

攻防世界misc新手区writeup

原创

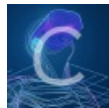
[a370793934](#) 于 2019-11-27 15:42:25 发布 835 收藏 2

分类专栏: [WriteUp](#) 文章标签: [攻防世界 misc writeup ctf](#)

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/a370793934/article/details/103276977>

版权



[WriteUp](#) 专栏收录该内容

20 篇文章 2 订阅

订阅专栏

this_is_flag

flag{th1s_!s_a_d4m0_4la9}

ext3

下载下来拿到kali下看文件类型file 21f60c9089224bc198fe7c5d03ad9001

Linux rev 1.0 ext3 filesystem data

可以将它系统挂载到kali上:

```
mount linux /mnt
```

挂载上后看一/mnt/下的文件, 用find ./ -name "flag.txt"命令查找

得到flag.txt文件内容为: ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=

base64解码得到

flag{sajbcibzskjjcnbhsbvcjbjszcszkbkzj}

give_you_flag

下载下来是gif文件用工具 stegosolve.jar分析

发现其中有一帧含有二维码

提取出来, 用画图软件补上残缺的二维码的三个角

然后二维码工具扫描得到flag

flag{e7d478cf6b915f50ab1277f78502a2c5}

pdf

下载打开发现是个图片

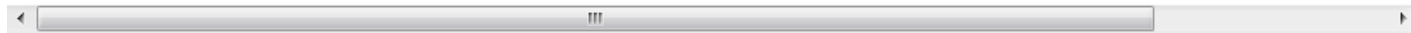
ctrl+a全选ctrl+c复制, 再粘贴到记事本, 得到flag

flag{DajiDali_JinwanChiji}

gif

一大堆的黑白图片，进行白为0黑为1的转换得到：

```
0110011001101100011000010110011101111011010001100111010101001110010111110110011101101001
```

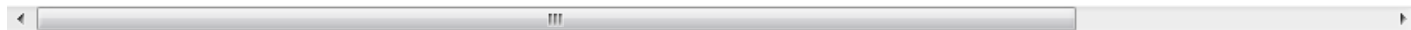


二进制转字符串得：flag{FuN_giF}

掀桌子

一串密文：

```
c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfabe3f5e7e
```



发现字符串由0-9、a-f组成，我们知道2位十六进制可表示1个字节，写脚本将该字符串两两分组转换成字节，发现所有字节均大于128，我们又知道ASCII码表示范围是0-127，于是每一个字节都减去128，再转换成字符串，得到flag

解密方法，两个一位，16进制转10进制，然后减去128再转成字符

python脚本

```
string =
```

```
"c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfabe3f5e7e"
```



```
flag = "
```

```
for i in range(0,len(string), 2):
```

```
    s = "0x" + string[i] + string[i+1]
```

```
    flag += chr(int(s, 16) - 128)
```

```
print(flag)
```

得到

Hi, FreshDog! The flag is: hjzcydjzbdckzkzcugisdchjysbdf

如来十三掌

与佛论禅解密：<http://www.keyfc.net/bbs/tools/tudoucode.aspx>

得到base64码：MzkuM3gvMUAwnzuvn3cgozMIMTuvqzAenJchMUAeqzWenzEmLJW9

但是要先进行ROT13然后再base64解码：

```
flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}
```

base64stego

下载得到zip文件打开需要密码

是伪加密，用winrar修复功能修复下可打开

得到一串base64加密文件，解密几行得到

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.

翻译：

隐写术是一种艺术和科学，以隐藏信息的方式，除了发送者和预期接收者之外，没有人怀疑消息的存在，通过默默无闻的安全形式。

base64隐写，解密python脚本：

```
#coding=utf-8

def get_base64_diff_value(s1, s2):

    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+'

    res = 0

    for i in xrange(len(s2)):

        if s1[i] != s2[i]:

            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))

    return res

def solve_stego():

    with open('stego.txt', 'rb') as f:

        file_lines = f.readlines()

        bin_str = ""

        for line in file_lines:

            steg_line = line.replace('\n', "")

            norm_line = line.replace('\n', "").decode('base64').encode('base64').replace('\n', "")

            diff = get_base64_diff_value(steg_line, norm_line)

            print diff

            pads_num = steg_line.count('=')

            if diff:

                bin_str += bin(diff)[2:].zfill(pads_num * 2)

            else:

                bin_str += '0' * pads_num * 2
```

```
print goflag(bin_str)
```

```
def goflag(bin_str):
```

```
    res_str = "
```

```
    for i in xrange(0, len(bin_str), 8):
```

```
        res_str += chr(int(bin_str[i:i + 8], 2))
```

```
    return res_str
```

```
if __name__ == '__main__':
```

```
    solve_stego()
```

得到

Base_sixty_four_point_five

flag{Base_sixty_four_point_five}

功夫再高也怕菜刀

foremost分离文件，得到一个加密的压缩包，点进去查看发现一个flag.txt文件，wireshark下查找flag.txt字符串，追踪TCP流，最终在第1150个包发现一段图片的16进制编码，将其用winhex另存为一个图片，得到压缩包的密码，解压得到flag.

flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}