bugku 密码学题目writeup整理（3）

原创

Void&Exists 于 2019-06-27 19:06:20 发布
分类专栏： CTF 文章标签： CTF 密码学 bugku 网络安全

> 接上一篇

19.Python(N1CTF)

下载下来两个py文件，是py2.x的，我电脑里没有py2环境所以花了点时间才跳到3.X可运行状态，运行之后得到密文：

```
HRlgC2ReHW1/WRk2DikfNBo1dl1XZBJrRR9qECMNOjNHDktBJSxcI1hZIz07YjVx
```

没有思路，我太菜了，这加密算法真心看不懂，后来看了别人的writeup，才知道这是一种加解密方式相同的加密算法，只需要将密文和明文交换过来即可，只是密文要取反，所以将N1ES.py中的加密方法改为：

```
    def encrypt(self, plaintext):
        if (len(plaintext) % 16 != 0 or isinstance(plaintext, bytes) == False):
            raise Exception("plaintext must be a multiple of 16 in length")
        res = ''
        plaintext=str(plaintext,'utf-8')
        for i in range(len(plaintext)//16):
            block = plaintext[i * 16:(i + 1) * 16]
            L = block[:8]
            R = block[8:]
            for round_cnt in range(32):
                L, R = R, (round_add(L, self.Kn[31-round_cnt]))
            L, R = R, L
            res += L + R
        return res
```

再在change.py交换明文和密文即可：

```
from CTFquestion.N1ES import N1ES
import base64
key = b"wxy191iss00000000000cute"
n1es = N1ES(key)
flag = base64.b64decode(b"HRlgC2ReHW1/WRk2DikfNBo1dl1XZBJrRR9qECMNOjNHDktBJSxcI1hZIz07YjVx")
cipher = n1es.encrypt(flag)
print(cipher)
```

20.进制转换

没有拐弯抹角，考察基本的脚本编写能力

```
str="d87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40 x6b b1100101 b1101100 o141 d105 x62 d101 b110
flag=""
str=str.split(" ")
for i in str:
    if i[0]=="d":
        flag += chr(int(i[1:]))
    elif i[0]=="x":
        flag += chr(int(i[1:],16))
    elif i[0]=="o":
        flag += chr(int(i[1:],8))
    elif i[0]=="b":
        flag += chr(int(i[1:],2))
print(flag)
```

```
Welcome to kelaibei. Give you a flag as a gift.  flag{                                    } . Have a good time~
```

21.affine

仿射密码，可以使用解码工具解码，也可以写脚本破解：

```
import re
str="szzyfimhyzd"
a="abcdefghijklmnopqrstuvwxyz"
list=re.findall(r'.{1}', a)
mw=[]
flag=[]
for i in str:
    mw.append(list.index(i))
for i in mw:
    for j in a:
        if (list.index(j)*17-8)%26==i:
            flag.append(list.index(j))
key=""
for i in flag:
    key+=list[i]
print(key)
```

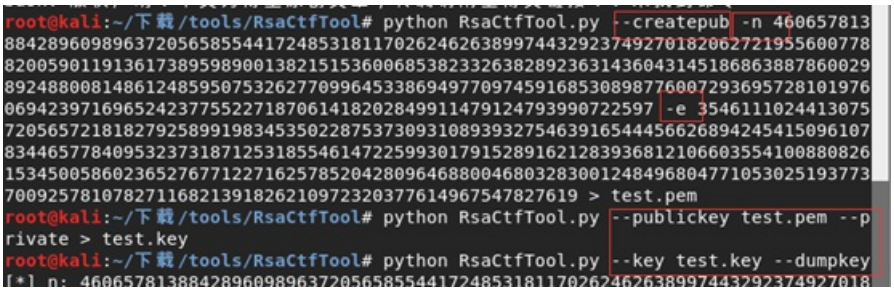
22.Crack it

Linux shadow文件破解，没想到是已经破解好的文件，kali下使用如下命令直接显示出信息即可

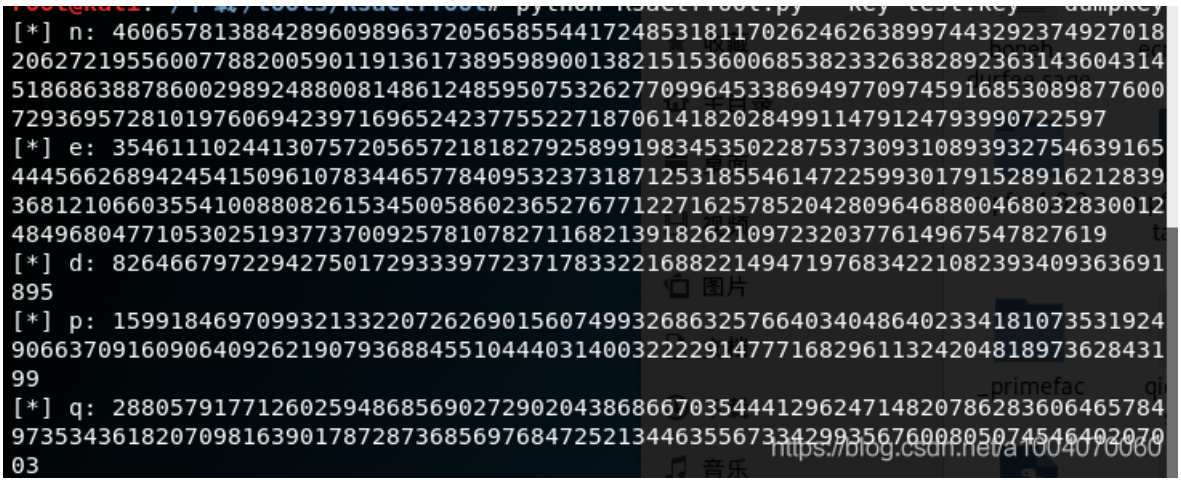
```
john --show shadow
```

23.RSA

N的长度有几百位，这种e过大的情况首先考虑wiener attack,一般使用RsaCtfTools求解p，q，关于wiener attack实现方法可以参考这位大佬的博文https://blog.csdn.net/d_vip/article/details/89162468，在此只介绍使用RsaCtfTools破解的方法（安装使用方法参考https://blog.csdn.net/qq_40657585/article/details/84865285）：



随后得到pqd：



求出明文破解出flag：

```
from Crypto.Util.number import *

n=460657813884289609896372056585544172485318117026246263899744329237492701820627219556007788200590119136173
d=826466797229427501729333977237178332216882214947197683422108239340936369189
c=382309913162293996518235675906923010600446204121917377646323846805462562284515182388429652213947118483378

# print(hex(pow(c,d,n)))
print(long_to_bytes(pow(c,d,n)))
```

24.来自宇宙的信号

怪我才疏学浅，把密码学问题做成了社工问题。。

AK总结：

bugku的题目总体偏基础，也有部分脑洞大开的题，AK过程中第19题--python（N1CTF）实在无奈参考了别的大佬的writeup，科来杯的题目由于我参加过所以感觉轻车熟路。一路做下来收获也是不小的。。。

加密