# bugku misc writeup（部分）

原创

youshangfashi 于 2017-09-20 17:01:28 发布 
分类专栏： CTF 文章标签： CTF bugku writeup



1、这是一张单纯的图片？？？

本题给出一张图片，用notepad++打开，然后就能看到最后一行有一些规律的数字（key{you are right}）猜测是ASCII，然后翻译出来（key{you are right}）,这就是flag。

2、隐写2

本题给出一个压缩包，解压后是一张图片，然后用winhex打开，在第二行第2,3列是宽，6,7列是高，把第六列的01改为11，那张图片就恢复原来的样子，flag就在那张图片上。

3、telnet

本题给出一个networking.pcap文件，用wireshark打开，然后随便打开一个消息，用tcp追踪流，就能看到flag。

4、有一张图片，还单纯吗？？

题目给了一张图片，把它拖到kali里面，在终端中，用foremost '/root/桌面/2.jpg'，然后在文件里的output文件夹里，有一个jpg文件，里面有两张图片，有一张上面就是flag.

5、多种方法解决（题目的提示，在解题过程中会碰到一张图片）

题目给了一个KEY.exe文件，用notepad++打开，然后就能看到（ 加上一段base64代码 ）说明这是base64转图片的情况，在 https://www.base64decode.org/ 网站上，进行解码，会得到一张图片，是一张二维码，然后用手机扫码就能得到flag。

6、猜？（提示KEY就是某人名字的全拼）

题目给出一张只能看到半截脸的图片，用百度查一下，就能查出来，这个人是刘亦菲。

7、linux????

题目中给出一个1.tar.gz文件，解压后得到一个flag文件，然后拖到kali里面，用binwalk分离一下，就能得到flag。

8、中国菜刀，不在web里？

题目中给出一个caidao.zip，，打开后是一个caidao.pcapng文件，然后用wireshark打开，然后因为跟菜刀有关系，所以应该是http文件，打开最后那个http文件，右键->显示字节流分组->去掉前后两个X@Y，把左下角解码为压缩，就能看到flag。

9、又是一道隐写

题目中给出了一张半截的大白的图片，然后解题过程跟第二道题一样。

10、linux基础1

解题过程跟第7题一样

11、仔细的大象

题目中给出一张图片，然后在图片的属性里面的备注信息里找到一串代码（TVNEUzQ1NkFTRDEyM3p6）这是base64，解码后（ MSDS456ASD123zz ），把图片拖到kali里面，然后binwalk一下，然后会得到一张加密的图片，把解码后的代码打开图片，图片是一张图片，什么都没有，然后用winhex打开，改变图片的高度，flag就在图片上。

12、妹子的陌陌

题目给出一张图片（momo.jpg），图片上有(喜欢我吗.)的字样，把这张图片放到kali里，binwalk一下没出来结果，后来foremost一下，得到一个加密过的TXT文件，然后试了一下图片上的字，结果打开后是（ 嘟嘟嘟嘟

士兵：报告首长！已截获纳粹的加密电报！

首长：拿来看看

电报内容：

..../-/-/.--/---.../-..-./-..-./.-./-.-./---/-../.../.-.-.-/-.-/..../.-/..../..-/---/.-.-.-/-.-./---/--/-..-.

首长：我操你在逗我吗？你确定是他们纳粹发的吗？

士兵：难道我弄错了？哦。。。等等是这一条

内容： http://c.bugku.com/U2FsdGVkX18tI8Yi7FaGiv6jK1SBxKD30eYb52onYe0 =

AES Key：@#@#￥%……￥￥%%……&￥

士兵：二维码真的扫不出来吗？？肯定可以扫出来 ）

从这些东西中可以确定第一个是一个摩斯电码，我没有全解出来，但是可以看出来，所以就从网上找了一个网站（http://www.sojson.com/encrypt_aes.html），第二个是一个AES解码，在上面的网站里，就可以把那段密文解出来，解出来以后是这样（ http://c.bugku.com/momoj2j.png），打开这个网址以后，是一个二维码，然后悲惨的发现扫不出来，然后发现这个二维码的黑色和白色区域反了，然后用StegSolve改变一下颜色，然后用手机扫一下就出来了。

13、宽带信息泄露

题目中给出一个conf.bin文件，主要是工具，用routerpassview打开，然后找到（ <Username val=053700357621 />  <Password val=210265 /> ）题目中给出了提示，flag是宽带用户名。

14、听首音乐

题目给了一个stego100.wav（音频文件），然后Audacity打开，一共有两栏，上面那一栏有一些不规则的小段，把这些小段放大，每一个小段都是有宽窄相间的小段组成，把宽的想象成—，窄的想象成".",然后你就会发现这是摩斯电码（ ..... -... -.-. ----. ..--- ..... -.... ....- ----. -.-. -... ----- .---- ---.. ---.. ..-. ..... ..--- . -.... .---- --... -.. --... ----- ----. ..--- ----. .---- ----. .---- -.-. ）然后翻译出来是（ 5BC925649CB0188F52E617D70929191C ）这就是答案。

15、这么多数据包

根据提示要找getshell流，wireshark打开

先大致浏览一下，不难发现从第104个包开始应该是攻击机（192.168.116.138）在向目标机（192.168.116.159）进行端口扫描

之后可以大致找到攻击机远程连接目标机的包（通过3389端口），以及smb协议的包（用于Web连接和客户端与服务器之间的信息沟通）

再往下可以找到以5542开始的包已经getshell，追踪流可以看到其中有一个s4cr4t.txt的文件，base64解码得到flag（CCTF{do_you_like_sniffer}）

16、图穷匕见

题目给出的是一张图片，用notepad++打开，会发现，后面都是规律的字符串，把前面的乱码都删了。全选这一大段字符串，点击插件-->Converter-->HEX->ASCII。然后这一大串代码就变成了一堆坐标（例如，（7,13）这种形式），写一个程序，把这些点都画出来，就是一个二维码，用手机扫一下，答案就出来了。

17、想蹭网先解开密码

http://blog.csdn.net/helloc0de/article/details/68956222

18、convert（意思是转换）

题目给以一大片儿的01代码，然后把他们转换为16进制，把转换完以后的放到winhex里，左边就显示出了一些字符，这些字符看着像base64，，解码以后答案就出来了。

19、好多压缩包

http://www.cnblogs.com/WangAoBo/p/6951160.html

（17/19都没做出来，链接是网上的大神做的文章，还有一道叫做“就五层，你能解开吗”也没做出来，待更）