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

本文链接：https://blog.csdn.net/a370793934/article/details/103276977

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{sajbcibzskjjcnbhsbvcjbjszcszbkzj}

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{security_through_obscurity}

stegano

pdf文件，打开许多文字，linux中查看pdf信息：使用命令pdfinfo

得到Tm9wZSAsIG5vdCBoZXJlIDspCg==base64解码后是Nope , not here ;)

再ctrl+a全选ctrl+c复制，再粘贴到记事本，得到一串

BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB

考虑是摩尔斯电码将A替换为.B替换为-

-.-. --- -. --. .-. .- - ..- .-.. .- - .. --- -. ... --..-- ..-. .-.. .- --. ---... .---- -. ...- .---- ..... .---- -... .-.. ...-- -- ...-- ....- --. ...--

解码得到

congratulations,flag:1nv151bl3m3554g3

SimpleRAR

1、打开附件RAR压缩包，提示有一个文件 secret.png已损坏，打开flag.txt，里面没有flag，那么flag应该就在损失的文件中。

2、我们使用 winhex 对RAR文件进行修复 ，ctrl+f搜索flag。"not here"这部分内容就是flag.txt的，那么下一个文件内容就是在A8 3C 7A开始，问题出现在7A，这是HEAD_TYPE标识，74才是表明这一块区域是一个文件。把7A修改为74，保存，就可以解压RAR文件了。

3、解压出来一个新的文件secret.png，再扔进winhex，发现这原本是一个gif动态图片，47 49 46 就是GIF格式的文件头部，有关部分文件的文件头格式可以转载到：https://www.cnblogs.com/lwy-kitty/p/3928317.html

4、那就把文件后缀名改为gif，既然是动态图片，就用stegsolve.jar打开，一片空白，应该是LSB隐写，

有关LSB隐写的原理，可转载到：https://segmentfault.com/a/1190000016223897?utm_source=tag-newest

不停地点击”>“，直到显现出半张二维码图。

5、另一半应该在其它帧中，点击FrameBroswer逐帧分析，发现还有另一帧，保存下来，格式为png，如果是bmp会出错，同前者做法一样，我们找到另一半二维码，PS拼接二维码，再修复缺失的一个角，扫码即可得到flag。

flag{yanji4n_bu_we1shi}

坚持60s

下载打开发现是一个java做的游戏，用java反编译工具反编译，在文件中可以找到PlaneGameFrame.class中找到flag

但内容是经过base64编码了，解码后得到：

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：
c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e

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 = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e
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: hjzcydjzbjdcjkzkcugisdchjyjsbdfr

如来十三掌

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

得到base64码：MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9

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}