bugku 杂项1-20 writeup

原创

louisPCuesr 于 2019-10-14 17:47:50 发布 242 收藏 1

一.签到

直接扫描题目所给的二维码关注公众号就可以得到flag。

flag格式通常为flag{.....}

或者key{.....}

或者KEY{.....}

得到flag后直接复制粘贴到题目框里，然后submit提交。

二.这是一张单纯的图片

将图片下载下来，打开看一下，没有任何发现，这时我们右键查看图片属性，也没有什么特别的。我们运用十六进制解析文件的工具winhex打开图片，拖到底部，我们发现它包含了一串unicode编码，不废话，直接在线解码，或者用html文件写出来，unciode可以在网页中直接显示。

最后得到flag　flag：key{you are right}

三. 隐写

打开题目，下载了一个压缩包，解压后得到一张图片。ctf的隐写题最多的就是图片隐写，打开图片，没发现什么有用信息。右键看一下图片属性，发现高度和宽度不确定，可能有问题。图片隐写常见的方法就有修改图片宽高尺寸来隐藏图片的信息的。我们把图片用winhex打开，发现这是个png图片，那么它的头文件格式就是十六进制数89504E47，高度和宽度在第二行的前八个字节，前四位表示宽度，后四位表示高度，我们先把宽度高度设计修改成一样的，都是500像素，看看会出现什么。

果然，flag出现了，BUGKU{a1e5aSA}

四.telnet

打开题目，依然是一个压缩包，解压缩得到一个纯数据流p.cap的数据包，直接用wireshark打开，然后追踪源，得到flag

五.眼见非实

得到一个名字是zip没有后缀的文件，用winhex打开，发现头文件是pk，压缩包，修改文件名，解压，得到一个docx文件，但是还是打不开，再放到winhex中打开，还是一个压缩包，再修改文件名，解压，得到flag。

六.啊哒

打开题目，得到一个压缩包，解压后是一张图片，老规矩，我们看一下图片的属性，看到照相机属性是一串十六进制数，暂时不知道干什么，先记下来。然后把图片用winhex打开，看到图片中包含exif，这说明这不是一张单独的图片，它里面包含着东西。用kali的binwalk工具分析以下，果然，图片中包含着一个压缩包。用foremost命令分离图片，得到一个压缩包文件，尝试解压，提示需要密码，爆破不现实，密码坑定隐藏在图片中，我们想到图片属性中的那串十六进制数，尝试输入，密码错误，随机想到，是不是十六进制数对应的ascii码，转一下，输入，对了，得到了flag

七.又一张图片，还单纯吗

打开题目，得到一个文件，先用winhex打开，看到里面包含着exif猜测图片中包含着别的文件，尝试用binwalk工具分离文件果然得到一张包含flag的图片，用图片转文字软件得到flag

八.猜

这题打开后是一张照片，图片很单纯，没有隐藏文件，也没有宽度高度的问题，也没有包含什么隐藏信息，就是单纯的猜，如果是对娱乐圈比较了解的话，还是能才出来这是刘亦菲的。

九.宽带信息泄露

因为是宽带信息泄露，所以此文件应该是路由器的备份文件，路由器的备份文件通常包括了isp的用户名和密码，路由器的登陆密码，无线网络的关键。我们可以用routerpassview这个工具打开。这个工具主要是找回路由器密码的工具，换言之，就是查看路由器备份文件的工具。用routepassview打开之后，题目要求的flag是用户名，直接搜索username，得到flag。

十.隐写2

打开题目得到一张图片，老规矩先放在winhex中打开，看到了exif，所以图片中坑定包含了什么东西，拖到最后，发现了flag.rar

所以废话不多说，直接foremost分离，分离出一个压缩包，和一张图片，图片上说压缩包的密码是三个数字，直接爆破，使用kaliLinux自带的暴力破解工具fcrackzip，打开工具，这个fcrackzip是一个命令行形式的工具，没有gui，没关系，先进到压缩包所在的目录中，然后输入下面一行命令

fcrackzip -b -c1 -l 3 -u flag.zip

-b:暴力破解

-c1:密码是纯数字 如果是纯字母的话就是c2 如果是数字字母混合的话就是c3，如果是小写字母的话就是ca（a-z），

-l：密码长度

-u:后面跟压缩包名字

成功破解出密码871

解压压缩包，得到一张图片，用winhex打开得到一串flag

f1@g{eTB1lEFyZSBhlGhAY2tlciE=}

显然，这是一串加密的flag，里面是base64码加密，因为有等于号。

使用在线解密工具解密，得到flag：fl@g{y0u Are a h@cker!}

十一.多种方法解决

打开题目，得到一个exe文件，肯定是执行不了，所以把他放在winhex中打开，看到是一个base64加密的图片，直接把后缀名改为jpg，发现是打不开的，没办法，只能考虑能不能base64解密了，在查了一些资料后，发现有一个在线base64转图片的工具http://imgbase64.duoshitong.com/，直接把winhex中的base64编码复制粘贴在编码框中，尝试生成图片，发现不行。考虑可能是格式的问题，估计winhex直接复制，格式会有错误。那就将exe文件的后缀名改为txt，将txt文件中的base64加密的编码复制，粘贴到编码框中，还原图片，果然成功了，得到一张二维码，扫码得到flag。

十二.闪的好快

打开题目发现一个gif文件一直在变化，所以可以用图片隐写查看神器stegsolve来打开，用其中的Frame Browser插件来解决，Frame Browser是帧浏览器，主要对GIF之类的东突进行分解，是动图变为一张张图片，便于查看。打开这个gif然后一张一张的扫码，得到flag

十三.come game

打开题目，解压压缩包，是一个小游戏，通关了就有答案，小游戏极难，正常玩通关的可能性不大，所以我们玩过一次后，游戏目录下会多出来一个存档save文件，题目说通关了就有flag，通关是指存档存到最后一关通过，就算通关，于是我们尝试修改存档。用winhex打开存档，发现是三个字 2 A C ,猜测 2 可能是第二关的 意思，但我们不知道游戏有几关，就三四五慢慢的试，试验到5，通关了，得到一张包含flag的图片。

十四.白哥的鸽子

打开题目，是一个名为jpg无后缀名的图片，用winhex打开，可以看出文件的头数据格式是jpg文件，在winhex中搜索flag，key KEY等字符发现都没有，但是发现了exif，好像文件里面由别的东西，但是用binwalk分析了一遍后，发现，好像就是一张单独的图片，很费解，查理一些资料，在一片常用隐写术的总结博客https://blog.csdn.net/u011028345/article/details/75311346中，我发现jpg文件的 开始标志是FFD8 结束标志：FFD9,迅速把winhex拉到最后，发现结束标志不对，然后发现了一串疑似不是乱码的数据fg2ivyo}l{2s3_o@aw__rcl@，查了下资料，发现好像是栅栏加密的数据，所以用栅栏在线解密，得到flag。

十五.linux

打开题目，下载了一个压缩包，后缀为tar.gz，放在Linux中，用tar -xf 文件名解压，得到一个名为flag的二进制文件，直接在flag文件中检索'flag'字符串，没有检索到有用的信息，换一个检索字段，换成key，使用检索命令

grep 'key' -a flag

成功检索到flag ：key{feb81d3834e2423c9903f4755464060b}

十六.隐写3

打开题目，解压得到一张图片，在winhex中修改图片高度与宽度一致，即可得到flag。

十七.做个游戏

打开后发现是由java代码写成的游戏，我们用jd-gui-v0.3.6这个java代码逆向工具来将其代码解析，很容易的在planegameFrame文件中找到flag：flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}

十八.想蹭网先解开密码

打开题目是一个wifi数据流文件，其中由eapol协议的四次握手包，给你数据包让你破解密码基本都是爆破。

爆破wifi密码，需要先用crunch生成密码字典，再用aircrack工具进行爆破。

crunch 11 11 -t 1391040%%%% -o password.txt

生成十一位纯数字密码字典，前七位题目给了，后四..位用%表示，穷举，输出为password.txt

aircrack-ng -a2 wifi.cap -w password.txt

使用aircrack工具爆破

可以看到第三个存在握手包，所以选择第三个，成功获得密码。

十九.linux 2

打开题目，一个压缩包，打开后是一个brave二进制文件，在kali中直接把搜索’key‘

根据题目中给的提示

grep 'KEY' -a brave

得到key

二十.账号被盗了

使用burpcuit软件进行抓包，在抓到的包中，close改成open即可获取flag