2021寒假MISC打卡DAY2

原创

煤矿路口西_CTF小学生 于 2021-01-12 20:12:43 发布 904 收藏

分类专栏： 打卡日常 文章标签： 信息安全 加密解密

本文链接：https://blog.csdn.net/LLKJSAF/article/details/112535087

> [GUET-CTF2019]zips

> 注意：得到的 flag 请包上 flag{} 提交

附件里有一名为222.zip的加密压缩包，通过ziperello暴力破解得密码723456

得到名为111.zip的加密压缩包，其中存在flag.zip以及一提示文件头损坏的setup.sh

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存失败,源站可能有防盗链机制,建议将图片保存下来直接上传上传(imrzxDgi-mF7-1610440605768)(https://s3.ax1x.com/2021/01/12/sJ4yVI.png)(https://s3.ax1x.com/2021/01/12/sJ4yVI.png)]

上图为111.zip的二进制查看。常见的伪加密。504B0102 1400 1400 *0*000此处改为偶数即可。

setup.sh

```
#!/bin/bash
#
zip -e --password=`python -c "print(__import__('time').time())"` flag.zip flag
```

按照提示执行这段代码

```
>python2 -c "print(__import__('time').time())"
1610439451.64

>python2 -c "print(__import__('time').time())"
1610439453.74

>python2 -c "print(__import__('time').time())"
1610439472.66
```

可看出跟时间戳有关（python3执行有精度差异

```
>python3 -c "print(__import__('time').time())"
1610439561.7353652
```

对flag.zip进行掩码爆破（出题时时间戳比已知的数字小，至于小多少就自行猜测了

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-1fGRmCW1-1610440605772)(https://s3.ax1x.com/2021/01/12/sJTiiq.png)]

密码1558080832.15

```
flag{fkjabPqnLawhvuikfhgzyffj}
```

> [SUCTF 2019]Game

> 感谢菠萝吹雪师傅出题。
> flag 请替换 SUCTF{} 为 flag{} 后提交。

图片貌似没啥东西，src里存在index.html,查看源代码发现

```
<?php echo "here is your flag:ON2WG5DGPNUECSDBNBQV6RTBNMZV6RRRMFTX2===" ?>
```

base32:

```
suctf{hAHaha_Fak3_F1ag}
```

返回观察图片，尝试lsb隐写后可得到

```
U2FsdGVkX1+zHjSBeYPtWQVSwXzcVFZLu6Qm0To/KeuHg8vKAxFrVQ==
```

此处划重点U2FsdGVkX1开头的为DES加密！

> 脑洞：密文为上述字符串，密钥为suctf{hAHaha_Fak3_F1ag}，通过http://www.metools.info/code/c27.html解密得到

```
suctf{U_F0und_1t}
```

> [MRCTF2020]千层套路

> 得到的 flag 请包上 flag{} 提交。
> 感谢天璇战队供题。
> 天璇战队平台：http://ctf.merak.codes/

这道题算是能得到锻炼的好题叭

首先是套娃解zip，名字就是下一层的密码：

```
import zipfile,os
def unzip(zipname):
    while True:
        passwd = zipname.split('.')[0]
        zf = zipfile.ZipFile(zipname,'r')
        zf.extractall(pwd=passwd.encode())
        zf.close()
        os.remove(zipname)
        zipname = zf.namelist()[0]
        zf.close()
unzip("0573.zip")
```

得到qr.txt：40000行格式为

```
(255, 255, 255)
```

不难想到是RGB成像。

40000=200*200

修改手头脚本：

```
from PIL import Image

x = y = 200
img = Image.new("RGB",(x,y))
file = open('qr.txt','r')

for width in range(0,x):
    for height in range(0,y):
        line = file.readline()
        print line
        if(line[1:2] == '2'):
            rgbs = line[1:4]+','+line[6:9]+','+line[11:14]
        if(line[1:2] == '0'):
            rgbs = line[1:2] +','+ line[4:5] +','+ line[7:8]
        rgb = rgbs.split(',')
        img.putpixel((width,height),(int(rgb[0]),int(rgb[1]),int(rgb[2])))
img.save('rgb.jpg')
```

得到一张二维码。扫码得

```
MRCTF{ta01uyout1nreet1n0usandtimes}
```

> 调通脚本的过程真是太有成就感了

> 二维码

> 一不小心把存放flag的二维码给撕破了，各位大侠帮忙想想办法吧 注意：得到的 flag 请包上 flag{} 提交

我爱PS（当然不可能了：）

修了半天依然不能识别，于是还是手拼叭淦

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-kQ7GRjsG-1610449428722)(https://s3.ax1x.com/2021/01/12/sYloo8.png)]

> [WUSTCTF2020]爬

> 得到的 flag 请包上 flag{} 提交。
> 感谢 Iven Huang 师傅供题。
> 比赛平台：https://ctfgame.w-ais.cn/

有一说一，在做了上一题的死亡二维码后，看到这道题的头都大了。

无后缀名的文件-》查看二进制-》.pdf-》提示flag在图片后面-》转word-》移动图片无发现-》.zip->查看word/media-》得到两张图片

一张是已知的【爬】，一张就是出题人想隐藏的

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-OlonlS7E-1610450334607)(https://s3.ax1x.com/2021/01/12/sYGD6H.jpg)]

手输十六进制

```
77637466323032307b746831735f31735f405f7064665f616e645f7930755f63616e5f7573655f70686f7430736830707d
```

```
wctf2020{th1s_1s_@_pdf_and_y0u_can_use_phot0sh0p}
```

> 看来出题人是想让咱们通过PS将pdf转换成word，这是笔者目前不会的，望告知（目前笔者用的是【迅读PDF大师】

6. **DTMF编码**

> [WUSTCTF2020]girlfriend
>
> > 得到的 flag 请包上 flag{} 提交。
> > 感谢 Iven Huang 师傅供题。
> > 比赛平台：https://ctfgame.w-ais.cn/

得到一音频，很明显是电话音

dtmf2num

```
>dtmf2num girlfriend.wav

DTMF2NUM 0.1c
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org

- open girlfriend.wav
  wave size      7466540
  format tag     1
  channels:      2
  samples/sec:   44100
  avg/bytes/sec: 176400
  block align:   4
  bits:          16
  samples:       3733270
  bias adjust:   215
  volume peaks:  -12024 12025
  normalize:     20742
  resampling to: 8000hz

- MF numbers:    47777777

- DTMF numbers:  999*666*88*2*777*33*6*999*4*4444*777*555*333*777*444*33*66*3*7777
```

999*666这串字符是啥意思呢，一开始以为是乘起来的意思。

后来知道是类似诺基亚手机的打字方式（按三次9就是y啦

```
flag{youaremygirlfriends}
```

7. *17*

> [MRCTF2020]CyberPunk
>
> > 得到的 flag 请包上 flag{} 提交。
> > 感谢天璇战队供题。
> > 天璇战队平台：http://ctf.merak.codes/

exe运行起来后□

```
I love cyberpunk2077!
It will on 2020.9.17
Since it has been open,I will give you the flag
```

修改系统时间即可

```
MRCTF{We1cOm3_70_cyber_security}每隔10s刷新一次
当前时间:
月: 9
日: 17
```

> USB

> Do your konw usb?? 注意：得到的 flag 请包上 flag{} 提交

得到233.rar及key.ftm，暂时放着，不知道有啥用

> 做压缩包题最好用winrar。360会自动过滤掉一些东西。

提示文件头损坏，对比大佬笔记https://www.freebuf.com/column/199854.html

常规文件头没问题，考虑【HEAD_TYPE应该是0x74而不是0x7A。】

得到233.png

分析一波，当Blue通道被置为0的时候出现了二维码！

```
ci{v3erf_0tygidv2_fc0}
```

图片的信息已经被榨干了，来处理key.ftm

查看二进制，能看到504b0304等字样，foremost可提取到压缩包

得到key.pcap一个usb流量

```
tshark -r key.pcap -T fields -e usb.capdata > usbdata.txt
```

通过脚本处理USB流量

```
mappings = { 0x04:"A", 0x05:"B", 0x06:"C", 0x07:"D", 0x08:"E",0x09:"F", 0x0A:"G", 0x0B:"H", 0x0C:"I", 0x0D:"J", 0x0E:"K",0x0F:"L", 0x10:"M", 0x11:"N",0x12:"O", 0x13:"P", 0x14:"Q",0x15:"R", 0x16:"S", 0x17:"T", 0x18:"U",0x19:"V", 0x1A:"W",0x1B:"X", 0x1C:"Y", 0x1D:"Z", 0x1E:"1", 0x1F:"2", 0x20:"3",0x21:"4", 0x22:"5", 0x23:"6", 0x24:"7", 0x25:"8", 0x26:"9",0x27:"0", 0x28:"\n", 0x2a:"[DEL]", 0X2B:" ", 0x2C:" ", 0x2D:"-", 0x2E:"=", 0x2F:"[", 0x30:"]", 0x31:"\\", 0x32:"~", 0x33:";",0x34:"'", 0x36:",", 0x37:"." }
nums = []
keys = open('usbdata.txt')
for line in keys:
    if line[0]!='0' or line[1]!='0' or line[3]!='0' or line[4]!='0'or line[9]!='0' or line[10]!='0' or line[12]!='0' or line[13]!='0'or line[15]!='0' or line[16]!='0' or line[18]!='0' or line[19]!='0'or line[21]!='0' or line[22]!='0':
        continue
    nums.append(int(line[6:8],16))
keys.close()
output = ""
for n in nums:
    if n == 0 :
        continue
    if n in mappings:
        output += mappings[n]
    else:
        output += '[unknown]'
print 'output :\n' + output
```

得到

```
output :
KEYXINAN
```

至此，我们已经得到了一个密文ci{v3erf_0tygidv2_fc0}和密钥XINAN

需要密钥的文本加密，考虑维吉尼亚编码：

```
fa{i3eei_0llgvgn2_sc0}
```

由于没有看到flag头，一把梭得到

```
flag{vig3ne2e_is_c00l}
```