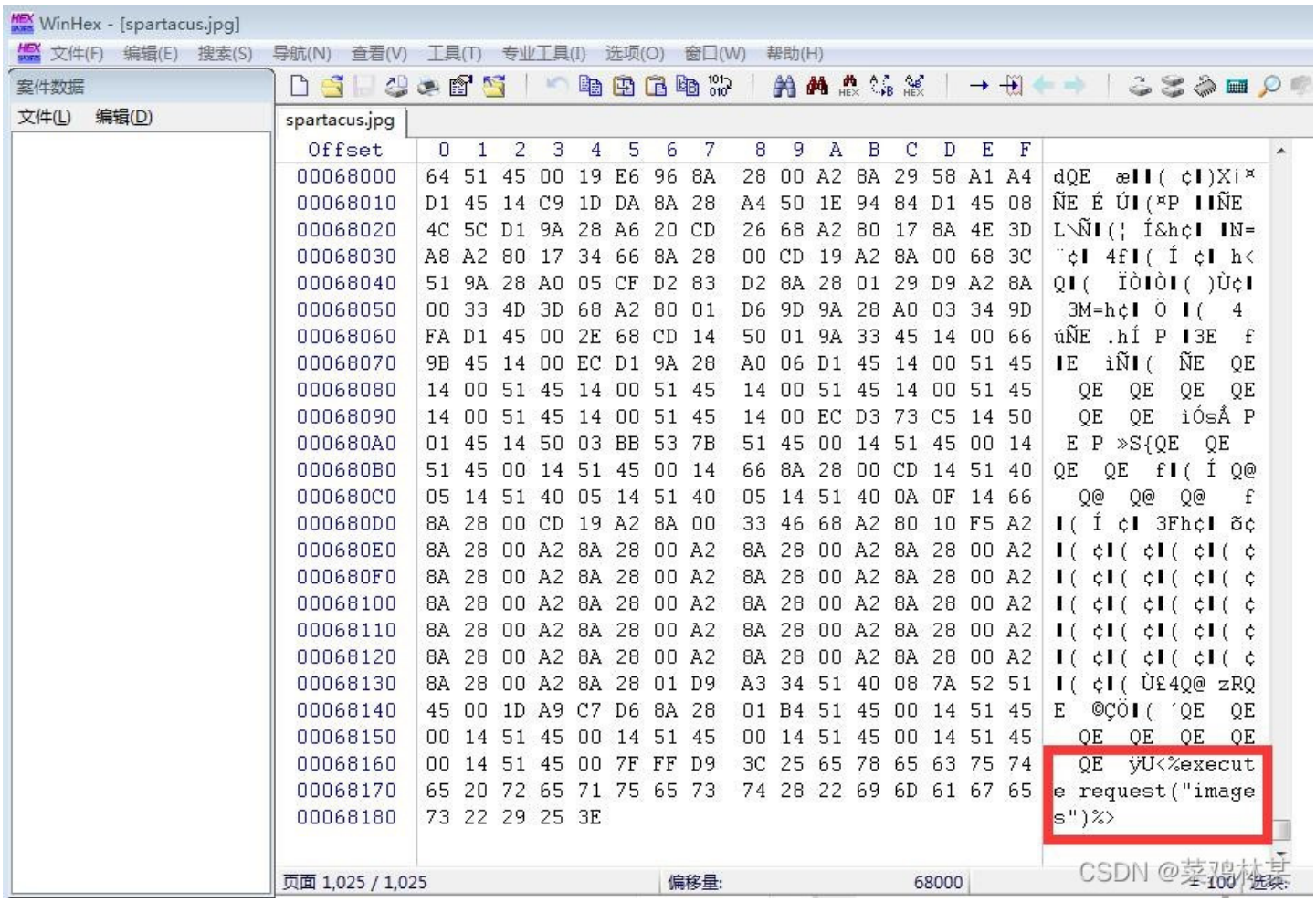
```
reborn@OOOO D:\forkali
# certutil -hashfile sim.jpg md5
MD5 的 sim.jpg 哈希:
d09e8a07b6dedb0633aa3c432f931362
CertUtil: -hashfile 命令成功完成。
```

文件内容隐写

文件内容，就是直接将KEY以十六进制的形式写在文件中，通常在文件的开头或结尾部分， 分析时通常重点观察文件开头和结尾部分。如果在文件中间部分，通常搜索关键字KEY或者flag 来查找隐藏内容。 使用场景：windows下，搜索隐写的文件内容

- Winhex/010Editor

通常将要识别的文件拖入winhex中， 查找具有关键字或明显与文件内容不和谐的部 分,通常优先观察文件首部和尾部，搜索flag或key等关键字，最后拖动滚轮寻找。



Notepad++

使用notepad++打开文件，查看文件头尾是否有

含有关键字的字符串，搜索flag或key等关键字，最后拖
动滚轮寻找。

另外通过安装插件HEX-Editor可以实现winhex的功能。