MISC

- Tools
  看压缩包得解密的工具。
  第一个压缩包名字为f5，可知是f5解密工具，查看图片属性可知密码，在ubuntu中下载完后输入指令 java Extract /mnt/hgfs/1.jpg -p !LyJJ9bi&M7E72*JyD得到压缩包的密码e@317S*p1A4bIYIs1M。
  第二个同理为steghide隐写在终端输入steghide extract -sf 01.jpg，在图片中找到密码输入后，在pwd.txt中得到下一个压缩包的密码u0!FO4JUhl5!L55%$&。
  第三个为outguess,在终端输入指令outguess -k 'z0GFieYAee%gdf0%lF' -r 02.jpg 1.txt
  得到密码@UjXL93044V5zl2ZKI。
  第四个为JPHS，在通过jphs得密码，然后将四张二维码连起来

  

  扫码得flag。

- Telegraph：1601 6639 3459 3134 0892
  将音频用audacity打开，转为频谱图，放大之后发现一串摩斯电码，翻译可得flag
  flag:hgame{4G00DS0NGBUTN0T4G00DMAN039310KI}

- Hallucigenia
  用stegsolve打开png，做一下调整后得到一个二维码。扫码得一串base64的码，但是不能在线转换。于是想到可能是一个一个文件。所以用脚本
  ' ' '

  input_file = open('1.txt', 'r')
  coded_string = input_file.read()
  decoded = base64.b64decode(coded_string)
  output_file = open('2', 'wb')
  output_file.write(decoded)
  output_file.close()

'''

将得到的文件winhex打开，又根据题目发现，它的16进制倒过来刚好是一个png形式的文件。然后就是把它的16进制逆过来就行了。上脚本

'''

a = ''

b=''

for i in range (len(a)//2,0,-1):

b+=a[2*i-2:2*i]

print(b)

'''

打开得到的png图片，可以辨认出flag。

flag:hgame{tenchi_souzou_dezain_bu}

- DNS
  打开数据包搜索http，发现和spf有关，搜索相关知识后，在终端进行一下操作，得到flag。

Crypto

- signin
  根据费马小定理，c=a^p*m%p可转换为*c=a*m%p,同时a*x%p=1(其中x为a的逆元)。根据两个式子可得脚本。
  '''

  import gmpy2

  import binascii

  a=16694044599779464626222598504419952126867000670029615539371945275226690600956286102351911443126744410472983459039173356055490358

18659775535728005539682663479602861235646104858869117275056385670652736325607369042413697702697744445375139102315777136081359067059463745445192227029129241733776672534906646147217

p=14157797815423025572520319264830185883563620235852932667480451471763490254277290197893360444721725174965165591232428440978889424108367581247722349904065948542338485748014455710250367930424315890433545838549078999343934673916947658406830185367781451292998881473176673456095372117259397368534638362104253922303

c=83100993208825805960288462822052002658654448425456067588785103016568243225935690211166949234700168269098577663978173476061572322864989530345549875688993822279419840455276876060268315756701711226608664564386549424754678794166485166800336410018160050867859193743800326163348757941655096459154690288871791392

x = gmpy2.invert(a,p)

*m = x*c%p

m_hex = hex(m)[2:]

print("ascii:\n%s"%(binascii.a2b_hex(m_hex).decode("utf8"),))

' ' '

flag:hgame{M0du1@r_m4th+1s^th3~ba5is-Of=cRypt0!!}

- gcd or more?
  根据rsa算法，百度得e=2时为特殊情况。上脚本
  ' ' '

  import gmpy2

  import libnum

e=2

p = 852285650211289018533149345831290834419890452250225412985505704493898396609019

q = 111614714641364911312915294479850549131835378046002423977989457843071188836271

cipher = 766500368283066645619389449101598964164785482664717787314198410720209908147598482780600728783047289961681808090727660674446745344590892305497539362350953 9

N=p*q

计算yp和yq

yp = gmpy2.invert(p,q)

yq = gmpy2.invert(q,p)

计算mp和mq

mp = pow(cipher, (p + 1) // 4, p)

mq = pow(cipher, (q + 1) // 4, q)

计算a,b,c,d

a = (yp * p * mq + yq * q * mp) % N

b = N - int(a)

c = (yp * p * mq - yq * q * mp) % N

d = N - int(c)

for i in (a,b,c,d):

s = '%x' % i

if len(s) % 2 != 0:

s = '0' + s

print (libnum.n2s(int(s,16)))

' ' '

flag:hgame{3xgCd~i5_re4l1y+e@sy^r1ght?}

- WhitegiveRSA
  上网了解rsa后，上脚本。
  ' ' '
  p = gmpy2.mpz(857504083339712752489993810777)
  q = gmpy2.mpz(1029224947942998075080348647219)
  e = gmpy2.mpz(65537)
  n = p*q*
  phi_n = (p-1)(q-1)
  d = gmpy2.invert(e, phi_n)
  c =

```
    gmpy2.mpz(747831491353896780365654517748216624798517769637260742155527)
m = pow(c, d, n)
m_hex = hex(m)[2:]
print("ascii:\n%s"%(binascii.a2b_hex(m_hex).decode("utf8"),))
'''
```

flag:hgame{w0w~yOU_kNoW+R5@!}

Web

- Liki的生日礼物
  根据hint得知是条件竞争。百度相关知识。将网页打开，将兑换数量设置为1点击兑换，然后bp抓包。将抓到的包send to intruder。将包改为500，线程改为100，进行攻击。刷新页面可得兑换券超过52张，得到flag。
  flag:hgame{L0ck_1s_TH3_S0lllut!on!!!}