攻防世界 Misc高手进阶区 5分题 恶臭的数据包

原创

思源湖的鱼 于 2021-01-07 14:00:51 发布 607 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 misc

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112235777

前言

继续ctf的旅程

攻防世界Misc高手进阶区的5分题

本篇是恶臭的数据包的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

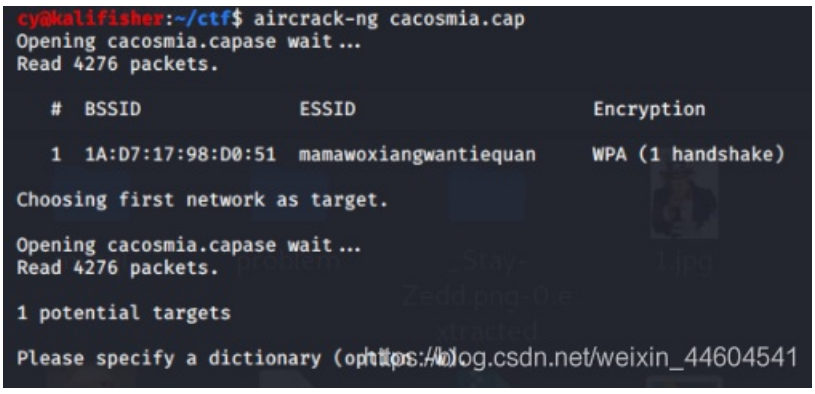
解题过程

得到一个数据包

什么都没看懂

因为题目描述是无线网

所以扔进aircrack-ng看看

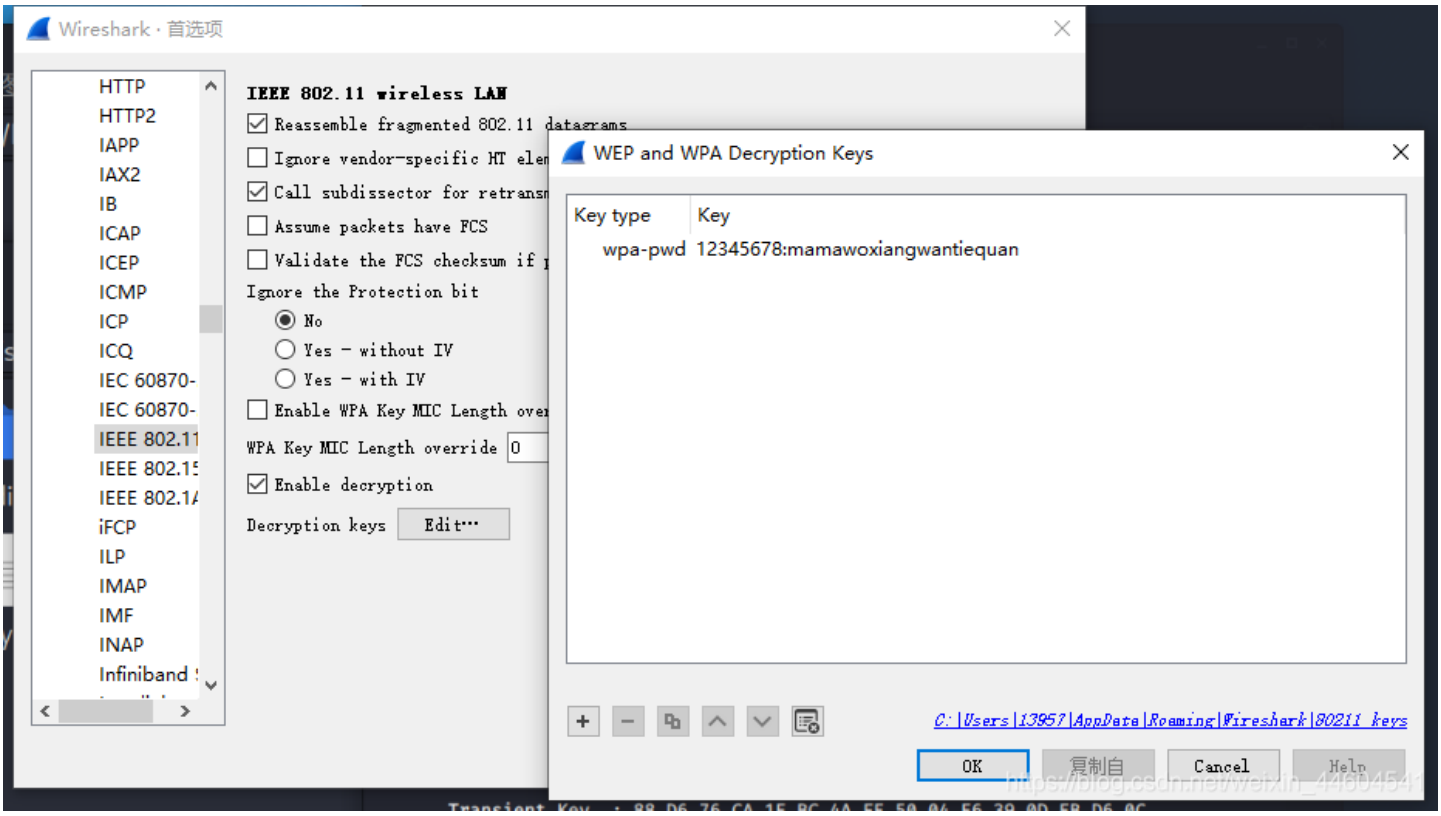


破解密码

```
aircrack-ng cacosmia.cap -w /usr/share/wordlists/rockyou.txt
```

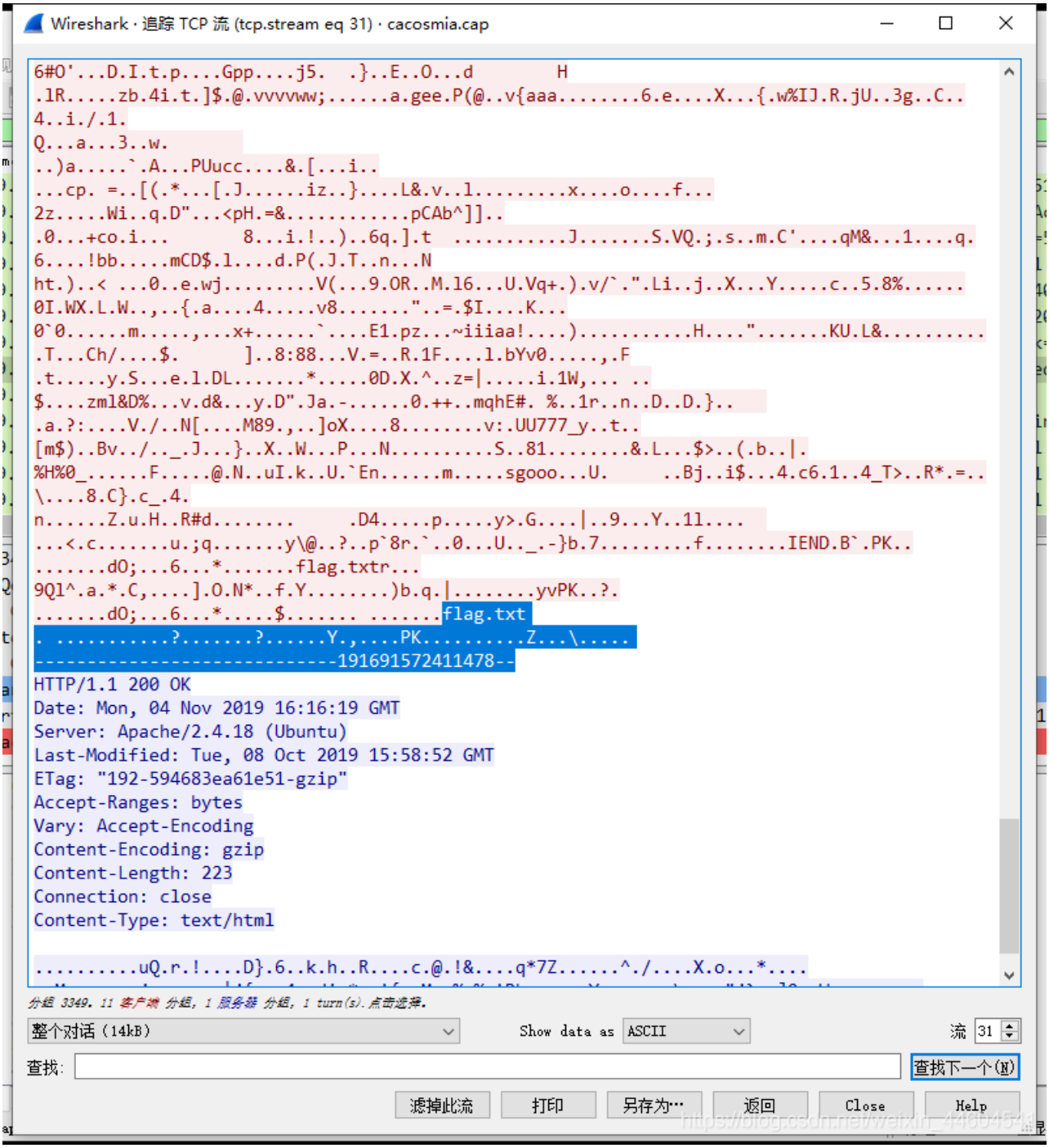
得到密码：`12345678`

那就可以破解了



出现了tcp流

翻找追踪到可疑流


Wireshark · 追踪 TCP 流 (tcp.stream eq 31) · cacosmia.cap
6#O'...D.I.t.p....Gpp....j5. .}..E..O...d H
.lR.....zb.4i.t.]$.@.vvvvww;......a.gee.P(@..v{aaa........6.e....X...{.w%IJ.R.jU..3g..C..
4..i./.1.
Q...a...3..w.
..)a.....`.A...PUucc....&.[...i..
...cp. =..[(.*...[.J......iz..}....L&.v..l.........x....o....f...
2z.....Wi..q.D"...<pH.=&............pCAb^]]..
.0...+co.i... 8...i.!..)..6q.].t ..........J.......S.VQ.;.s..m.C'....qM&...1....q.
6....!bb.....mCD$.l....d.P(.J.T..n...N
ht.)..< ...0..e.wj.........V(...9.OR..M.16...U.Vq+.).v/`.".Li..j..X...Y.....c..5.8%.....
0I.WX.L.W..,..{.a....4.....v8......"..=.$I....K...
0`0.....m.....,...x+......`....E1.pz...~iiiaa!....)..........H...."........KU.L&.........
.T...Ch/....$.]..8:88...V.=..R.1F....l.bYv0.....,.F
.t.....y.S...e.l.DL.......*.....0D.X.^..z=|.....i.1W,... ..
$....zml&D%...v.d&...y.D".Ja.-......0.++..mqhE#. %..1r..n..D..D.}..
.a.?:....V./..N[....M89.,..]oX....8........v:.UU777_y..t..
[m$)..Bv../..._.J...}..X..W...P...N..........S..81........&.L...$>..(.b..|.
%H%0_......F.....@.N..uI.k..U.`En......m.....sgooo...U. ..Bj..i$...4.c6.1..4_T>..R*.=..
\....8.C}.c_.4.
n......Z.u.H..R#d........ .D4.....p.....y>.G....|..9...Y..1l....
...<.c.......u.;q.......y\@..?..p`8r.`..0...U.._.-}b.7.........f........IEND.B`.PK..
.......dO;...6...*.......flag.txtr...
9Ql^.a.*.C,....].O.N*..f.Y........)b.q.|........yvPK..?.
.......dO;...6...*.....$....... ....flag.txt
. ...?.......?......Y.,....PK..........Z...\.....
----------------------------191691572411478--
HTTP/1.1 200 OK
Date: Mon, 04 Nov 2019 16:16:19 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Tue, 08 Oct 2019 15:58:52 GMT
ETag: "192-594683ea61e51-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 223
Connection: close
Content-Type: text/html
..........uQ.r.!....D}.6..k.h..R....c.@.!&....q*7Z......^./....X.o...*....
分组 3349. 11 客户端 分组, 1 服务器 分组, 1 turn(s). 点击选择.
整个对话 (14kB)
Show data as ASCII
流 31
查找:
查找下一个(N)
滤掉此流
打印
另存为…
返回
Close
Help

搞出来
处理下文件头

```
00000000  89 50 4E 47 0D 0A 1A 0A  00 00 00 0D 49 48 44 52  ‰PNG        IHDR
00000016  00 00 00 68 00 00 00 65  08 02 00 00 00 2E E0 31     h   e      .à1
00000032  28 00 00 00 09 70 48 59  73 00 00 0B 13 00 00 0B  (    pHYs
00000048  13 01 00 9A 9C 18 00 00  00 20 63 48 52 4D 00 00     šœ      cHRM
00000064  7A 25 00 00 80 83 00 00  F9 FF 00 00 80 E9 00 00  z%  €ƒ  ùÿ  €é
00000080  75 30 00 00 EA 60 00 00  3A 98 00 00 17 6F 92 5F  u0  ê`  :˜   o'_
00000096  C5 46 00 00 32 31 49 44  41 54 78 DA BC 7D 59 8F  ÅF  21IDATxÚ¼}Y
00000112  23 E7 95 65 EC 1B 23 48  06 77 26 C9 CC 64 EE 59  #ç•eì #H w&ÉÌdîY
00000128  AA 4D 52 D9 96 CB 76 DB  56 F7 C8 D6 08 8D 99 6E  ªMRÙ–ËvÛV÷ÈÖ  ™n
00000144  A8 E7 41 1E 0C 30 80 7F  40 FF 80 46 BF F7 5F 98  ¨çA  0€ @ÿ€F¿÷_˜
00000160  C1 00 D3 2F 3D 0F F6 A0  81 86 3C 5E 20 59 B6 6C  Á Ó/= ö  †<^ Y¶l
00000176  B7 24 AB 4A B5 6F 59 B9  91 C9 25 B9 AF 11 8C 3D  ·$«JµoY¹'É%¹¯ Œ=
00000192  E6 E1 94 3E B3 B3 2A 4B  56 75 95 E3 A1 90 99 C5  æá"›³³*KVu•ã¡ ™Å
00000208  25 78 BF BB 9E 7B EE 25  3D 1A 8D 18 86 61 59 96  %x¿»ž{î%=   †aY–
00000224  A2 28 DF F7 1D C7 B1 6D  DB 75 DD 7F F8 87 7F E8  ¢(ß÷ Ç±mÛuÝ ø‡ è
00000240  F7 FB 0C C3 BC FC F2 CB  6F BD F5 D6 F6 F6 36 45  ÷û Ã¼üòËo½õÖöö6E
00000256  51 A3 D1 C8 B6 ED 68 34  2A 49 92 EF FB E3 F1 D8  Q£ÑÈ¶íh4*I'ïûãñØ
00000272  75 5D 55 55 15 45 B1 2C  8B A6 69 96 65 69 9A A6  u]UU E±,‹¦i–eiš¦
00000288  28 2A 0C 43 DF F7 C3 30  0C 82 80 E7 79 D7 75 67  (* Cß÷Ã0 ‚€çy×ug
00000304  B3 99 A2 28 B2 2C 53 14  65 18 46 18 86 9E E7 F9  ³™¢(²,S e F †žçù
00000320  BE CF 30 0C CF F3 1C C7  D1 34 1D 86 21 EE E4 F1  ¾Ï0 Ïó ÇÑ4 †!îäñ
00000336  8B E7 79 BC 5A 10 04 14  45 D1 34 CD 30 0C 4D D3  ‹çy¼Z   EÑ4Í0 MÓ
00000352  A6 69 72 1C C7 71 1C F9  08 9E E7 79 9E 87 37 7A  ¦ir Çq ù žçyž‡7z
00000368  71 17 FB 77 7F F7 77 0C  C3 E0 97 30 0C C3 30 64  q ûw ÷w Ãà–0 Ã0d
00000384  18 86 E3 B8 E9 74 6A 59  56 BF DF A7 28 2A 99 4C  †ã¸étjYV¿ß§(*™L
00000400  EA BA 1E 04 C1 78 3C B6  6D 9B A6 69 7C 4E DC 3D  ê°  Áx<¶m›¦i|NÜ=
```

得到一张图片

binwalk处理

```
cy@kalifisher:~/ctf$ binwalk -e ca.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 104 x 101, 8-bit/color RGB, non-interlaced
106           0x6A            Zlib compressed data, best compression
```

得到压缩包

解压要密码
爆破失败

回数据包里找密码

发现session是个jwt

```
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJoaW50IjoiZm9yIHNlY3VyaXR5LCBJIHNldCBteSBwYXNzd29yZCBhcyBhIHdlYnNpdGUgd2hpY2ggaSBqdXN0IHBpbmdlZCBiZWZvcmUifQ.P3xOErNrUkYqdMBoo8WvU63kUVyOkZjiTK-hwOIIS5A
```

解码

那回去找DNS和ICMP

试了试
最后是`26rsfb.dnslog.cn`

得到flag

结语

知识点

- aircrack-ng破解无线密码
- 图片隐写
- JWT
- DNS