

攻防世界 Misc Dtf

原创

==Microsoft== 于 2022-03-05 12:41:50 发布 2344 收藏

分类专栏: [Misc](#) 文章标签: [安全](#) [密码学](#) [ctf](#) [misc](#)

和你一起终身学习, 这里是程序员Android

本文链接: <https://blog.csdn.net/MrTreebook/article/details/123292179>

版权



[Misc 专栏收录该内容](#)

50 篇文章 0 订阅

订阅专栏

攻防世界 Misc Dtf

- 1.winhex分析
- 2.binwalk分析
- 3.foremost分离
- 4.修改图片Dtf.png的高度
- 5.wireshark打开
- 6.exp

1.winhex分析

The screenshot shows the WinHex application window with the file 'Dtf.png' open. The interface is split into three main panes: Hex view, ASCII view, and UTF-8 view. The Hex view shows the raw bytes of the file, starting with the PNG signature '89 50 4E 47 0D 0A 1A 0A'. The ASCII view shows the corresponding text, including 'PNG IHDR', 'z L 8 Z', and '4 pHYs'. The UTF-8 view shows the text in a more readable format, including 'L:com.adobe.xmp', 'Core 5.6-c142 7', and 'xmp:CreateDate=2022/03/05 11:27:40'. The status bar at the bottom indicates the current position in the file: '页 1 / 8,552' and '偏移地址: 0'.

- 看到了html代码，怀疑是一个网页

2.binwalk分析

```
(msc@kali) - [~/Desktop/git/ctf-misc]
$ binwalk Dtf.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 926 x 1100, 8-bit/color RGB, non-interlaced
1822	0x71E	Zlib compressed data, default compression
989714	0xF1A12	RAR archive data, version 4.x, first volume type: MAIN_HEAD

CSDN @==Microsoft==

- 发现有一个rar文件

3.foremost分离

```
(root@kali) - [~/home/.../git/ctf-misc/output/png]
# foremost -i Dtf.png
```

- 打开rar文件发现需要密码
-

4.修改图片Dtf.png的高度

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII	UTF-8
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG	IHDR	□ □ □ □ IHDR
00000010	00	00	03	9E	00	00	05	4C	08	02	00	00	00	38	16	5A	ž	L 8 Z	□ □ □ □ L □ □ □ □ 8 □ Z
00000020	34	00	00	00	09	70	48	59	73	00	00	0B	13	00	00	0B	4	pHYs	4 □ □ □ pHYs □ □ □ □ □ □
00000030	13	01	00	9A	9C	18	00	00	06	D4	69	54	58	74	58	4D	šæ	ôiTtXM	□ □ □ □ □ □ □ □ tXM
00000040	4C	3A	63	6F	6D	2E	61	64	6F	62	65	2E	78	6D	70	00	L:com.adobe.xmp	L:com.adobe.xmp□	
00000050	00	00	00	00	3C	3F	78	70	61	63	6B	65	74	20	62	65	<?xpacket be	□ □ □ □ <?xpacket be	
00000060	67	69	6E	3D	22	EF	BB	BF	22	20	69	64	3D	22	57	35	gin="i>?" id="W5	gin=" " id="W5	
00000070	4D	30	4D	70	43	65	68	69	48	7A	72	65	53	7A	4E	54	M0MpCehiHzreSzNT	M0MpCehiHzreSzNT	
00000080	63	7A	6B	63	39	64	22	3F	3E	20	3C	78	3A	78	6D	70	czkc9d"?> <x:xmp	czkc9d"?> <x:xmp	
00000090	6D	65	74	61	20	78	6D	6C	6E	73	3A	78	3D	22	61	64	meta xmlns:x="ad	meta xmlns:x="ad	
000000A0	6F	62	65	3A	6E	73	3A	6D	65	74	61	2F	22	20	78	3A	obe:ns:meta/" x:	obe:ns:meta/" x:	

- 修改成05即可
- 再次打开图片可以看到密码



StRe1izia

CSDN @==Microsoft==

- 输入密码得到一个流量包文件

5.wireshark打开

- 搜索有关png的内容

No.	Time	Source	Destination	Protocol	Length	Info
6971	20.304633	192.168.31.59	123.206.131.120	TCP	54	33307 → 80
6972	20.304869	123.206.131.120	192.168.31.59	TCP	66	80 → 33306
6973	20.304916	192.168.31.59	123.206.131.120	TCP	54	33306 → 80
6974	20.305051	192.168.31.59	123.206.131.120	HTTP	432	GET / HTTP/1.1
6975	20.305749	112.10.47.131	192.168.31.59	UDP	75	41733 → 248
6976	20.313675	192.168.31.59	111.147.144.142	UDP	1107	24889 → 406
6977	20.313790	192.168.31.59	112.10.47.131	UDP	1107	24889 → 417
6978	20.317912	123.206.131.120	192.168.31.59	TCP	54	80 → 33307
6979	20.318474	123.206.131.120	192.168.31.59	HTTP	567	HTTP/1.1 200

```
</head>\n
<body>\n
  \n
  ZmxhZ3tPel180bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9\n
</body>\n
</html>\n
\n
```

0000	3c 68 74 6d 6c 3e 0a 20	20 3c 68 65 61 64 3e 0a	<html>· <head>·
0010	20 20 20 20 3c 6d 65 74	61 20 68 74 74 70 2d 65	<meta http-e
0020	71 75 69 76 3d 22 43 6f	6e 74 65 6e 74 2d 54 79	quiv="Co ntent-Ty
0030	70 65 22 20 63 6f 6e 74	65 6e 74 3d 22 74 65 78	pe" cont ent="tex
0040	74 2f 68 74 6d 6c 3b 20	63 68 61 72 73 65 74 3d	t/html; charset=
0050	55 54 46 2d 38 22 20 2f	3e 0a 20 20 3c 2f 68 65	UTF-8" / >· </he
0060	61 64 3e 0a 20 20 3c 62	6f 64 79 3e 0a 20 20 09	ad>· <b ody>·
0070	3c 69 6d 67 20 73 72 63	3d 22 2f 6b 69 73 73 2e	<img src ="/kiss.
0080	70 6e 67 22 20 2f 3e 0a	20 20 5a 6d 78 68 5a 33	png" />· ZmxhZ3
0090	74 50 65 6c 38 30 62 6d	52 66 53 47 6c 79 4d 46	tPel180bm RfSGlyMF
00a0	39 73 62 33 59 7a 58 30	5a 76 63 6a 4e 32 5a 58	9sb3YzX0 ZvcjN2ZX
00b0	4a 39 0a 20 20 3c 2f 62	6f 64 79 3e 0a 3c 2f 68	J9· </b ody>·</h
00c0	74 6d 6c 3e 0a 0a		tml>··

CSDN @Captain0507

- 发现base64加密的内容
- 使用工具解密

Wireshark · 追踪 HTTP 流 (tcp.stream eq 75) · Dtf.pcapng

```
Content-Length: 177
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html;
charset=UTF-8" />
  </head>
  <body>
    
    ZmxhZ3tPel180bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9
  </body>
</html>

GET /kiss.png HTTP/1.1
Host: 123.206.131.120
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99
Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://123.206.131.120/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

2 客户端 分组, 1 服务器 分组, 2 turn(s).

整个对话 (1256 bytes) 显示和保存数据为 ASCII

查找: 查找下一个 (N)

滤掉此流 打印 Save as... 返回 Close Help

6.exp

```
import base64
basecode = "ZmxhZ3tPe180bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9"
result = base64.b64decode(basecode)
print(result)
```

- 得到flag

```
PS C:\Users\17849\Desktop> python exp.py
b'flag{0z_4nd_Hir0_lov3_For3ver}'
PS C:\Users\17849\Desktop>
```