ctf-Ringzer0ctf

原创

逃课的小学生 于 2018-08-09 11:30:38 发布 2632 收藏
分类专栏： ctf crypto misc Ringzer0ctf 文章标签： ctf Ringzer0ctf crypto misc misc

Cryptography:

1.Some martian message

使用rot13对字符串解密，即可获得答案

2.File recovery

拿到一个压缩包，打开发现一个RSA密钥文件和一个加密后存放于flag.enc的密文，用openssl找出rsa密钥文件的私钥，对密文解密即可得到答案

```
def shuchu(mingwenstr):
    if mingwenstr[len(mingwenstr)-1]=='L':
        mingwenstr=mingwenstr[2:len(mingwenstr)-1]
    else:
        mingwenstr=mingwenstr[2:len(mingwenstr)]
    if not len(mingwenstr)%2==0:
            mingwenstr='0'+mingwenstr
    i=len(mingwenstr)
    mingwen=""
    while i>=1:
        str1=mingwenstr[i-2:i]
        if int(str1,16)>33 and int(str1,16)<126:
            mingwen=chr(int(str1,16))+mingwen
        else :
            mingwen=" "+mingwen
        i=i-2
    print mingwen
n=0xc50f1acbcff94169ba3f26b46f28de3b211cd4826fcbcc6f736e7de0f073273c8a72e193857e18db96f6fc88d78531b5080c04f
e=65537
p=0xe5b7df49730ec987519d4cccbc710ec4048f3660f79d44fe529c0bf4fec08881cb0199b0013ba5b009e4b50558e889c7fea4f98
q=0xdb9ab04440a59e6fb6a880512da97ea46f2def16651326be1eb957de881385fffd1b26df226cca6506a06e89b7b039914debba3
d=0x5f54274a6199db23228e5a52ff536dee7cde4d8fac3592f87787042e4523efdf41bac1957406c44fb680553a7dc8597b9220fe6
fi=open("flag.enc","rb")
s=fi.read()
fi.close()
miwen=long(s.encode('hex'),16)
mingwenint=pow(miwen,d,n)
mingwenstr=hex(mingwenint)
shuchu(mingwenstr)
```

3.You're drunk!

这里用的是单表加密，可在https://quipqiup.com/将密文和一些猜测输入，得到答案

4.Fashion victim

获得gif文件，在ubuntu下使用命令identify tv.gif即可得到gif图的组成，再使用命令convert tv.gif tv.png即可获得将gif图每一帧拆分出来（但这里拆分出来的结果与PS拆分结果不同）。通过查询可知这里使用了可视密码技术加密，其原理是将图像像素拆分，在这里只需对图像像素做异或重新组回原图即可获得答案FLAG-AcsW3fK9NxJMn2，脚本如下(要将1x1的图片剔除):

```
from PIL import Image
lenalist=[]
for i in xrange(0,20):
    im=Image.open("tv-"+str(i)+".jpg")
    lenalist.append(im.load())
    width=im.size[0]
    height=im.size[1]
imnew=Image.new("L",(width,height))
i=0
j=0
while i<19:
    j=i+1
    while j<20:
        for x in xrange(width):
            for y in xrange(height):
                r=lenalist[i][x,y]
                r1=lenalist[j][x,y]
                imnew.putpixel((x,y),(r^r1))
        imnew.save(str(i)+"-"+str(j)+".jpg")
        j=j+1
    i=i+1
```

5.Public key recovery

题目给出的是RSA私钥文件内容，我们只需使用openssl提取处对应公钥文件，将其中内容提取出来求md5值，将md5填入即可得到flag

```
import hashlib
s="MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwkrxVrZ+KCl1cX27SHDI7EfgnFJZ0qTHUD6uEeSoZsiVkcu0/XOPbz1RtpK7xxpKM
tmp = hashlib.md5(s).hexdigest()
print tmp
```

6.I Lost my password can you find it?

下载获得gpp配置文件，直接寻找里面的xml文件，在里面可看到cpassword选项，这个密文是使用aes-cbc加密，密钥已被微软公布在msdn上，
为“4e9906e8fcb66cc9faf49310620ffee8f496e806cc057990209b09a433b66c1b“，直接用脚本解密即可获得答案

```
import base64
from Crypto.Cipher import AES
miwen="PCXrmCkYWyRRx3bf+zqEydW9/trbFToMDx6fAvmeCDw"
miwen=miwen+(4-len(miwen)%4)*"="
miwens=base64.b64decode(miwen)
key="4e9906e8fcb66cc9faf49310620ffee8f496e806cc057990209b09a433b66c1b".decode("hex")
iiv="\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0"
cipher = AES.new(key,AES.MODE_CBC,iiv)
mingwen=cipher.decrypt(miwens)
print mingwen
```

7.Martian message part 3

获得字符串，首先查看其长度有36位，是4的倍数，有可能使用base64加密，解密获得字符串“EOBD.7igq4;1ikb51ibOO0;:41R“，发现前四位与FLAG相似，猜测这里可能做了异或处理。尝试，发现flag

```
import base64
miwen=base64.b64decode("RU9CRC43aWdxNDsxaWtiNTFpYk9PMDs6NDFS")
#miwen="EOBD.7igq4;1ikb51ibOO0;:41R"
mingwen=""
for i in xrange(0,256):
    sign=True
    for j in miwen:
        mingwenint=(ord(j)^i)
        if mingwenint>32 and mingwenint<128:
            mingwen+=chr(mingwenint)
        else:
            sign=False
            break
    if sign:
        print mingwen
    mingwen=""
```

8.Hangovers and more: Bacon

题目中有提示bacon，观察密文可发现其中含有许多大小写字母，猜测这里是大小写字母对应’a'或‘b’，再进行培根解密即可得到答案

```
s="VoiCI unE SUpeRbe reCeTtE cONcontee pAR un GrouPe d'ArtistEs culinaiRe, dONT le BOn Gout et lE SeNs de L
codebook1 = {
    'A':"aaaaa",
    'B':"aaaab",
    'C':"aaaba",
    'D':"aaabb",
    'E':"aabaa",
    'F':"aabab",
    'G':"aabba",
    'H':"aabbb",
    'I':"abaaa",
    'J':"abaab",
    'K':"ababa",
    'L':"ababb",
    'M':"abbaa",
    'N':"abbab",
    'O':"abbba",
    'P':"abbbb",
    'Q':"baaaa",
    'R':"baaab",
    'S':"baaba",
    'T':"baabb",
    'U':"babaa",
    'V':"babab",
    'W':"babba",
    'X':"babbb",
    'Y':"bbaaa",
    'Z':"bbaab",
}
def zhuanhua(s):
    str1=""
    j=0
```

```
    for i in s:
        if ord(i)>64 and ord(i)<91:
            str1=str1+"b"
            j=j+1
        elif ord(i)>96 and ord(i)<123:
            str1=str1+'a'
            j=j+1
        if j==5:
            str1+=" "
            j=0
    return str1
def decode(s):
    cipher=""
    ss = s.split(" ")
    for c in ss:
        sign=True
        for k in codebook1.keys():
            if codebook1[k] == c:
                cipher+=k
                sign=False
                break
        if sign:
            #cipher+=c
            pass
    return(cipher)

a=zhuanhua(s)
b=decode(a)
print b
mingwen=""
```

8.Crypto object

将红带子上的字母抄写下来，获得字符串“GMODCDOOKCDBIOYDRMKDPQLDPVWYOIVRVSEOV“，进行凯撒解密，找到有着关键字母f，l，a，g的字符串“WCETSTEEASTRYEOTHCATFGBTFLMOEYLHLIUEL“。经过尝试发现这里是对字符串进行Columnar transposition加密，对其解密即可获得答案

9.Is it a secure strings?

根据题意我们得知信息secure strings，查询secure strings，在https://blogs.msdn.microsoft.com/besidethepoint/2010/09/21/decrypt-secure-strings-in-powershell/和https://blogs.msdn.microsoft.com/timid/2009/09/10/powershell-one-liner-decrypt-securestring/可以查到如何将secure strings解码以及解码原理，在https://msdn.microsoft.com/zh-cn/library/dd347656.aspx可以看到一些获得SecureString的语法，而将最后获得的非托管的BSTR使用PtrToStringAuto转变为非托管的string，输出即可得到答案(其中System.Runtime.InteropServices.Marshal用于托管和非托管之间的转变)，代码(powershell)如下

```
$Flag='76492d1116743f0423413b16050a5345MgB8AEEAYQBNAHgAZQAxAFEAVABIAEEAcABtAE4ATgBVAFoAMwBOAFIAagBIAGcAPQA9
$key = (3,4,2,3,56,34,254,222,205,34,2,23,42,64,33,223,1,34,2,7,6,5,35,12)
$SecureFlag = ConvertTo-SecureString -String $Flag -Key $key
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($S
```

Steganography:

1.You're lost? Use the map

在红点右边唯一可见的字符串是标志。

2.Victor you're hidding me something

注意诗的每个句子的开头，将他们组合便可以得到结果。

3.Missing Pieces

可以直接打开网址https://29a.ch/photo-forensics/#forensic-magnifier，载入用鼠标点击下方黑色部分，可以找到一张二维码，扫描即可得到结果。也可以选择使用photoshop打开图片，你会发现下方的黑色像素的值并不相同，为（0，0，0）和（3，3，3），将他们区分开就会发现有一张二维码，扫描即可得到结果。

```
from PIL import Image
im=Image.open("aa.jpeg")
lena=im.load()
width=im.size[0]
height=im.size[1]
imnew=Image.new("1",((width-1600),(height-1600)))
for x in xrange(1600,width):
    for y in xrange(1600,height):
        r,g,b=lena[x,y]
        if r==0 and g==0 and b==0:
            imnew.putpixel((x-1600,y-1600),0)
        else:
            imnew.putpixel((x-1600,y-1600),1)

imnew.save("aaa.jpg")
```

4.Brainsick

使用binwalk检查图片，可以发现图片结束的地方有一个rar文件，取出解压打开即可获得一张图片，打开图片即可获得答案。

5.Look inside the house

使用steghide解密图片，获得一个txt文件，打开即可获得结果