攻防世界 Crypto高手进阶区 5分题 说我作弊需要证据

原创

思源湖的鱼 于 2020-12-31 14:25:42 发布 210 收藏

分类专栏： ctf 文章标签： rsa base64 ctf 攻防世界 crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112007545

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的5分题

本篇是说我作弊需要证据的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

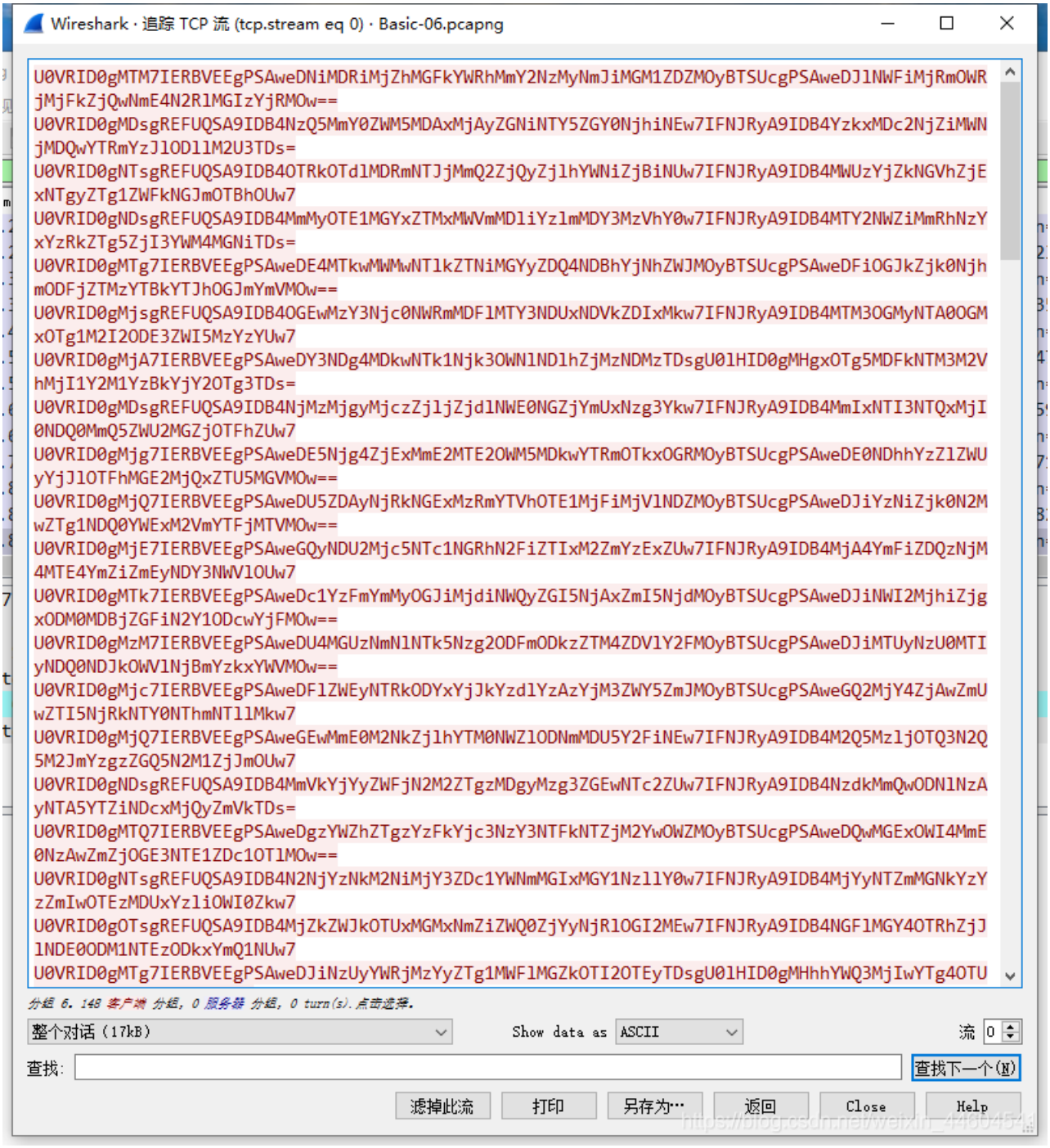
解题过程

描述

```
X老师怀疑一些调皮的学生在一次自动化计算机测试中作弊，他使用抓包工具捕获到了Alice和Bob的通信流量。狡猾的Alice和Bob同学好像使用某些加密方式隐藏通信内容，使得X老师无法破解它，也许你有办法帮助X老师。X老师知道Alice的RSA密钥为(n, e) = (0x53a121a11e36d7a84dde3f5d73cf, 0x10001) (192.168.0.13)?,Bob的RSA密钥为(n, e) =(0x99122e61dc7bede74711185598c7, 0x10001) (192.168.0.37)
```

得到一个流量包

追踪TCP



一堆base64

保存下来

先解密几个看看

前三个

```
SEQ = 13; DATA = 0x3b04b26a0adada2f67326bb0c5d6L; SIG = 0x2e5ab24f9dc21df406a87de0b3b4L;
SEQ = 0; DATA = 0x7492f4ec9001202dcb569df468b4L; SIG = 0xc9107666b1cc040a4fc2e89e3e7L;
SEQ = 5; DATA = 0x94d97e04f52c2d6f42f9aacbf0b5L; SIG = 0x1e3b6d4eaf11582e85ead4bf90a9L;
```

- DATA应该是密文
- SEQ是明文的顺序
- SIG是对明文的签名

因此对保存的TCP流依次解码
使用Bob的私钥对密文DATA解密
再验证SIG是否为Alice对明文的签名
如果是则放到明文列表的第SEQ位置

```
from Crypto.PublicKey import RSA
from gmpy2 import invert,powmod
from base64 import b64decode

def solve():
    N1=0x53a121a11e36d7a84dde3f5d73cfL
    N2=0x99122e61dc7bede74711185598c7L
    e=0x10001L
#   p1,q1=38456719616722997L,44106885765559411L
    p2,q2=49662237675630289L,62515288803124247L

#   phi1=(p1-1)*(q1-1)
    phi2=(p2-1)*(q2-1)
#   d1=invert(e,phi1)
    d2=invert(e,phi2)

#   rsa_key1=RSA.construct((N1,e,long(d1),p1,q1))
    rsa_key2=RSA.construct((N2,e,long(d2),p2,q2))

    with open('data.txt','r') as f:
        data=f.read()

    cips=data.split('\n')
    res=['']*len(cips)
    for cip in cips[:-1]:
        data=b64decode(cip)
        seq=int(data[(data.find('= ')+2):data.find(';')])
        cipher=data[(data.find('x')+1):data.find('L')]
        sig=data[(data.rfind('x')+1):data.rfind('L')]
        msg=rsa_key2.decrypt(long(cipher,16))
        if msg==powmod(long(sig,16),e,N1):
            res[seq]+=chr(msg)
    return res

if __name__=='__main__':
    print ''.join(solve())
```

得到flag：`flag{n0th1ng_t0_533_h3r3_m0v3_0n}`

结语

rsa为主