


HGAME WEEK4 WP

——EkkoSonya

MISC

Akira之瞳-1

下载下来压缩包里面是一个raw文件 查找资料知道是一个内存镜像文件(应该)

 important_work.raw

于是用内存取证工具volatility 获得系统的profile后列举里面的进程 找到一个特别的进程 important_work.exe

```
0xfffffa800f263b30 important_work 1092 2232 1 16 1 1 2021-02-18 09:47:15 UTC+0000
```

后尝试用其pid号将其导出得到bmp文件

用foremost分离后 得到一个可疑的压缩包  00002256.zip

发现里面有两张图片 且有密码 卡住了后 问了下Akira 害 又没有仔细看压缩包

接下来就是找登陆密码勒

```
..6...àze.8.i»P
assword is sha25
6(login password
)
```

emm 我记得我当时一直在试volatility的时候 有一个指令了解到运行important_work.exe的用户是 Genga03(但现在不知道是啥指令勒)

找到用户的密码哈希值

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Genga03:1001:aad3b435b51404eeaad3b435b51404ee:84b0d9c9f830238933e7131d60ac6436:::
```

查阅资料知晓后两者是对同一个密码的不同编码

密文: 84b0d9c9f830238933e7131d60ac6436

类型: NTLM ▼ [\[帮助\]](#)

查询

加密

查询结果:
asdqwe123

解码后再对其sha256编码 得到

20504cdfddaad0b590ca53c4861edd4f5f5cf9c348c38295bd2dbf0e91bca4c3 为其密码成功打开

之后面对两张一样的图片 但其所占大小不同 并且一张为Blind的提示 知道是盲水印 起初用python2破解 无用(不知为啥) 尝试用python3成功得到flag

```
python bwmforpy3.py decode src.png Blind.png flag.png
ark<flag.png>
```

CRYPTO

夺宝大冒险2

很神奇的一题

最开始认真看了python源码 大体了解这个函数的功能啥的 但是很迷茫 不知道从哪里下手

然后抱着查一查的心理 复制了下差不多这一段代码

```
def next(self):
    nextdata = (self.init << 1) & self.lengthmask """lengthmask = 1111111111.... nextdata = self.init<<1"""
    i = self.init & self.mask & self.lengthmask """lengthmask 确保位数长度至多为41位"""
    output = 0
```

到百度 结果就查到了类似的题型<https://www.anquanke.com/post/id/181811>

原来是LFSR的题目 抓紧了解一下 结合一开始分析的 基本知道了原理后 知道要先答错十个知道这40bit完全替换后的输出序列便可以得出最开始的40bit 于是先写了个python算最初序列

```
mask = '1011001010001010000100001000111011110101'
key = '0001010011001101000111001011000101010111'

tmp=key

R = ''
for i in range(40):
    output = key[:39]
    ans = int(tmp[-1-i])^int(output[-1])^int(output[-3])^int(output[-5])^int(output[-6])^int(output[-7])^int(output[-8])^int(output[-10])^int(output[-11])
    R += str(ans)
    key = str(ans) + key[:39]

print(R)
print(R[::-1])
print(int(R[::-1],2))
```

成功后把夺宝大冒险2的原码稍微改一下(由于不太会写与服务器交互的脚本 怕浪费时间 用人工获取flag的 蛮快的 pwntools在week1了解过.....会补的TAT) 先人工nc后获取十个数据 人工转换为二进制 再运行后 手动继续输入即可

```
self.mask = mask
self.lengthmask = 2*(length+1)-1

def next(self):
    nextdata = (self.init << 1) & self.lengthmask
    i = self.init & self.mask & self.lengthmask
    output = 0
    while i != 0:
        output ^= (i & 1)
        i = i >> 1
    nextdata ^= output
    self.init = nextdata
    return output

def random(self, nbit):
    output = 0
    for _ in range(nbit):
        output <= 1
        output |= self.next()
    return output

prng = LXFIQNN(0b10010111101110010110011111100110111101, 0b1011001010001010000100001000111011110101, 40)
while(1):
    print(prng.random(4))
```

得到flag

```
round 93 :: score 83
guess: 2
Right
round 94 :: score 84
guess: 7
Right
round 95 :: score 85
guess: 1
Right
round 96 :: score 86
guess: 11
Right
round 97 :: score 87
guess: 6
Right
round 98 :: score 88
guess: 5
Right
round 99 :: score 89
guess: 10
Right
hgame{lfsr_121a111y^use-in&crypto}
```

总结

四周的hgame结束勒 感觉学的有点糊 有点混乱 并没有达到最开始所设想的那样

对于re的学习还是很弱 后几周虽然都尝试并去做re的题目，但最终都是和flag擦肩而过，特别是像week2的hellore2和week3的FAKE(完完全全擦肩而过)

最终靠着做crypto和misc 划到了第四周

但还是想好好学习re的知识 之后慢慢复现下re的题目

确实在hgame中学到了很多知识 也是第一次在寒假尝试努力去学习很多新知识

(ノ◡•◡ノ)