
CTF 解题技能之 MISC 基础一

CTF 解题技能之 MISC 基础一	1
前言	2
（一）杂项介绍	3
杂项大致有几种类型：	3
0x00 文件类型识别	4
1. file 命令	4
2. 010Editor	4
0x01 文件分离	7
1. Binwalk	7
Linux 安装 Binwalk	7
2. foremost	8
Kali 安装 foremost	8
3. dd	9
4. fcrackzip	9
5. 010Editor	10
练习部分：	11
0x02 文件合并	11
1. linux 环境文件合并	12
2. windows 环境文件合并	12
3. Python 文件合并	12
0x03 总结	13

前言

以下是我近两个月对 MISC 的学习，学习思路大多来源于网络，因为学习过程查询的资料太多，部分资料记录了原文链接，部分资料原文链接忘了记录。

本人只是在前人学习的基础上做了系统的整理。

来源于网络，回馈于网络~

整理后资料分为两个部分《CTF 解题技能之 MISC 基础一》和《CTF 解题技能之 MISC 基础二》，目录结构如下：

CTF 解题技能之 MISC 基础	1
（一）杂项介绍	2
杂项大致有几种类型：	3
0x00 文件类型识别	3
1. file 命令	4
2. 010Editor	4
0x01 文件分离	6
1. Binwalk	7
Linux 安装 Binwalk	7
2. foremost	7
Kali 安装 foremost	8
3. dd	8
4. fcrackzip	9
5. 010Editor	9
练习部分：	10
0x02 文件合并	11
1. linux 环境文件合并	11
2. windows 环境文件合并	11
3. Python 文件合并	12
0x03 总结	12
（二）隐写术总结—CTF 指南	13
1) 图片隐写术	13
1. 图种	13
破解方法一：	13
破解方法二：	13
2. LSB 隐写	13
3. 文件格式缺失&GIF 隐写	14
4. stegsolve—图片隐写查看器	14
练习部分：	15
练习部分：	15
2) 压缩包隐写术	15
3) 音频及视频隐写术	15
1. MP3 隐写术	15
练习部分：	16
2. 频谱隐写	16
练习部分：	17
摩斯密码	17
练习部分：	17
4) 进制转换与加解密	18

5) RGB 值.....	18 ^u
RGB 值.....	18 ^u
6) 游戏隐写	18 ^u
练习部分:	18 ^u
7) 颜文字	19 ^u
8) 其他	19 ^u
1、PDF 隐写	19 ^u
2、DOC 隐藏	19 ^u
3、数据包隐写术.....	20 ^u
练习部分:	20 ^u
4、linux 隐写	21 ^u
练习部分:	21 ^u
5、其他练习部分:	21 ^u
(三) PNG 文件格式详解	21 ^u
文件结构	21 ^u
一个例子	22 ^u
练习部分:	24 ^u
(四) 根据文件头数据判断文件类型.....	24 ^u
练习部分:	25 ^u
(五) 压缩包解密的几种方法.....	25 ^u
压缩包解密通用方法:	25 ^u
1、zip 伪加密	25 ^u
2、crc32 碰撞:	26 ^u
已知明文攻击即 crc32 爆破:	27 ^u
3、直接爆破:	29 ^u
练习部分:	30 ^u

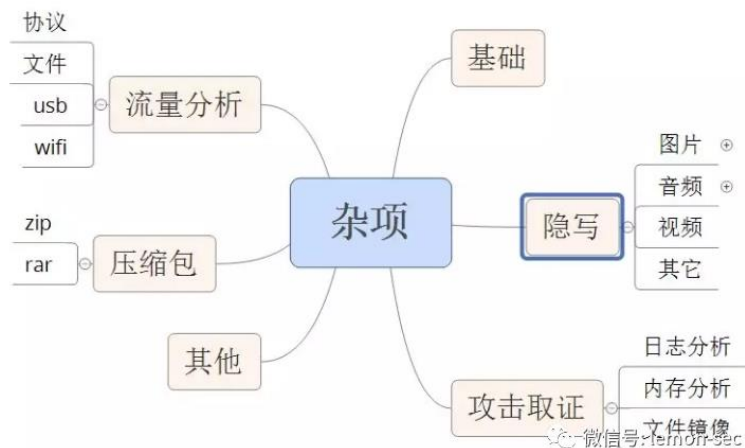
红圈外的部分会在《CTF 解题技能之 MISC 基础二》中介绍。

(一) 杂项介绍

Miscellaneous 简称 MISC，意思是杂项，混杂的意思。

杂项大致有几种类型：

1. 隐写
2. 压缩包处理
3. 流量分析
4. 攻击取证
5. 其它



本篇主要介绍杂项基础题目的知识点以及解题思路。

0x00 文件类型识别

杂项题目主要是以文件附件作为题目，但是给的文件不一定是带后缀名的，这就需要我们识别这些文件

1. file 命令

file 命令实际上是一个命令行工具，用来查看文件类型。

使用方法：

将文件复制到 kail 或者带有 file 工具的系统中，使用 file 查看文件。

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

将文件后缀名补上即可正常打开。

然后根据实际情况进行初步判断可能是什么类型的题目。

2. 010Editor

010Editor 是一款快速且强大的十六进制编辑器。用来编辑二进制文件。有一个友好易于使用的界面，无限次的 undo 和 redo 操作。另外还可以打印 x 十六进制的字节或者以书签的方式标出某些重要的字节。我们可以通过使用 010Editor 查看文件的头部来判断类型。

以下是常见的文件头：

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)	4D3C231A

根据文件头数据判断文件类型。

PNG 文件头中包含 IHDR 信息。

编辑为: 十六进制(H)	运行脚本	运行模板	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	00	0D	49	48	44	52		%PNG.....IHDR
0010h:	00	00	07	80	00	00	04	38	08	02	00	00	00	00	67	B1	56		...e...8.....g±V
0020h:	14	00	00	21	32	49	44	41	54	78	DA	EC	D8	31	01	00			...!2IDATxÜiØ1..
0030h:	00	0C	83	B0	FA	37	BD	A9	E0	4B	24	70	B2	03	00	00			..f°ú7*caKsp²...
0040h:	00	00	80	C0	24	00	00	00	00	00	A0	60	40	03	00	00			..eAs.....`@...
0050h:	00	00	90	30	A0	01	00	00	00	00	48	18	D0	00	00	00			...0.....H.D...
0060h:	00	00	24	0C	68	00	00	00	00	00	12	06	34	00	00	00			...H.D...
0070h:	00	00	09	03	1A	00	00	00	00	80	84	01	0D	00	00	00		e.....

IHDR 的作用将在后续的图片类隐写中详细讲解：（四）PNG 文件格式的介绍

当文件类型不确定时就可以尝试查看文件头来判断。

编辑为: 十六进制(H)	运行脚本	运行模板: ZIP.bt	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	50	4B	03	04	14	00	00	00	00	00	16	A9	52	4D	00	00			PK.....@RM..
0010h:	00	00	00	00	00	00	00	00	00	00	0F	00	1D	00	D0	C2		DÂ
0020h:	BD	A8	CE	C4	BC	FE	BC	D0	20	28	32	29	2F	75	70	19			%iA*pb*(2)/up.
0030h:	00	01	4E	3F	42	F5	E6	96	B0	E5	BB	BA	E6	96	87	E4			..N?B0æ-°â»°æ-tâ
0040h:	BB	B6	E5	A4	B9	20	28	32	29	2F	50	4B	03	04	14	00			»Iâ² (2)/PK....
0050h:	00	00	00	00	1A	A9	52	4D	00	00	00	00	00	00	00	00		@RM..
0060h:	00	00	00	00	1A	00	[2C	00]	D0	C2	BD	A8	CE	C4	BC	FE		,DÂ* iA*pb
0070h:	BC	D0	20	28	32	29	2F	31	2D	B5	E7	D7	D3	BD	CC	B0			%D (2)/1-µç×Ó×i°
0080h:	B8	2F	75	70	28	00	01	A1	F7	9E	85	E6	96	B0	E5	BB			/up(..;÷ž...æ-°â»
0090h:	BA	E6	96	87	E4	BB	B6	E5	A4	B9	20	28	32	29	2F	31			°æ-tâ»Iâ² (2)/1
00A0h:	2D	E7	94	B5	E5	AD	90	E6	95	99	E6	A1	88	2F	50	4B			-ç"µâ-..æ*µæ;^/PK
00B0h:	03	04	14	00	00	00	08	00	89	7D	8D	43	40	AD	96	3D		%}.C@--=
00C0h:	CB	E9	16	00	00	1E	21	00	2D	00	42	00	D0	C2	BD	A8			Ee.....!...B.DÂ*"
00D0h:	CE	C4	BC	FE	BC	D0	20	28	32	29	2F	31	2D	B5	E7	D7			iA*pb*(2)/1-µç×
00E0h:	D3	BD	CC	B0	B8	2F	B5	DA	31	30	D5	C2	20	44	41	43			...H.D...
00F0h:	D3	EB	41	44	43	2E	70	70	74	75	70	3E	00	01	BB	D0			0eADC.pptup>...»D

如果没有后缀名，也可以查看文件尾部来判断文件类型。

以下是常见的文件尾部:

zip 文件的结尾以一串 504B0506 开始。

光盘文件.zipx																		
* 编辑为: 十六进制(H) v 运行脚本 v 运行模板: ZIP.bt v D																		
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF	
825:FA10h:	D0	C2	BD	A8	CE	C4	BC	FE	BC	D0	20	28	32	29	2F	B1	DÄ"iA4p4D (2)/±	
825:FA20h:	BE	B9	E2	C5	CC	CA	B9	D3	C3	CB	B5	C3	F7	2E	70	70	%:aAiE:0AEuA+.pp	
825:FA30h:	74	0A	00	20	00	00	00	00	00	01	00	18	00	00	A6	EE	t..i	
825:FA40h:	4D	EA	0C	CF	01	32	FB	4D	B2	E3	66	D4	01	EE	4D	43	Mè.i.20M°af0.iMC	
825:FA50h:	B2	E3	66	D4	01	75	70	32	00	01	74	5B	C1	F3	E6	96	"af0.up2..t[Áóæ-	
825:FA60h:	B0	E5	BB	BA	E6	96	87	E4	BB	B6	E5	A4	B9	20	28	32	°â»°æ-+â»iâ» (2	
825:FA70h:	29	2F	E6	9C	AC	E5	85	89	E7	9B	98	E4	BD	BF	E7	94) /ææ-â...kç>"a4ç"	
825:FA80h:	A8	E8	AF	B4	E6	98	8E	2E	70	70	74	50	4B	05	06	00	"è"æ"ž.pptPK...	
825:FA90h:	00	00	00	6D	01	6D	01	A0	6B	01	00	EB	8E	24	08	00	...m..y: ežs...	
825:FAA0h:	00																微信号: lemon-sec	

rar 文件以 C43D7B00400700 结尾。


编辑为: 十六进制(H) 运行脚本 运行模板: RAR.v7.1.bt		0 1 2 3 4 5 6 7 8 9 A B C D E F																0123456789ABCDEF
15:93C0h:	59	3A	FA	40	B9	5D	74	E0	90	38	00	00	00	00	00	00	00	Y:ú@:]tä.8.....
15:93D0h:	00	00	00	02	00	00	00	00	18	60	8B	4C	14	30	13	00	00<L.O.....
15:93E0h:	10	00	00	00	73	65	72	76	65	72	5C	63	6C	69	65	6E	00	...server\client
15:93F0h:	74	5C	44	65	62	75	67	00	F0	0F	17	6F	73	53	74	E0	00	t\Debug.0...osStà
15:9400h:	90	32	00	00	00	00	00	00	00	00	00	02	00	00	00	00	00	.2.....
15:9410h:	3D	60	8B	4C	14	30	0D	00	10	00	00	00	73	65	72	76	00	=<L.O.....serv
15:9420h:	65	72	5C	63	6C	69	65	6E	74	00	F0	6D	8D	35	D7	14	00	er\client.0m.5×.
15:9430h:	74	E0	90	31	00	00	00	00	00	00	00	00	00	02	00	00	00	tà.1.....
15:9440h:	00	00	AA	5E	8B	4C	14	30	0C	00	10	00	00	00	73	65	00	..*^<L.O.....se
15:9450h:	72	76	65	72	5C	44	65	62	75	67	00	F0	ED	82	7F	0F	00	rver\Debug.0i,..
15:9460h:	38	74	E0	90	2B	00	00	00	00	00	00	00	00	00	02	00	00	8tà.+.....
15:9470h:	00	00	00	3D	60	8B	4C	14	30	06	00	10	00	00	00	73	00	...=<L.O.....s
15:9480h:	65	72	76	65	72	00	F0	CD	EE	37	C4	3D	7B	00	40	00	00	微信号: lemon-sec
15:9490h:	00																	

JPG 文件结尾为 FFD9。

2.jpg x		编辑为: 十六进制(H) 运行脚本 运行模板																0123456789ABCDEF																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																					
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																						

PNG 文件 结尾为 000049454E44AE426082。

A0.png x		编辑为: 十六进制(H) 运行脚本 运行模板																0123456789ABCDEF															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F																
20D0h:	00	80	85	80	06	00	00	00	00	60	21	A0	01	00	00	00	00	.e...e...!															
20E0h:	00	58	08	68	00	00	00	00	00	00	16	02	1A	00	00	00	00	.X.h.....															
20F0h:	80	85	80	06	00	00	00	00	00	60	21	A0	01	00	00	00	00	e...e...!															
2100h:	58	08	68	00	00	00	00	00	00	16	02	1A	00	00	00	00	80	X.h.....e															
2110h:	85	80	06	00	00	00	00	00	60	21	A0	01	00	00	00	00	58	...e...!X															
2120h:	08	68	00	00	00	00	00	16	02	1A	00	00	00	00	00	80	85	.h.....e...															
2130h:	80	06	00	00	00	00	60	21	A0	01	00	00	00	00	58	08		e...!X.															
2140h:	68	00	00	00	00	00	16	02	1A	00	00	00	00	00	80	85	80	h.....e...e															
2150h:	06	00	00	00	00	60	11	F8	03	9E	8F	6F	58	8E	8F	00	ø.ž.oxž..															
2160h:	00	00	00	49	45	4E	44	AE	42	60	82							...IEND0B...															

 微信号: lemon-sec

Gif 文件结尾为 3B。



0x01 文件分离

介绍了文件类型的识别方法了，接下来来讲一下文件分离

文件分离的原因：

在 CTF 这个充满脑洞的比赛中，出题人往往会以一些稀奇古怪的出题方式出题，因此你可以常常看见暴打出题人等字眼出现在比赛论坛中。在 CTF 中一个文件中隐藏着另外其他文件的题目是经常有的。这就需要掌握文件分离的技巧来应对。下面介绍几种姿势

1.、Binwalk

1.1 Binwalk 工具介绍

Binwalk 是一个自动提取文件系统，该工具可以自动完成指定文件的扫描，智能发掘潜藏在文件中所有可疑的文件类型及文件系统。相比于之前介绍的 file 命令行工具来说，file 只能把一个文件识别成一个类型的文件，很难看出是否隐藏着其他的文件，Binwalk 就能很好的完成这项任务。

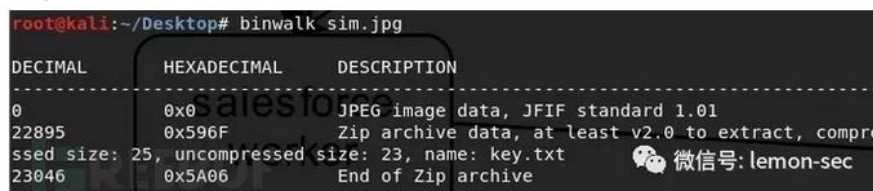
1.2 Binwalk 文件扫描和提取

Linux 安装 Binwalk

参考链接：<https://blog.csdn.net/u011297466/article/details/81264340>

Binwalk 分析文件

命令：binwalk +file 通过扫描能够发现目标文件中包含的所有可识别的文件类型。



通过 Binwalk 我们可以看到这一张 jpg 文件中藏着 zip 文件。

Binwalk 提取文件。

命令 binwalk +file -e。

```
root@kali:~/Desktop# binwalk sim.jpg -e
DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0            0x0           JPEG image data, JFIF standard 1.01
22895       0x596F        Zip archive data, at least v2.0 to extract, compressed size: 25, uncompressed size: 23, name: key.txt
23046       0x5A06        End of Zip archive
```

“-e” 和 “-extract” 用于按照定义的配置文件中的提取方法从固件中提取探测到的文件系统。

若提取成功则会生成一个_文件名_extracted 的目录，目录中存放的就是提取出的文件

2、foremost

2.1 foremost 工具介绍

foremost 该工具通过分析不同类型文件的头、尾和内部数据结构，同镜像文件的数据进行对比，以还原文件。它默认支持 19 种类型文件的恢复。用户还可以通过配置文件扩展支持其他文件类型。

2.2 foremost 提取文件

有时候 binwalk 无法正确分离出文件，这时候就可以使用 foremost，将目标文件复制到 kali 中，在终端中使用命令行进入文件所在文件夹，使用如下命令：

Foremost+file -o 输出目录名。

```
root@kali:~/ctf# foremost oddpic.jpg -o oddpic
Processing: oddpic.jpg
[*]
```

执行成功后会在目标文件的文件目录下生成我们设置的目录，目录中有按照文件类型分离出文件。



Kali 安装 foremost

参考链接：https://blog.csdn.net/qq_30445397/article/details/105787417

```
root@kali:~# apt-get install foremost
正在读取软件包列表 ... 完成
正在分析软件包的依赖关系树
正在读取状态信息 ... 完成
下列软件包是自动安装的并且现在不需要了:
cython hashcat-data lib32gcc1 lib32stdc++6 libasan5 libc-dev-bin libc6-i386 libcc1-0 libclang1-8 libffi-dev
libgcc12 libgcc-9-dev libgfortran0 libgfrpc0 libgfxdr0 libglusterfs0 libitm1 libllvm8 liblsan0 libobjc-9-dev libobjc4
libomp-8-dev libomp5-8 libpfm4 libpocl2-common libtidy5deb1 libtsan0 libubsan1 linux-headers-5.3.0-kali2-common
linux-kbuild-5.3 linux-libc-dev llvm-8 llvm-8-runtime manpages-dev python-alembic python-attr python-autobahn
python-automat python-backports-abc python-bottle python-cbor python-chameleon python-concurrent.futures
python-constantin python-cssselect python-deprecation python-editor python-feedparser python-filedepot
python-flask-classful python-flask-kvsession python-flask-login python-flask-mail python-flask-principal
python-flask-restless python-flask-session python-flask-sqlalchemy python-flaskext.wtf python-formencode
python-html2text python-hupper python-hyperlink python-incremental python-ipy python-libxml2 python-lz4
python-mashmallow python-mashmallow-sqlalchemy python-mimeparse python-mimerender python-nplune python-openid
python-packaging python-passlib python-paste python-pcapfile python-plaster python-png python-pyasnl-modules
python-pydot python-pyparsing python-pyqrcode python-pyquery python-repoze.lru python-scgi python-selenium
python-service-identity python-simplekv python-singledispatch python-snappy python-speaklater
python-sqlalchemy-schemadisplay python-sqlparse python-syslog-rfc5424-formatter python-tempita python-tornado
python-tqdm python-translationstring python-trie python-trollius python-twisted python-twisted-bin
python-twisted-core python-txaio python-typing python-tz python-u-msgpack python-ubjson python-unidecode
python-utidylib python-venusian python-waitress python-webob python-websocket python-wsaccel python-wtforms
python-zope.component python-zope.deprecation python-zope.event python-zope.hookable python-zope.interface
使用 'apt autoremove' 来卸载它(它们)。
下列【新】软件包将被安装:
foremost
升级了 0 个软件包，新安装了 1 个软件包，要卸载 0 个软件包，有 1174 个软件包未被升级。
需要下载 42.1 kB 的归档。
解压后会消耗 103 kB 的额外空间。
获取:1 http://mirrors.aliyun.com/kali kali-rolling/main amd64 foremost amd64 1.5.7-9+b1 [42.1 kB]
已下载 42.1 kB，耗时 0 秒 (192 kB/s)
正在选中未选择的软件包 foremost。
```


3、dd

前面介绍的两种都是自动化分离工具，dd 这个工具是一种半自动化工具，有的时候自动化工具不能实现文件的分离，所以需要这个工具来进行分离。

使用 dd 命令分离文件格式：`dd if=源文件名 bs=1 skip=开始分离的字节数 of=目标文件名`

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。

以 IDF 实验室“抓到一只苍蝇”为例，需要将获得的文件去除前 364 个字节：

```
dd if=s1 bs=1 skip=364 of=d1
```

使用 dd 命令分离文件格式：`dd if=源文件名 bs=1 skip=开始分离的字节数 of=目标文件名`

参数说明：

`if=file` #输入文件名，缺省为标准输入。

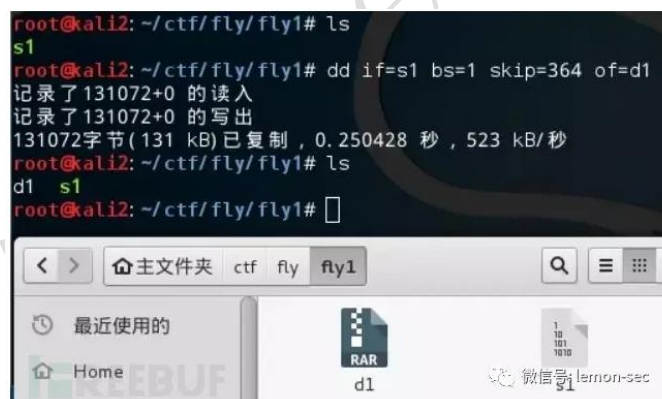
`of=file` #输出文件名，缺省为标准输出。

`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。

若需要将获得的文件去除前 364 个字节：

```
dd if=s1 bs=1 skip=364 of=d1
```



4、fcrackzip

简介

Fcrackzip 是一款专门破解 zip 类型压缩文件密码的工具，工具小巧方便、破解速度快，能使用字典和指定字符集破解，适用于 linux、mac osx 系统。

FCrackZip 是 Free/Fast Zip Crack(免费，快速 Zip 密码破解) 的意思。

Kali 安装 `apt-get install fcrackzip`

```

cython hashcat-data lib32gcc1 lib32stdc++6 libasan5 libc-dev-bin libc6-i386 libc6-i386 liblang1-8 libffi-dev
libgcc1-2 libgcc-9-dev libgfortran0 libgfortran5 libglusterfs0 libitm1 libllvm8 liblsan0 libobjc-9-dev libobjc4
libomp-8-dev libomp5-8 libpfm4 libpocl2-common libtidy5deb1 libtsan0 libubsan1 linux-headers-5.3.0-kali2-common
linux-kbuild-5.3 linux-libc-dev llvm-8 llvm-8-runtime manpages-dev python-alembic python-attr python-autobahn
python-automat python-backports-abc python-bottle python-chor python-chameleon python-concurrent.futures
python-constantin python-cssselect python-deprecation python-editor python-feedparser python-filedepot
python-flask-classful python-flask-kvsession python-flask-login python-flask-mail python-flask-principal
python-flask-restless python-flask-session python-flask-sqlalchemy python-flaskext.wtf python-formencode
python-html2text python-hupper python-hyperlink python-incremental python-ipy python-libxml2 python-lz4
python-marshmallow python-marshmallow-sqlalchemy python-mimeparse python-mimerender python-nplussone python-openid
python-packaging python-passlib python-paste python-pcapfile python-plaster python-png python-pyasn1-modules
python-pydot python-pyparsing python-pyqrcode python-pyquery python-repoze.lru python-scgi python-selenium
python-service-identity python-simplekv python-singledispatch python-snappy python-speaklater
python-sqlalchemy-schemadisplay python-sqlparse python-syslog-rfc5424-formatter python-tempita python-tornado
python-tqdm python-translationstring python-trie python-trollius python-twisted python-twisted-bin
python-twisted-core python-txaio python-typing python-tz python-u-msgpack python-ubjson python-unidecode
python-utidylib python-venusian python-waitress python-webob python-websocket python-wsaccel python-wtforms
python-zope.component python-zope.deprecation python-zope.event python-zope.hookable python-zope.interface
使用 'apt autoremove' 来卸载它(它们)。
下列【新】软件包将被安装：
  fcrackzip
升级了 0 个软件包，新安装了 1 个软件包，要卸载 0 个软件包，有 1174 个软件包未被升级。
需要下载 28.8 kB 的归档。
解压后会消耗 81.9 kB 的额外空间。
获取 11 http://mirrors.aliyun.com/kali-rolling/main amd64 fcrackzip amd64 1.0-10 [28.8 kB]
已下载 28.8 kB，耗时 0秒 (166 kB/s)
正在选中未选择的软件包 fcrackzip。
(正在读取数据库 ... 系统当前共安装有 275064 个文件和目录。)
准备解压 .../fcrackzip 1.0-10_amd64.deb ...
正在解压 fcrackzip (1.0-10) ...
正在设置 fcrackzip (1.0-10) ...
正在处理用于 man-db (2.9.0-1) 的触发器

```

5、010Editor

在之前文件识别中提到这个工具，手动分离文件也可以使用这个工具
拖动想要分离的部分。





右键->选择->保存选择。

然后根据需要分离的文件类型选择后缀名。



练习部分：

通常做图片隐写的题，大概都是先右键查看属性，看下有没有一些特殊的信息，用 UE 随便看了下文件头和文件尾，没有发现字符串，没有就放 binwalk 看下有没有隐藏什么文件，又或者直接 stegsolve 分析一波。

杂项第六题：啊哒、

杂项第七题：又一张图片，还单纯吗、

杂项第十题：隐写 2、

0x02 文件合并

在介绍了文件分离后，还需要提到的是文件合并。

既然 CTF 有文件分离的题目，那自然也少不了文件合成的了，但是文件合成还是有技巧的。

1. linux 环境文件合并

cat 是 linux 系统下的一个能提取文件的内容的命令，使用 cat 命令将文件内容提取出来再导入目标文件。使用方式如下：

将 chapter01、chapter02、chapter03 三个文件按从左到右顺序合并，输出到 book 文件中。

所使用的命令：`cat chapter01 chapter02 chapter03 > book`

将所有以 chapter 开头的文件按文件名从小到大的顺序合并，输出到 book 文件中。

所使用的命令：`cat chapter* > book`

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

但是要注意的一点是，cat 是需要遵循顺序来获取文件内容的，所以在 cat 之前需要判断一下文件的先后顺序。

2. windows 环境文件合并

linux 中有 cat 等命令，windows 环境下也有类似的命令 copy，使用方式如下：

将 chapter01、chapter02、chapter03 三个文件按从左到右顺序合并，输出到 book 文件中。

所使用的命令：`copy /B chapter01+chapter02+chapter03 book`

将所有以 chapter 开头的文件按文件名从小到大的顺序合并，输出到 book1 文件中。

所使用的命令：`copy /B chapter* book1`

```
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。

微信号: lemon-sec
```

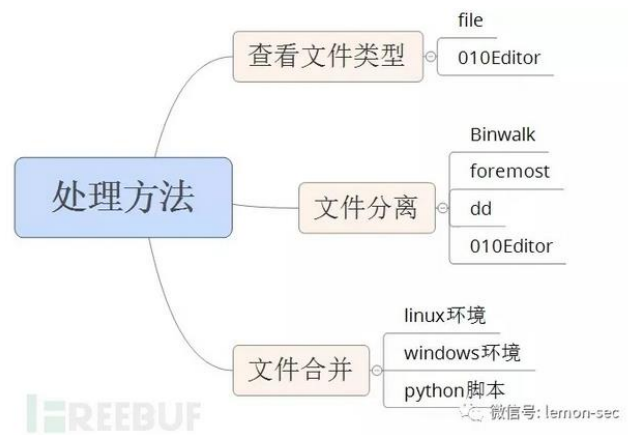
3. Python 文件合并

python 环境适用于 linux 也适用于 windows，它是通过编写脚本来实现的文件合并，以之前的例子来。

```
# -*- coding: utf8 -*-
def foo():
    path=r".\chapter%d"
    s=""
    for i in xrange(1,4):
        f=open(path % i).read()
        s+=f
    print s
    pass
if __name__ == '__main__':
    foo()
    print 'ok'
```

0x03 总结

介绍了这么多关于 CTF 基础类型的文件处理方法，为了方便大家梳理，提供一个思维导图给大家来参考。



用来处理文件的方法和工具不仅仅只有这些，这就需要靠大家自己发现和探索。

转载自: <https://www.freebuf.com/column/196815.html>