buuctf-misc部分wp（更新一下）

原创

a3uRa 于 2020-02-17 00:42:27 发布 5902 收藏 6

前言（撮合看看吧 因为直接复制的本地 所以图片就没法显示了 有什么不懂的地方可以给我留言哦~ 然后推荐一个公众号:lin先森 求关注）

b站

[BJDCTF2020]纳尼

添加gif头

[BJDCTF2020]鸡你太美

添加gif头

[BJDCTF2020]just_a_rar

爆破
ss的file format

[BJDCTF2020]认真你就输了

xls文件
binwalk

[BJDCTF2020]一叶障目□

png图片打不开
可能
png的CRC校验问题，图片的宽高被改了导致无法打开，自动修复脚本：

```
import zlib
import struct
#读文件
file = '1.png'
fr = open(file,'rb').read()
data = bytearray(fr[12:29])
crc32key = eval(str(fr[29:33]).replace('\\x','').replace("b'",'0x').replace("'",''))
#crc32key = 0xCBD6DF8A #补上0x, copy hex value
#data = bytearray(b'\x49\x48\x44\x52\x00\x00\x01\xF4\x00\x00\x01\xF1\x08\x06\x00\x00\x00')  #hex下copy grep hex
n = 4095 #理论上0xffffffff,但考虑到屏幕实际，0x0fff就差不多了
for w in range(n):#高和宽一起爆破
    width = bytearray(struct.pack('>i', w))#q为8字节，i为4字节，h为2字节
    for h in range(n):
        height = bytearray(struct.pack('>i', h))
        for x in range(4):
            data[x+4] = width[x]
            data[x+8] = height[x]
            #print(data)
        crc32result = zlib.crc32(data)
        if crc32result == crc32key:
            print(width,height)
            #写文件
            newpic = bytearray(fr)
            for x in range(4):
                newpic[x+16] = width[x]
                newpic[x+20] = height[x]
            fw = open(file+'.png','wb')#保存副本
            fw.write(newpic)
            fw.close
            # return None
```

[BJDCTF2020]你猜我是个啥

直接cat

[BJDCTF2020]藏藏藏

easy

[安洵杯 2019]吹着贝斯扫二维码

拼二维码扫描 可用ps 不好拼
BASE Family Bucket ???
85->64->85->13->16->32

压缩包注释
base32
base16
rot13
base85
base64
base85

rot13的python编解码
base85网站解码
https://base85.io/

```
import base64
a = 'GNATOMJVIQZUKNJXGRCTGNRTGI3EMNZTGNBTKRJWGI2UIMRRGNBDEQZWGI3DKMSFGNCDMRJTII3TMNBQGM4TERRTGEZTOMRXGQYDGOBWGI2
DCNBY'
print base64.b32decode(a)
b = '3A715D3E574E36326F733C5E625D213B2C62652E3D6E3B7640392F3137274038624148'
print base64.b16decode(b)
c = base64.b16decode(b)
def rot13(s, OffSet=13):
    def encodeCh(ch):
        f=lambda x: chr((ord(ch)-x+OffSet) % 26 + x)
        return f(97) if ch.islower() else (f(65) if ch.isupper() else ch)
    return ''.join(encodeCh(c) for c in s)
c = rot13(c)
print c
c = 'PCtvdWU4VFJnQUByYy4mK1lraTA='
print base64.b64decode(c)
```

[SWPU2019]伟大的侦探

01editor 选择 EBCDIC编码得到压缩包的密码
[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-zTSdOwFA-1581871148021)(misc.resources/B3FBBD16-11B2-4436-BFD5-12AFD980BC4E.png)]
解压很多小人图片
福尔摩斯里面的跳舞的小人加密
[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-tZWhvi0P-1581871148022)(misc.resources/3E10BFB3-4880-41BA-84B1-0DE8CF88B093.png)]
密码表
iloveholmesandwllm

[SWPU2019]Network

下载后发现里面只有一个txt文档，而且里面只有四个数字
这道题比较误导人的地方就是，它的标题叫做Network，刚好这四个数字又对应了四个网关地址，于是方向错误，最后对比其二进制才发现端倪，这四个数字转成8位二进制后，只有最高两位二进制不同，我们尝试写一个脚本将其最高两位提取出来，并且4个一组转换位ASCII。发现写出来的16进制数开头是50 4B，应该也就是zip了，脚本如下

```
fp = open('1.txt','r')
a = fp.readlines()
p = []
for i in a:
    p.append(int(i))
s = ''
for i in p:
    if i == 63:
        a = '00'
    elif i == 127:
        a = '01'
    elif i == 191:
        a = '10'
    elif i == 255:
        a = '11'
    s += a

import binascii
flag = ''
for i in range(0,len(s),8):
    flag += chr(int(s[i:i+8],2))
flag = binascii.unhexlify(flag)
wp = open('ans.zip','wb')
wp.write(flag)
wp.close()
```

解压
base64循环解码

[GXYCTF2019]gakki

参考

https://www.cnblogs.com/Cl0ud/p/12207865.html

foremost
爆破
[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-EwrgjllX-1581871148023)
(misc.resources/EEB01820-AAB8-411D-8096-48219B74F8FF.png)]

flag.txt文件里面是一大堆乱七八糟的字符，这种无规律的字符集我们就尝试
字频统计
词频分析

```
alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()_+- ={}[]"
f = open("flag.txt", "r")
data = f.read()
result = {d:0 for d in alphabet}

def sort_by_value(d):
    items = d.items()
    backitems = [[v[1],v[0]] for v in items]
    backitems.sort(reverse=True)
    return [ backitems[i][1] for i in range(0,len(backitems))]

for d in data:
    for alpha in alphabet:
        if d == alpha:
            result[alpha] = result[alpha] + 1

print(sort_by_value(result))
```

[SWPU2019]我有一只马里奥

参考

https://www.freebuf.com/articles/terminal/195721.html

ntfs
Windows ADS

一个exe 运行得到一个1.txt
dir /r
[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-6htxFiVY-1581871148024)
(misc.resources/F02DCAE7-8B75-41B8-A251-D2B94F3645D5.png)]
notepad 1.txt:flag.txt

[SWPU2019]神奇的二维码

binwalk -e
base64
摩尔斯密码

[GXYCTF2019]佛系青年

http://www.keyfc.net/bbs/tools/tudoucode.aspx
与佛论禅

john-in-the-middle

导出http对象
logo.png到ss打开

寂静之城 | 社工题

http://foreversong.cn/wp-content/uploads/2017/07/%E7%AC%AC%E4%B8%80%E5%B1%8AHappyCTF%E5%A4%A7%E8%B5%9BWriteUp.pdf
https://www.cnblogs.com/puluotiya/p/5462114.html
http://blog.sina.com.cn/s/blog_bb4702370102w4oa.html

aes
http://tool.chacuo.net/cryptaes

[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-BOyWJlPO-1581871148024)(misc.resources/D7A02F2F-CBCC-48FB-ADB2-4CBF243488BB.png)]

间谍启示录

解压iso
解压exe
发现flag.exe 运行得到flag

这是什么 | easy

改后缀为rar
解压
其中一个文件 010editor打开
发现
)[+[]]+([][(![]+[])[+[]]+([![]
f12 运行

派大星的烦恼 | easy

https://shawroot.hatenablog.com/entry/2019/09/14/BUUCTF-%E6%B4%BE%E5%A4%A7%E6%98%9F%E7%9A%84%E7%83%A6%E6%81%BC

```
a = "01101100 00101100 00001100 01101100 10011100 10101100 00001100 10000110 10101100 00101100 10001100 00011100
 00101100 01000110 00100110 10101100 01100110 10100110 01101100 01000110 01101100 10100110 10101100 01000110 001
01100 11000110 10100110 00101100 11001100 00011100 11001100 01001100"
a = a.split()
flag = ''
for i in a:
    flag += chr(int(i[::-1],2))

print flag
```

真的很杂 | easy

binwalk -e
发现一个zip 解压 是apk的内容
改后缀为apk
反编译apk

小易的U盘 | 脑洞

解压iso

[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-JKWWFUCi-1581871148025)(misc.resources/E63FE8B6-11D7-4C68-8F6E-203A814F027C.png)]

[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-3XHdtcsp-1581871148025)(misc.resources/B84EC567-2D99-416D-A817-48257E6020D0.png)]

大白 | png图片改高度

png图片改高度
[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-R6a435tE-1581871148026)(misc.resources/A793E7C2-2364-4D92-9958-C0346ED0C71A.png)]

基础破解 | archpr爆破

你竟然赶我走 | 打开

010editor打开 最后面flag

ningen | easy

binwalk
foremost
爆破

LSB | ss

[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-tGw1uww1-1581871148026)(misc.resources/90DF4A8A-EBDC-4477-BA51-78B69492BB2C.png)]

[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-jQdvZylH-1581871148026)(misc.resources/ED1F80C7-2774-4930-8E6D-6FB9674DCDCB.png)]

save bin
二维码扫描

rar | archpr爆破

qr | 二维码扫描

乌镇峰会种图 | 记事本打开

wireshark | 导出http对象

导出http对象
搜索flag

[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-hHQzFW4O-1581871148027)(misc.resources/493EB390-F0C6-41FE-B536-DFD30662F914.png)]
找到password

文件中的秘密 | 右键属性

假如给我三天光明

盲文
wav文件
audacity打开
摩尔斯密码

来首歌吧 | 摩尔斯密码

镜子里面的世界 | ss

[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-nE4VnMCA-1581871148027)(misc.resources/835CF311-43D5-4B3A-9649-468760EBE26D.png)]

爱因斯坦

binwalk
foremost
图片属性
this_is_not_password
为解压密码

小明的保险箱

binwalk
foremost
爆破四位数字密码

FLAG

ss打开
[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-OVP6ROMu-1581871148028)(misc.resources/D61DA1F8-1570-48BA-9E62-A22C4E1C698B.png)]

save bin
解压缩 一个elf文件
ida打开看到hctf

strings 1 | grep “hctf”

easycap

追踪tcp流

被嗅探的流量

导出http对象
一个php文件 实际上不是php 用010editor打开 十六进制视图
flag

梅花香之苦寒来

010editor打开 后面很多0-9 a-f

```
with open('1.txt','r') as h:
    h=h.read()
bb = ''
tem=''
for i in range(0,len(h),2):
    tem='0x'+h[i]+h[i+1]
    tem=int(tem,base=16)
    bb += (chr(tem))

with open('2.txt','w') as ff:
 ff.write(bb)
```

[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-K4vGUcb5-1581871148029)(misc.resources/2C361B0F-4B19-4ED3-8B87-61C976FB55A5.png)]

```
with open('2.txt','r') as f:
 f = f.read()
b = open('3.txt','w')
for i in f.split('\n'):
 b.write(i.lstrip('(').rstrip(')').replace(',',' ')+'\n')
```

[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-nMe1aOkD-1581871148030)(misc.resources/31B60B84-C913-4EB2-A1B1-98C6B20B6024.png)]

gnuplot
plot '3.txt'

https://tu.sioe.cn/gj/huidu/
灰度处理

后门查杀

d盾扫一下

[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-PuM9rCN6-1581871148030)(misc.resources/914DE44A-6C3E-4F68-B48C-A61270FF46F6.png)]

snake

binwalk
foremost
base64

https://blog.csdn.net/zz_Caleb/article/details/91973626

http://serpent.online-domain-tools.com/

[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-tQF0Mkpw-1581871148031)(misc.resources/65941DD7-61AA-4EF0-A8D7-D47047D49D44.png)]

```
a = '''C T F { w h o _ k n e w _ s e r
p e n t _ c i p h e r _ e x i s
t e d } .'''
print a.replace(' ','').replace(' ','').replace('\n','')
```

荷兰宽带数据泄露

RouterPassView
打开
搜索username

九连环

binwalk
foremost
steghide info xx.jpg

steghide extract -sf xx.jpg

ko.txt

解压

另外一个世界

记事本打开
最后010
八个一组 转字符

```
import binascii

a = '''01101011
01101111
01100101
01101011
01101010
00110011
01110011'''
b = ''
for ii in a.split('\n'):
 b += chr(int(ii,2))
print b
```

神秘龙卷风

爆破
++++++.>++++++++++++++
ook
brainfuck

https://www.splitbrain.org/services/ook

面具下的flag

binwalk
foremost

7z解压vmdk
7z x filename

https://www.splitbrain.org/services/ook

刷新过的图片

F5-steganography

java Extract ./Misc.jpg -e misc

得到一个压缩包 伪加密直接解压

穿越时空的思念

audacity 打开
摩尔斯密码

Mysterious □

输入
122xyz

od也应该可以

webshell后门

d盾扫描

隐藏的钥匙

记事本
搜索flag

数据包中的线索

导出http对象

由开头”/9j/”，可知以下数据为jpg图片，“/9j/”经base64解码后结果为“\xff \xd8 \xff”，该三字节为jpg文件的开头三字节，所以可推断出以下文件为jpg文件。

浏览器

菜刀666

导出http对象

压缩包 需要密码
图片 画着密码

https://4hou.win/wordpress/?paged=2&cat=1023

喵喵喵

ss得到png
[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-gedUUfgG-1581871148031)
(misc.resources/E3C4A6FB-21D7-47D6-B8BB-066E5B784ED6.png)]

[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-ZiqgK7iz-1581871148032)
(misc.resources/A9B7CFBF-4E5A-4C31-A94E-EA0C4E034E26.png)]
修改高度

[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-GUPulWD5-1581871148032)
(misc.resources/8B2CC685-EC6C-480C-B2DF-F0ADBF751B8C.png)]
win10画图 反色
扫描二维码

下载一个压缩包
只能用winrar解压

ntfstreamseditor扫描

pyc文件

https://tool.lu/pyc/
反编译 得到加密脚本和c 逆向

```
def decrypt(c):
    c = c[::-1]
    flag = ''
    for i in range(len(c)):
        if i%2 == 0:
            s = int(c[i])-10
        else:
            s = int(c[i])+10
        s = chr(s^i)
        flag += s
    return flag
```

弱口令

压缩包打开 注释中不可见字符
复制到sublime text3 全选 显示摩尔斯密码
解码 转大写
解压
lsb隐写
lsb.py

蜘蛛侠呀

时间隐写

https://coxxs.me/642
http://yulige.top/?p=236

tshark -r out.pcap -T fields -e data >out.txt

```
lines = open("out00.txt",'rb').readlines()
files = open("out01.txt","wb")
for line in lines:
 files.write(line.strip().decode('hex'))
files.close()
```

```
import base64
lines = open("out0.txt",'rb').readlines()
file1 = open("new",'wb')
result = ''
for line in lines[4:-4]:
 result += line[9:].strip()
file1.write(base64.b64decode(result))

'''
result = ''
lines = open("out.txt",'rb').readlines()
print lines[4:-4]
'''
```

```
a = open("out01.txt",'rb').readlines()
file1 = open("result1",'wb')
for i in range(len(a)):
 bb = a[i].strip()
 if bb == a[i-1].strip():
  continue
 file1.write(bb+'\n')
```

解压 flag.gif
identify -format “%T” flag.gif

[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-yQYB8FdQ-1581871148033)(misc.resources/3C0102F3-8F39-4F33-8011-4B09EB0AAD9F.png)]

明显的二进制了，把20换0，把50换1.

binary转hex转ascii码

```
# coding:utf-8
import binascii
import hashlib
# import base64
# lines = open('result1.txt','rb').readlines()
# file = open('file','wb')
# flag = ''
# for line in lines[1:-1]:
#  flag += line[9:]
# file.write(base64.b64decode(flag))

a = open("11",'r')
b = a.read().replace("“",'').replace("”","").replace("20",'0').replace("50",'1').replace('6','')

bb = binascii.unhexlify(hex(int(b,2))[2:-1])
print 'flag{'+hashlib.md5(bb).hexdigest()+'}'
```

identify -format “%s %T \n” flag.gif

我爱Linux

https://www.cnblogs.com/puluotiya/p/5462114.html

https://www.cnblogs.com/harmonica11/p/11365782.html

python序列化文件的数据
将FF D9后保存出来，将序列化文件读出来

```
import pickle
with open('q', 'rb') as f:
    f= pickle.load(f)
data = list()
for i in range(len(f)):
    tem = [' ']*100
    data.append(tem)
for i, j in enumerate(f):
    for m in j:
        data[i][m[0]] = m[1]
for i in data:
    print(''.join(i))
```

[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-lquvlKlC-1581871148033)
(misc.resources/FFF2AF2F-1C7E-430C-AC2A-6C3A7E7B50F9.png)]

usb

https://wenku.baidu.com/view/b7889b64783e0912a2162aa4.html
rar文件结构
[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-jplzrjlo-1581871148034)
(misc.resources/684F0CD2-8436-484A-9E50-C12C24505909.png)]

[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-lkeEd9bf-1581871148034)
(misc.resources/242A34FF-73CC-4BF6-A4D2-9382CE270792.png)]

https://blog.csdn.net/like98k/article/details/79533536

https://blog.csdn.net/qq_36609913/article/details/78578406

https://www.mygeocachingprofile.com/codebreaker.vigenerecipher.aspx

```
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:"=", 0
x2F:"[",  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 l
ine[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



output :
KEYXINAN
[Finished in 0.1s]
```

binwalk xxx
foremost xxx

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

ci{v3erf_0tygidv2_fc0}

fa{i3eei_0llgvgn2_sc0}
栅栏

flag{vig3ne2e_is_c00l}

被劫持的神秘礼物

http过滤
追踪tcp流

```
import hashlib
print hashlib.md5('adminaadminb').hexdigest()
```

sqltest | sql布尔盲注

[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-6z0jXFza-1581871148034)(misc.resources/EF0299A1-C289-45A6-862C-322211B47696.png)]

voip | wireshark

https://shawroot.hatenablog.com/entry/2019/10/05/BUUCTF-voip

wireshark
电话→RTP→RTP流

点分析→播放流→一个充满机械感的声音出现惹 念出了flag

百里挑一 | exiftool

wireshark 导出http对象 很多图片
exiftool *|grep flag

[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-r7YA9DtV-1581871148035)(misc.resources/3957D3FA-0779-42B3-8CE6-ED2B5C77B98F.png)]

[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-5J39FkNd-1581871148035)(misc.resources/F2F3F755-54B9-4EA3-94B0-B2089B438A00.png)]