BugKu CTF(杂项篇MISC)---黑客的照片

原创

肖萧然 已于 2022-03-16 12:49:47 修改 1205 收藏 3

分类专栏： MyCTF # MISC 文章标签： 安全 rsa 杂项 crypto

于 2022-03-13 22:25:08 首次发布

BugKu CTF(杂项篇MISC)—黑客的照片

文章目录

题目

提取文件

```
foremost hacker.png
```

```
┌──(root💀192)-[/mnt/hgfs/mykali]
└─# foremost hacker.png
Processing: hacker.png
}•••r□□•E•p•H_is_passwd.txt□•I••Q□••
              ••••
••□w••□□•A•4••]•w]+<•eV••"-%Zk¸e}•L•F,K••R'4••
                  ••••••iwG••E•• %•3an•Z•••□•••••••tf7Xs•c,••&I□0A•
A••••Œ(•
foundat=flag3.png□•
*|

┌──(root💀192)-[/mnt/hgfs/mykali]
└─# tree output
output
├── audit.txt
├── png
│   └── 00000000.png
└── zip
    ├── 00000436.zip
    └── 00000438.zip
```


00000436 rsa 解密

rsa详解 --> rsa详解

```
e = 65537
p = 164350308907712452504716893470938822086802561377251841485619431897833167640001783092159677313093192408910634
151587217774530424780799210606788423235161145718338446278412594875577030585348241677399115351594884341730030967 7
759048265773797103708215105964379210271557677800966524378264921447755412212097016572789 49
q = 107494571486621948612091613779149137205875732174969005765729543731117585892506950289230919634697561179755186
311617524660328836580868616958686987611614233013077705519528946490721065002342868403557070176752015767206263130 3
915548209659318934852367274152303337361763513928822660053568975382862409461516167991803 09
c = 172105717681128595126067638716024320302580099226540889895663287273811908496845134751248133647780512006509440
851603873682051900941142484707955504664119408899233830142466986245247574311631338444519100498049853590216558935 6
408118513625001478438302006120227775820299556804581782213341874873733205658511549962103595818269756868790746977 5
302076271824469564025505064692884524991123703791933906950170434627603154363327534790335960055199999942362152676 2
400791342249110132728735617105227941636809383117204543251972795899186533863787430044640880715528606063023785950 2
490924209652484068178676906868066609303364002286204278658661 2
#longs_to_bytes(m) = passwd
```

p 和 q：两个大的质数，是另一个参数N的的两个因子。
N：大整数，可以称之为模数
e 和 d：互为无反数的两个指数
c 和 m：密文和明文

```
from Crypto.Util.number import *
import gmpy2

e = 65537
p = 164350308907712452504716893470938822086802561377251841485619431897833167640001783092159677313093192408910634
151587217774530424780799210606788423235161145718338446278412594875577030585348241677399115351594884341730030967 7
759048265773797103708215105964379210271557677800966524378264921447755412212097016572789 49
q = 107494571486621948612091613779149137205875732174969005765729543731117585892506950289230919634697561179755186
311617524660328836580868616958686987611614233013077705519528946490721065002342868403557070176752015767206263130 3
915548209659318934852367274152303337361763513928822660053568975382862409461516167991803 09
c = 172105717681128595126067638716024320302580099226540889895663287273811908496845134751248133647780512006509440
851603873682051900941142484707955504664119408899233830142466986245247574311631338444519100498049853590216558935 6
408118513625001478438302006120227775820299556804581782213341874873733205658511549962103595818269756868790746977 5
302076271824469564025505064692884524991123703791933906950170434627603154363327534790335960055199999942362152676 2
400791342249110132728735617105227941636809383117204543251972795899186533863787430044640880715528606063023785950 2
490924209652484068178676906868066609303364002286204278658661 2


n = p * q
phi = (p-1)*(q-1)  # 求φ(n)，φ(n)=(p-1)(q-1)
d = gmpy2.invert(e, phi)  # 求e对于模n的逆元，即解密指数d
m = pow(c, d, n)  # m=c^d mod n
passwd = long_to_bytes(m)  # m的字符串形式
print(passwd.decode())
```

```
I_1ove_mumuz1!
```

00000438 图片隐写

flag2 改高

flag3 stegpy

```
┌──(root💀192)-[/mnt/…/mykali/output/zip/00000438]
└─# stegpy  flag3.png
sc_d0n't_love_me}
```

flag1 zsteg

```
zsteg  hacker.png
```

```
┌──(root💀192)-[/mnt/hgfs/mykali]
└─# zsteg  hacker.png
[?] 922784 bytes of extra data after image end (IEND), offset = 0x368bc
extradata:0         ..
    00000000: 66 6c 61 67 7b 6d 31 73  50 4b 03 04 14 00 00 00  |flag{m1sPK......|
    00000010: 08 00 78 23 51 54 b1 33  ef 3c ae 02 00 00 0b 05  |..x#QT.3.<......|
    00000020: 00 00 12 00 00 00 74 68  69 73 5f 69 73 5f 70 61  |......this_is_pa|
    00000030: 73 73 77 64 2e 74 78 74  1d 94 49 8a 94 51 10 84  |sswd.txt..I..Q..|
    00000040: f7 0d 7d 07 c1 8d ee 72  1e 16 9e 45 9c 70 e3 48  |..}....r...E.p.H|
    00000050: 0b e2 ed fd b2 0a 8a 7f  ca 21 32 22 f2 7d 79 f5  |.........!2".}y.|
    00000060: ee 55 65 7a 3f 3f fd e2  56 2b 3c c5 65 56 ba d5  |.Uez??..V+<.eV..|
    00000070: 22 2d 25 5a 6b d6 a3 65  7d c6 4c a6 46 2c 4b bd  |"-%Zk..e}.L.F,K.|
    00000080: db 52 27 34 86 a7 0d d7  d9 1e 77 ad ae 10 11 e5  |.R'4......w.....|
    00000090: 41 d6 34 b7 ba 5d b9 77  5d 0b 8a ab 94 87 a6 e6  |A.4..].w].......|
    000000a0: b4 69 77 47 ba 84 45 8f  f4 92 20 25 d5 33 61 6e  |.iwG..E... %.3an|
    000000b0: 9e 5a aa 91 ad 14 9e 88  b2 a6 a1 e5 c6 74 66 37  |.Z...........tf7|
    000000c0: 58 73 d2 63 2c f4 ba ec  aa 26 49 17 30 41 93 76  |Xs.c,....&I.0A.v|
    000000d0: 21 e6 10 74 ae 10 57 64  79 6f ab 78 cb 80 4e 05  |!..t..Wdyo.x..N.|
    000000e0: 80 e1 7d 8d ad 95 aa 04  8f 90 53 69 bc 27 25 f8  |..}.......Si.'%.|
    000000f0: 16 41 85 a4 b7 a9 c9 b6  28 85 00 b3 b1 cf 4f bf  |.A......(.....O.|

```

flag 拼接

```
flag{m1s3_1s_eas3_bu1_misc_d0n't_love_me}
```

最后感谢大佬**树木有点绿** 的提示

相关软件github上都可找到,最好装在kali中,方便没爆错

用共享文件夹去映射文件 -> 我的设置