

WEEK3 misc

1. 至少像那雪一样

用binwalk先分析一波，发现里面有一个zip文件，于是用winhex打开，手动将zip分离出来。发现zip文件中有一个一样的jpg和一个藏着flag的txt文件，于是想到明文攻击。将无密码的jpg解压成压缩包，和原zip文件构成用ar解密（这里吐槽一波好2345压缩，一直出问题，请教了学长，学长也很无奈，后来换用7z压缩成功开启爆破）。得到了密码，点开txt，发现是空的（ex me?），出题人说可以做，于是硬着头皮把文件放到winhex中，发现很奇怪的现象，只用09 和20 两种字符，百度了一下，对应的ascii码分别是空格和制表符。灵光乍现发现数据是从上到下15行，从左到右16格，想到了ascii解密，于是将09换成0, 20换成1，二进制转ascii码，成功得到了flag。

2. 听听音乐

百度搜索ctf 音乐题，看到了类似的题目，用音乐软件将mp3放入，得到了长波和短波，即为摩斯密码，摩斯密码转换及得到flag