BugKu CTF(杂项篇MISC)—赛博朋克

原创

网络安全研究所 于 2021-02-02 11:13:36 发布 1324 收藏 6
文章标签： 乱码 css html 微软 md5

本文链接：https://blog.csdn.net/zjzqxzhj/article/details/113578023

CTF

BugKu CTF

(杂项篇MISC)

攻与防

赛博朋克

描　　述: flag{}

下载之后是一个压缩包，包含一个txt文本文件 。

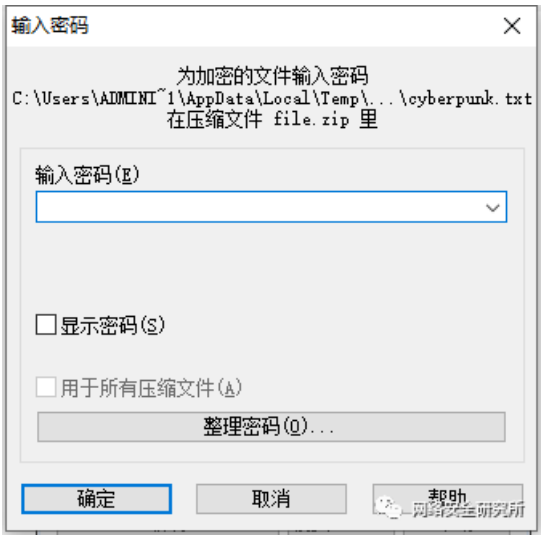
一、工具

十六进制工具 010 editor

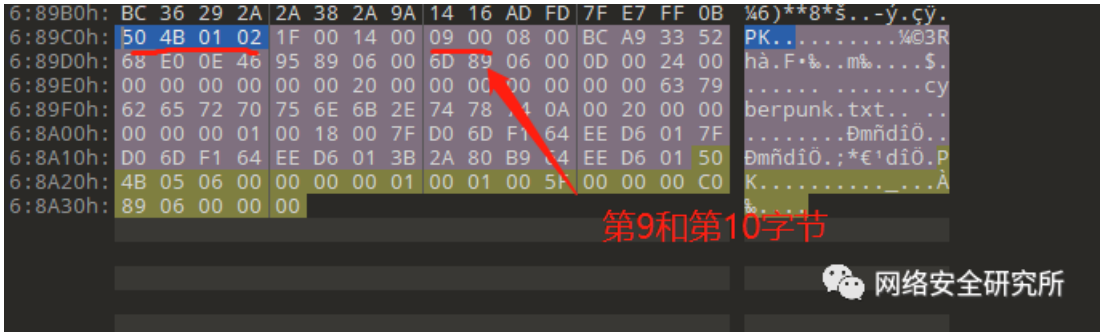
图片分析工具 Stegsolve

二、解题思路

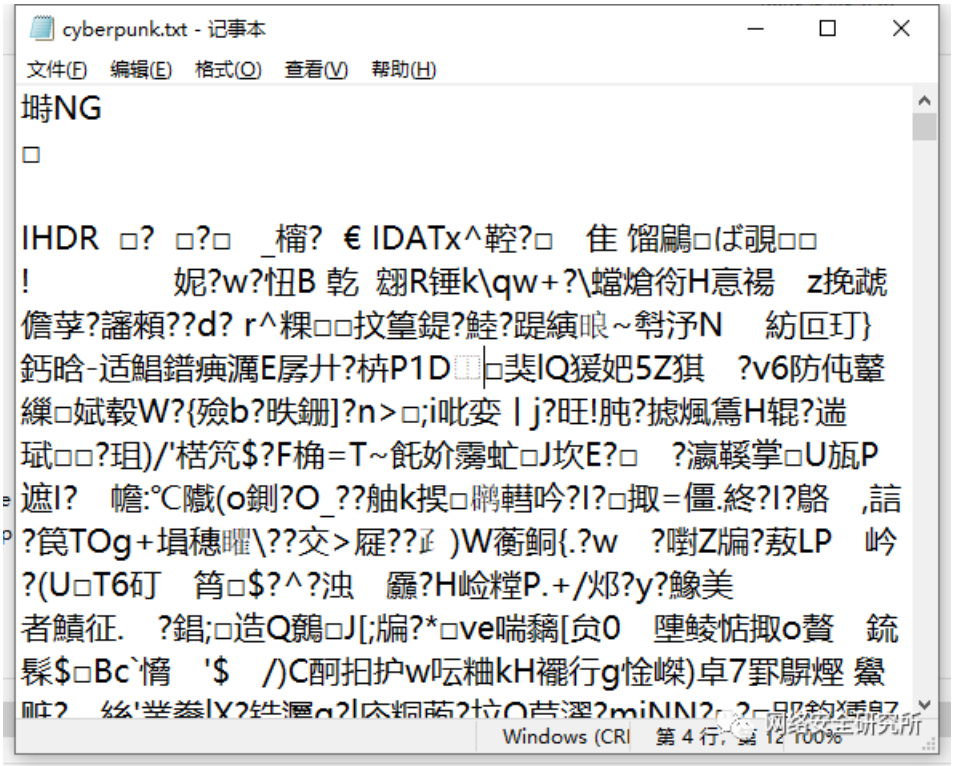
1.先尝试把压缩包解压，提示需要密码。看看压缩包属性也没有发现特殊字段。



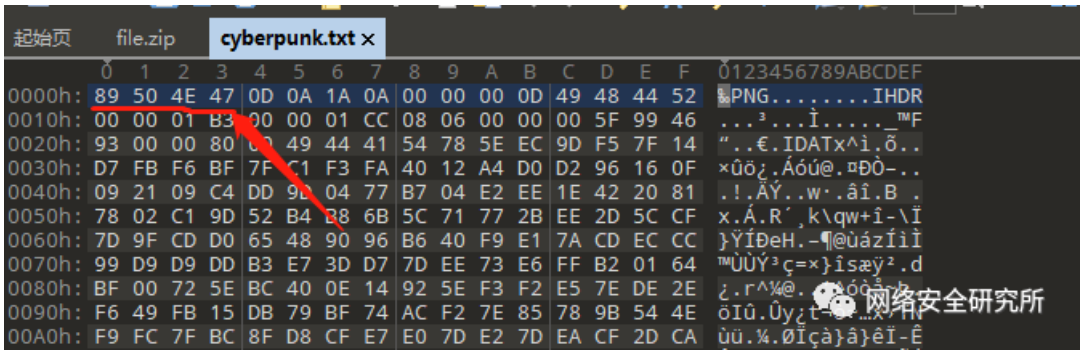
2.考虑有没有可能是zip压缩包的伪加密了。用010 editor编辑器打开看一看。找到从504B0102字节，从50开始算，第9和第10个字节改为0000



3.压缩包可以正常解压了。确实是伪加密。但是打开之后是一堆乱码。发现头部有个NG，猜测可能是png图片。

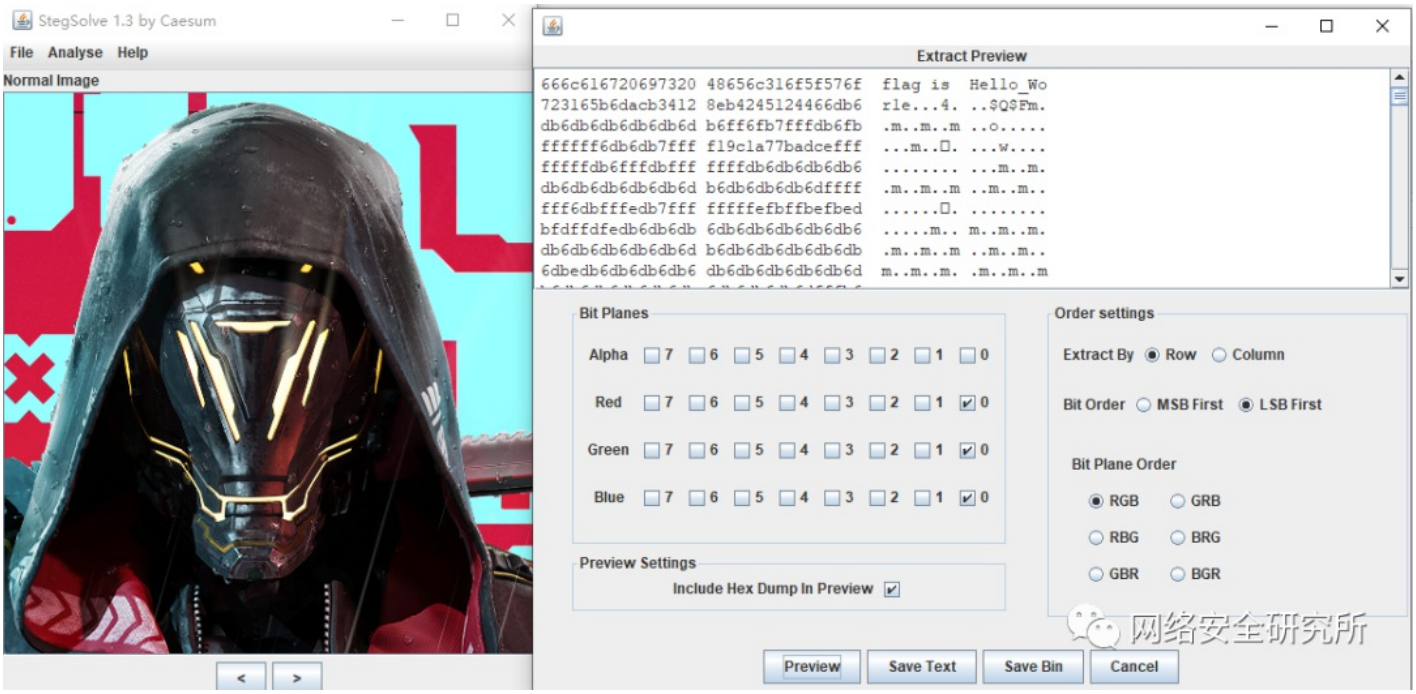


4.用010 editor编辑器打开看看，前面讲过89504E47是PNG文件头标识。这应该是一张图片被改后缀了。因此将txt后缀改为png。



5.打开看到一张图片。用010打开之后未看到报错信息，没有CRC错误之类的。

6.考虑图片隐写，用Stegsolve工具看一看吧。最常见的就是LSB隐写，RGB模式。设置完之后往上翻，发现最上面就是flag了。



3.总结

本题需要掌握010 editor编辑器，zip压缩包文件头和伪加密方式，图片隐写查看器Stegsolve，LSB隐写等。

常用文件的文件头如下(16进制)：

JPEG (jpg)，文件头：FFD8FFE1

PNG (png)，文件头：89504E47

GIF (gif)，文件头：47494638

TIFF (tif)，文件头：49492A00

CAD (dwg)，文件头：41433130

Adobe Photoshop (psd)，文件头：38425053

Rich Text Format (rtf)，文件头：7B5C727466

MS Word/Excel (xls.or.doc)，文件头：D0CF11E0

ZIP Archive (zip)，文件头：504B0304

RAR Archive (rar)，文件头：52617221

END

扫码关注

网络安全研究所

更多精彩等着你