小塔WEEK3汪汪叫的wp

crypto

Block Cipher

判断出是CBC模式的AES加密

解密过程通过密文分组进行xor运算再进行加密

在原加密代码上修改得：

```
import operator
from functools import reduce

def xor(a, b):
    assert len(a) == len(b)
    return bytes(map(operator.xor, a, b))

iv = b'Up\x14\x98r\x14%\xb9'
key = b'\r\xe8\xb86\x9c33^'
parts=...#省略数据
results = []
for i in range(0,4):
   if i == 0:
      results.append(reduce(xor, [parts[i], iv, key]))
   else:
      results.append(reduce(xor, [parts[i], parts[i-1], key]))


print(results)
```

运行后得到flag

Multi Prime RSA

多素数的RSA

用到取值为素数方幂的欧拉函数

$\varphi(p^{**}r)=p^{**}r-1*(p-1)$.

```
from libnum import n2s
import gmpy2
p =
617899321487194773840274583333805689780562861361378290929523173077119083534 77
q =
912079693533557636856332843788335063197947145070273329292907017487275341938 61
r =
105471299607375388622347272479207944509670502835651250945203397530010861809367
```

```
s =
831532387489037724481383075055797992771626521512444773914651305042671718814 37
n = ...#省略过长数据
e = 65537
c = ...#省略过长数据
list= [[p,2],[q,3],[r,5],[s,7]]
a=1
for i in range(0,4):
a = a * ((list[i][0]-1)*(list[i][0])**(list[i][1]-1) )
d = gmpy2.invert(e,a)
m=pow(c, d, n)
print (n2s(int(m)))
```

运行后得到flag

RSA Attack 3

本题的e很大，考虑采用低解密指数攻击

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

# 对e/n进行连分数展开
def continued(x, y):
    cF = []
    while y:
        cF += [x // y]
        x, y = y, x % y
    return cF

#得到渐进分数的分子分母
def Simplify(ctnf):
    numer = 0
    denomin = 1
    for x in ctnf[::-1]:
        numer, denomin = denomin, x * denomin + numer
    return (numer, denomin)

def calculate(x, y):
    cF = continued(x, y)
    cF = list(map(Simplify, (cF[0:i] for i in range(1, len(cF)))))
    return cF

# 韦达定理
def solve(a, b, c):
    par = gmpy2.isqrt(abs(b * b - 4 * a * c))
    return (-b + par) // (2 * a), (-b - par) // (2 * a)

def Attack(e, n):
    for (d, k) in calculate(e, n):
        if k == 0: continue
        if (e * d - 1) % k != 0: continue

        phi = (e * d - 1) // k
        p, q = solve(1, n - phi + 1, n)
```

```
        if p * q == n:
            return abs(int(p)), abs(int(q))
    print ('not find!')
n =...
e =...
c =...
#省略过长数据
p, q = Attack(e, n)
d = gmpy2.invert(e,(p-1)*(q-1))
m=pow(c,d,n)
string = long_to_bytes(m)
print(string)
```

运行完成得到flag

misc

卡中毒

附件是一个raw文件

查了一下觉得应该用内存取证的方法做【放进linux里】

```
volatility -f ACTUE.raw imageinfo
```

查看镜像系统，选其中一个，对其进行文件扫描

(因为文件很多，所以用txt为筛选条件试探一下)

```
volatility -f ACTUE.raw  --profile=Win7SP1x64 filescan | grep txt
```

发现确实有命名为flag的文件：

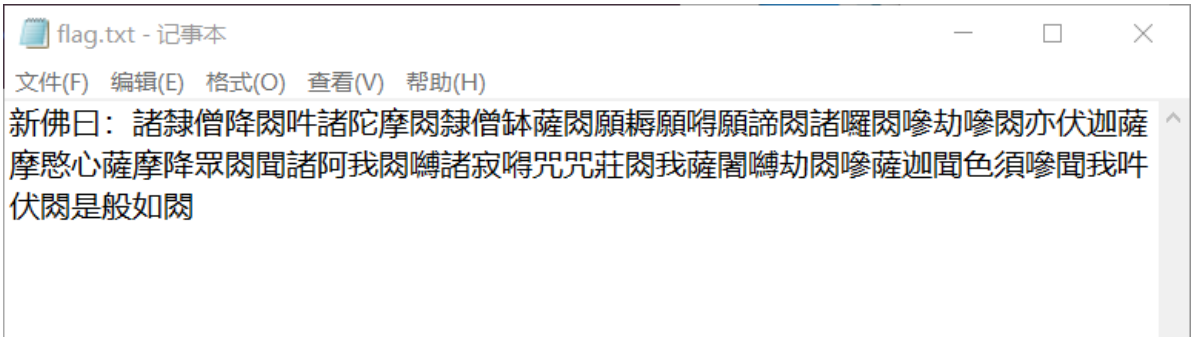
```
0x000000007eccc900      2      0 -W---- \Device\HarddiskVolume2\Users\Actue\Desk
top\flag.txt.txt.7z
0x000000007f3e8070      2      1 R--r-- \Device\HarddiskVolume2\Users\Actue\Desk
top\flag.txt.txt.7z
0x000000007f743720      1      0 R--r-- \Device\HarddiskVolume2\Users\Actue\Desk
top\flag.txt.txt.WannaRen
```

把文件提取出来，修改后缀名得到一个7z压缩包

里面是一个后缀为WannaRen的文件

搜索相关信息得知这是一个被病毒加密的文件

用火绒提供的WannaRen解密软件解密，拿到flag.txt



打开发现与佛论禅（而且看开头得知是“新与佛论禅”）

参悟佛所言的真谛得到flag