2018科来杯WriteUp

原创

向那风 于 2018-11-07 21:38:30 发布 2021 收藏 2
分类专栏： WriteUp 文章标签： 2018科来杯 WriteUp
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/x_yhy/article/details/83832146
版权


WriteUp 专栏收录该内容
3 篇文章 0 订阅
订阅专栏

啊哒

查看图片属性

base16：sdnisc_2018

使用binwalk分析，有个压缩包，binwalk -e 分离，输入密码得到

flag{3XiF_iNf0rM@ti0n}

进制转换

d:10进制 o:8进制 x:16进制 b:2进制

当时手撕的

d87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40

87 101 108 99 111 109 101 32 116 111 32

Welcome to

x6b b1100101 b1101100 o141 d105 x62 d101 b1101001 d46 o40 d71 x69 d118 x65 x20

107 101 108 97 105 98 101 105 46 32 71 105 118 101 32

kelaibei. Give

b1111001 o157 b1110101 d32 o141 d32 d102 o154 x61 x67 b100000 o141 d115 b100000

121 111 117 32 97 32 102 108 97 103 32 97 115 32

you a flag as

b1100001 d32 x67 o151 x66 d116 b101110 b100000 d32 d102 d108 d97 o147 d123 x31

48 32 103 105 102 116 46 32 32 102 108 97 103 123 49

0 gift. flag{1

b1100101 b110100 d98 d102 b111000 d49 b1100001 d54 b110011 x39 o64 o144 o145 d53

101 52 98 102 56 49 97 54 51 57 52 100 101 53

e4bf81a6394de5

x61 b1100010 b1100011 o60 d48 o65 b1100001 x63 b110110 d101 o63 b111001 d97 d51

97 98 99 48 48 53 97 99 54 101 51 57 97 51

abc005ac6e39a3

o70 d55 b1100010 d125 x20 b101110 x20 b1001000 d97 d118 o145 x20 d97 o40 d103

56 55 98 125 32 46 32 72 97 118 101 32 97 32 103

87b} . Have a g

d111 d111 x64 d32 o164 b1101001 x6d o145 x7e

111 111 100 32 116 105 109 101 126

ood time~

赛后看别人写的脚本

```
file = open('text.txt')

s = file.read().split(' ')

data = ''

for i in s:

   if str(i)[:1] == 'd':

      tmp = chr(int(str(i)[1:]))

      data += tmp

   if str(i)[:1] == 'x':

      tmp = chr(int(str(i)[1:], 16))

      data += tmp

   if str(i)[:1] == 'b':

      tmp = chr(int(str(i)[1:], 2))

      data += tmp

   if str(i)[:1] == 'o':

      tmp = chr(int(str(i)[1:], 8))

      data += tmp

print(data)
```

flag{1e4bf81a6394de5abc005ac6e39a387b}

日志分析

url转码，根据状态码404和200可分析出，字符是状态码为200的加1，这是状态码为200的

flag LIMIT 0,1),1,1))>101 AND

flag LIMIT 0,1),2,1))>107 AND

flag LIMIT 0,1),3,1))>96 AND

flag LIMIT 0,1),4,1))>102 AND

flag LIMIT 0,1),5,1))>122 AND

flag LIMIT 0,1),6,1))>114 AND

flag LIMIT 0,1),7,1))>112 AND

flag LIMIT 0,1),8,1))>107 AND

flag LIMIT 0,1),9,1))>108 AND

flag LIMIT 0,1),10,1))>51 AND

flag LIMIT 0,1),11,1))>111 AND

flag LIMIT 0,1),12,1))>94 AND

flag LIMIT 0,1),13,1))>48 AND

flag LIMIT 0,1),14,1))>52 AND

flag LIMIT 0,1),15,1))>94 AND

flag LIMIT 0,1),16,1))>111 AND

flag LIMIT 0,1),17,1))>47 AND

flag LIMIT 0,1),18,1))>118 AND

flag LIMIT 0,1),19,1))>100 AND

flag LIMIT 0,1),20,1))>113 AND

flag LIMIT 0,1),21,1))>101 AND

flag LIMIT 0,1),22,1))>116 AND

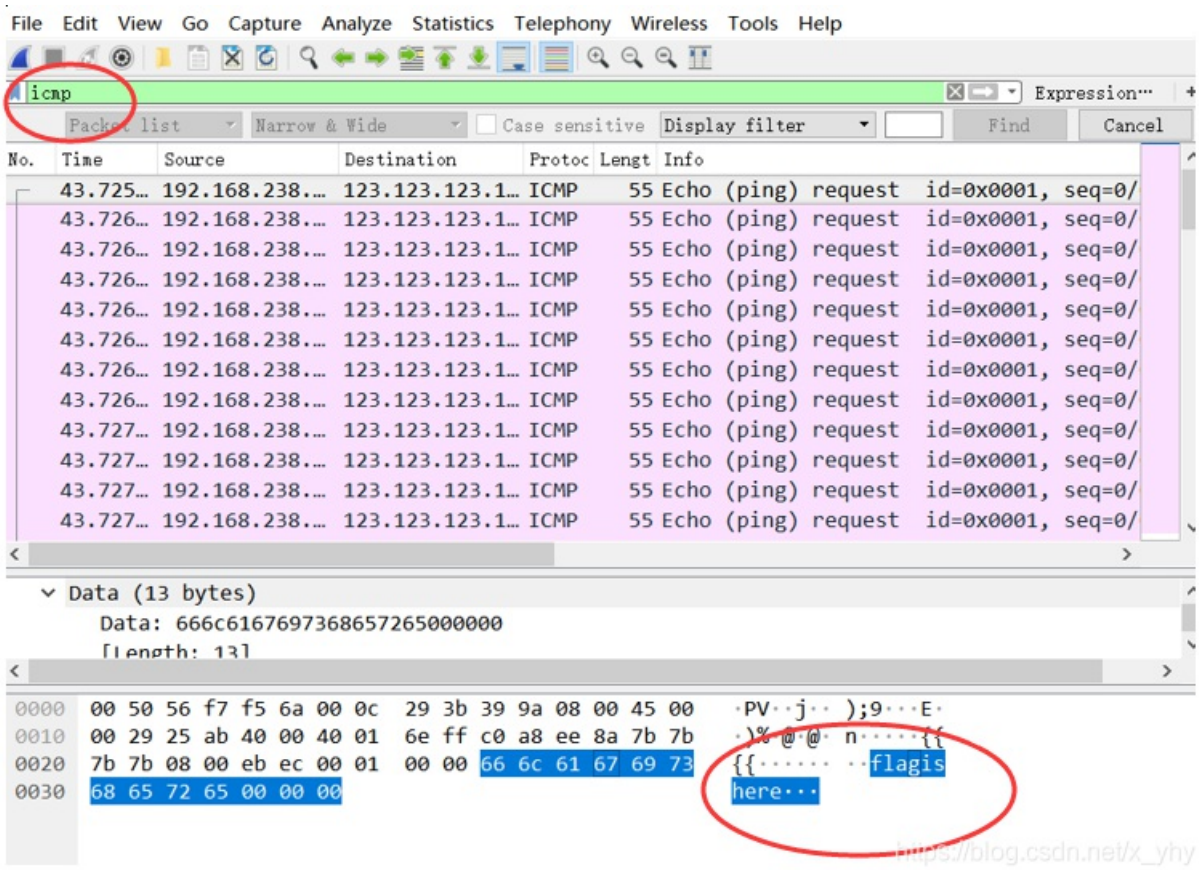
flag LIMIT 0,1),23,1))>107 AND

flag LIMIT 0,1),24,1))>124 AND

字符串ASCII为：102 108 97 103 123 115 113 108 109 52 112 95 49 53 95 112 48 119 101 114 102 117 108 125

ascii转码： **flag{sqlm4p_15_p0werful}**

特殊后门



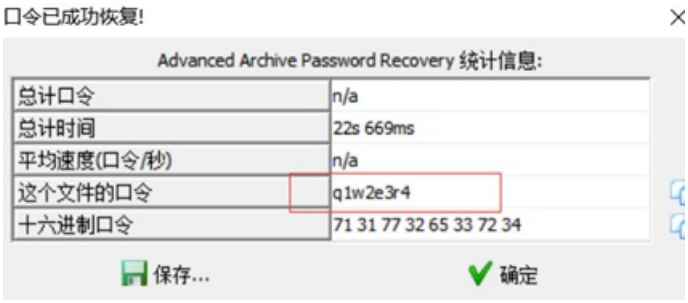
之后查看每个Icmp协议，下方都有一个字符，最后拼接成

flag{Icmp_backdoor_can_transfer-some_infomation}

神秘的文件

flag里有一个logo.png,明文攻击，使用WinRAR压缩(360不行，这好像跟压缩算法啥的有关，不同的压缩软件用的压缩算法不同)logo图片后，crc一样，

使用aapr明文攻击

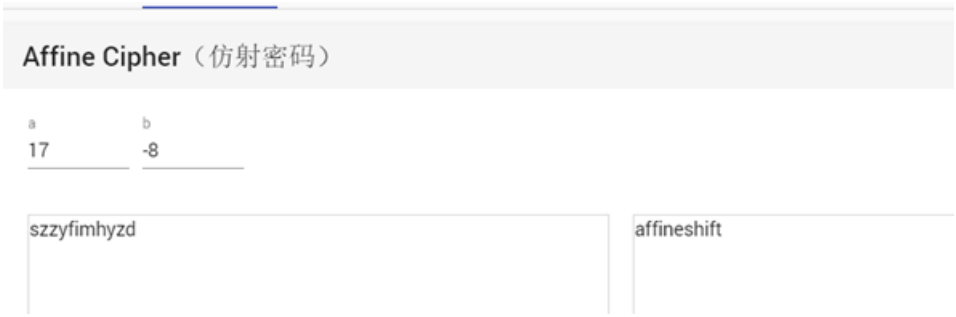


打开压缩包，发现word打不开，改成压缩包，解密，找到flag.txt文件，

ZmxhZ3tkMGNYXzFzX3ppUF9maWxlfQ==

base64解码即可 **flag{d0cX_1s_ziP_file}**

Affine

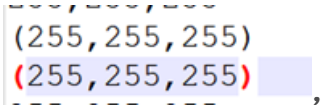


flag{affineshift}

想了解仿射密码如何解密的可以看我另一篇文章仿射密码解密（Affine Cipher）

basic

文件打开



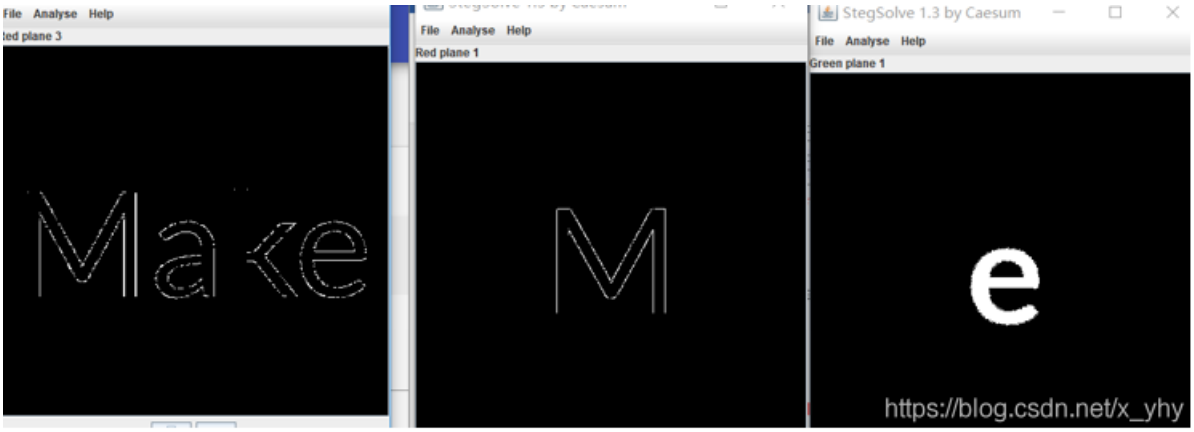
，很像RGB的表示方式，脚本跑，

```
from PIL import Image

x = 50    #x坐标  通过对txt里的行数进行整数分解
y = 2700    #y坐标  x * y = 行数

im = Image.new("RGB", (x, y))   #创建图片
file = open('basic.txt')    #打开rbg值的文件

#通过每个rgb点生成图片

for i in range(0, x):
    for j in range(0, y):
        line = file.readline()  #获取一行的rgb值
        rgb = line.split(",")  #分离rgb，文本中逗号后面有空格
        im.putpixel((i, j), (int(rgb[0]), int(rgb[1]), int(rgb[2])))    #将rgb转化为像素

im.show()   #也可用im.save('flag.jpg')保存下来
```

flag{RGB_1s_e4sY}

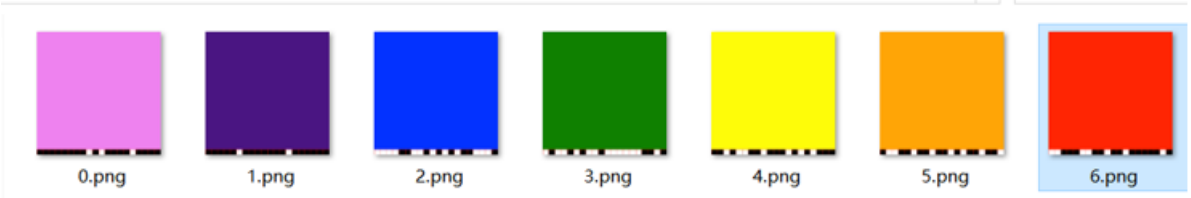
Color

图片使用StegSlove打开，



....

全部查看后： **Make Me Tall（变高）**，使用HxD打开，第二行前8组，其中前4组代表宽，后四组代表高，修改高度，之后图片样式为：



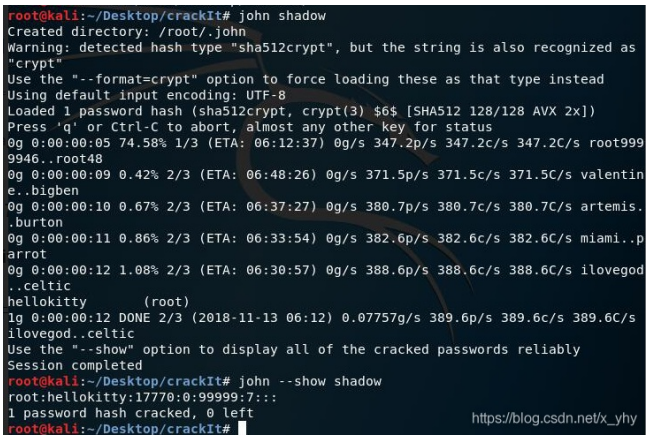
二进制，黑：1 白：0，脚本跑，竖着数组a里的内容看，

```
a = [

'11111111010111101111',

'11111011111110111111',

'00001100101010110001',

'01001010010000001101',

'11010011011101010111',

'10011011011010110110',

'00111001101101111101']

flag=''

for i in range(20):

   c=a[0][i] + a[1][i] + a[2][i] + a[3][i]+ a[4][i]+ a[5][i]+ a[6][i]

   flag+=chr(int(c,2))

print(flag)
```

flag{Png1n7erEs7iof}

Crack it

shadow文件，Linux密码文件，可使用kali自带的John工具破解,首先进入下载的文件目录下，之后



flag{hellokitty}

就先写那么多吧，想看2018科来杯全部wp的请点击第七届山东省大学生网络安全技能大赛Writeup

这是题目复现地址：

组委会提供答题平台、题目、复现地址， http://47.105.148.65:4000

学长复现了部分：http://101.132.69.145:88/