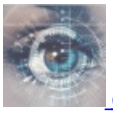
攻防世界 Ditf misc

原创

听门外雪花飞 于 2022-02-12 19:52:46 发布 525 收藏

分类专栏： ctf刷题纪 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_52268949/article/details/122901031

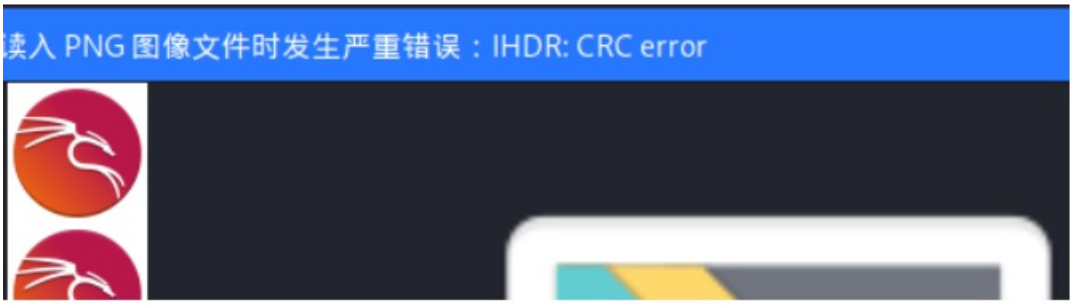


Ditf

附件下载下来就是一张图片，我们拉到hxd中发现应该有隐藏的压缩包

```
74 62 EE 77 A0 88 C2 E4 87 2C 13 F3 39 C2 F1 86   tbîw ˆÂä‡,.ó9Âñ†
C1 28 4D 80 3E 06 84 2B 41 B9 09 35 57 15 A3 4F   Á(M€>.„+A¹.5W.£O
9B 3A 68 5A B1 45 0C 72 36 E6 DE 72 50 4B BA 5D   ›:hZ±E.r6æÞrPKº]
85 83 3A 5F 73 7B 82 AB EA D6 23 2C 06 9F D1 09   …ƒ:_s{‚«êÖ#,.ŸÑ.
18 51 84 E5 DB E0 E2 F8 30 03 0C BC 18 59 F2 37   .Q„åÛàâø0..¼.Yò7
C0 15 23 C5 34 91 9A 20 74 40 8C BD D3 F2 5F 43   À.#Å4'š t@Œ½Óò_C
ED D9 99 F9 28 37 C1 EE EB ED 0A 72 83 F4 E8 32   íÙ™ù(7Áîëí.rƒôè2
90 67 E0 67 62 0F 2F 88 EB B4 4D D6 6C 56 49 B1   .gàgb./ˆë´MÖlVI±
C8 FE 67 DE 78 1C 00 58 22 23 2C 75 79 5F 94 0E   ÈþgÞx..X"#,uy_".
```


我们拉入到kali里面分析



意外发现图片高度被修改过我们先用binwalk分析图片看看

```
# binwalk e02c9de40be145dba6baa80ef1d270ba.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 926 x 1100, 8-bit/color RGB,
1822          0x71E           Zlib compressed data, default compressio
989714        0xF1A12         RAR archive data, version 4.x, first vol
AD
```


我们先尝试分离一下分离出一个压缩包但是需要密码想到高度有问题我们用hxd修改一下

```
┌──(root💀kali)-[~]
└─# foremost e02c9de40be145dba6baa80ef1d270ba.png
Processing: e02c9de40be145dba6baa80ef1d270ba.png
|*|
```

```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  %PNG........
00 00 03 9E 00 00 05 4C 08 02 00 00 00 38 16 5A  ...ž...L.....
34 00 00 00 09 70 48 59 73 00 00 0B 13 00 00 0B  4....pHYs....
```

得出密码解压出一个流量包

StRe1izia

Hypertext Transfer Protocol	1.4	163	2.5	136619	37 k	151	43180	11 k
MIME Multipart Media Encapsulation	0.0	1	0.0	264	71	1	522	141
Media Type	0.0	3	1.4	75040	20 k	3	76501	20 k
Line-based text data	0.0	4	0.1	5202	1412	4	5534	1502
JavaScript Object Notation	0.0	1	0.1	5981	1623	1	6612	1795
HTML Form URL Encoded	0.0	1	0.0	652	177	1	652	177

发现一些http流量我们过滤一下

6979	20.318474	123.206.131.120	192.168.31.59	HTTP	567 HTTP/1.1 200 OK (text/html)
6983	20.324928	192.168.31.59	123.206.131.120	HTTP	398 GET /kiss.png HTTP/1.1
6993	20.338330	123.206.131.120	192.168.31.59	TCP	1458 80 → 33307 [ACK] Seq=514 Ack=723 Win=31360 Len=1404 [TC

在这里发现一个png文件的流量我们追踪一下http流

```
  <body>
        <img src="/kiss.png" />
  ZmxhZ3tPel80bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9
  </body>
</html>
```

这明显是一个base64加密我们去解密

```
>>> import base64
>>> base64.b64decode('ZmxhZ3tPel80bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9')
b'flag{Oz_4nd_Hir0_lov3_For3ver}'
>>>
```

得出flag