2021年中国工业互联网安全大赛核能行业赛道writeup之隐写

原创

苦行僧(csdn) 于 2021-10-18 23:44:56 发布 47 收藏 1
分类专栏： 信息安全 文章标签： CTF writeup john zip2john

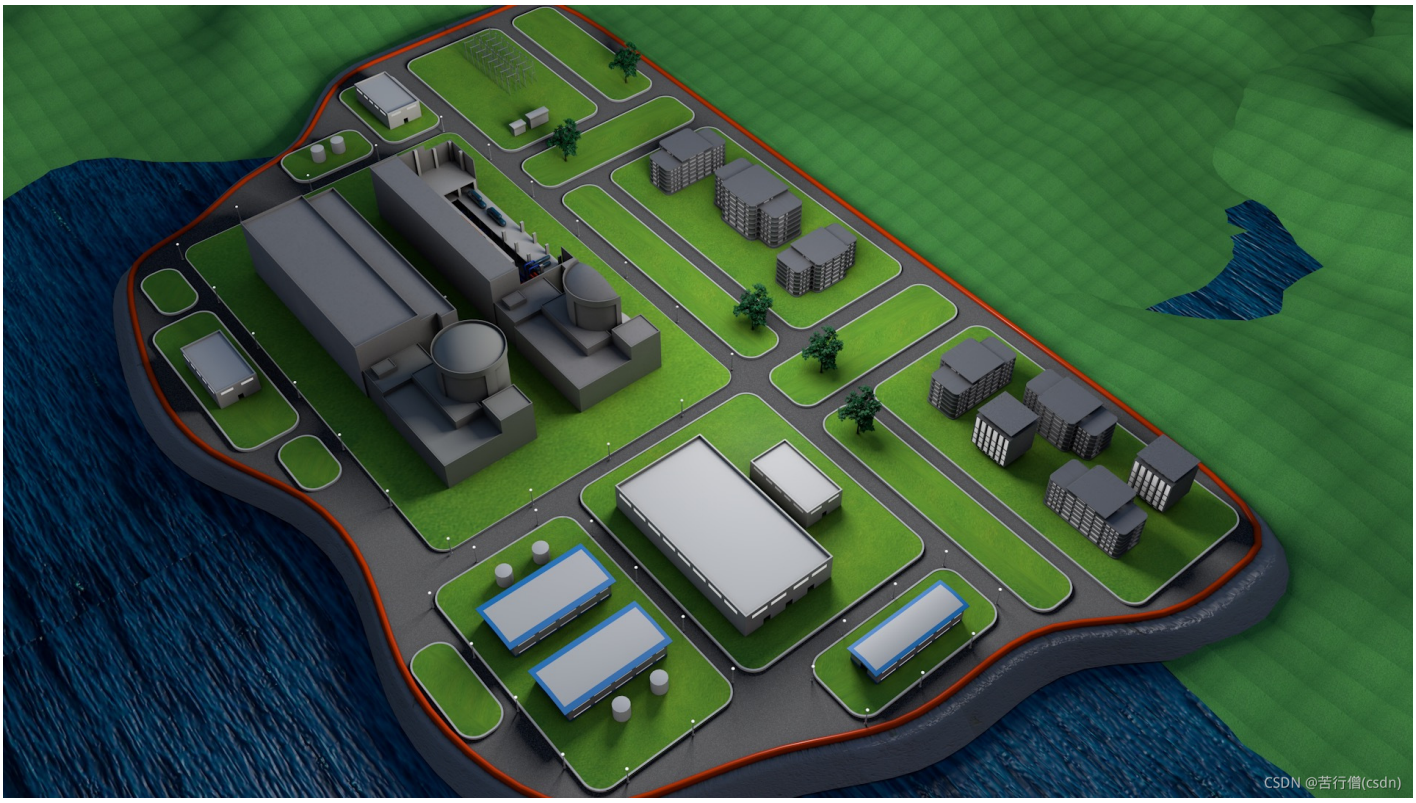
本文链接：https://blog.csdn.net/qpeity/article/details/120819012

附件题：隐写

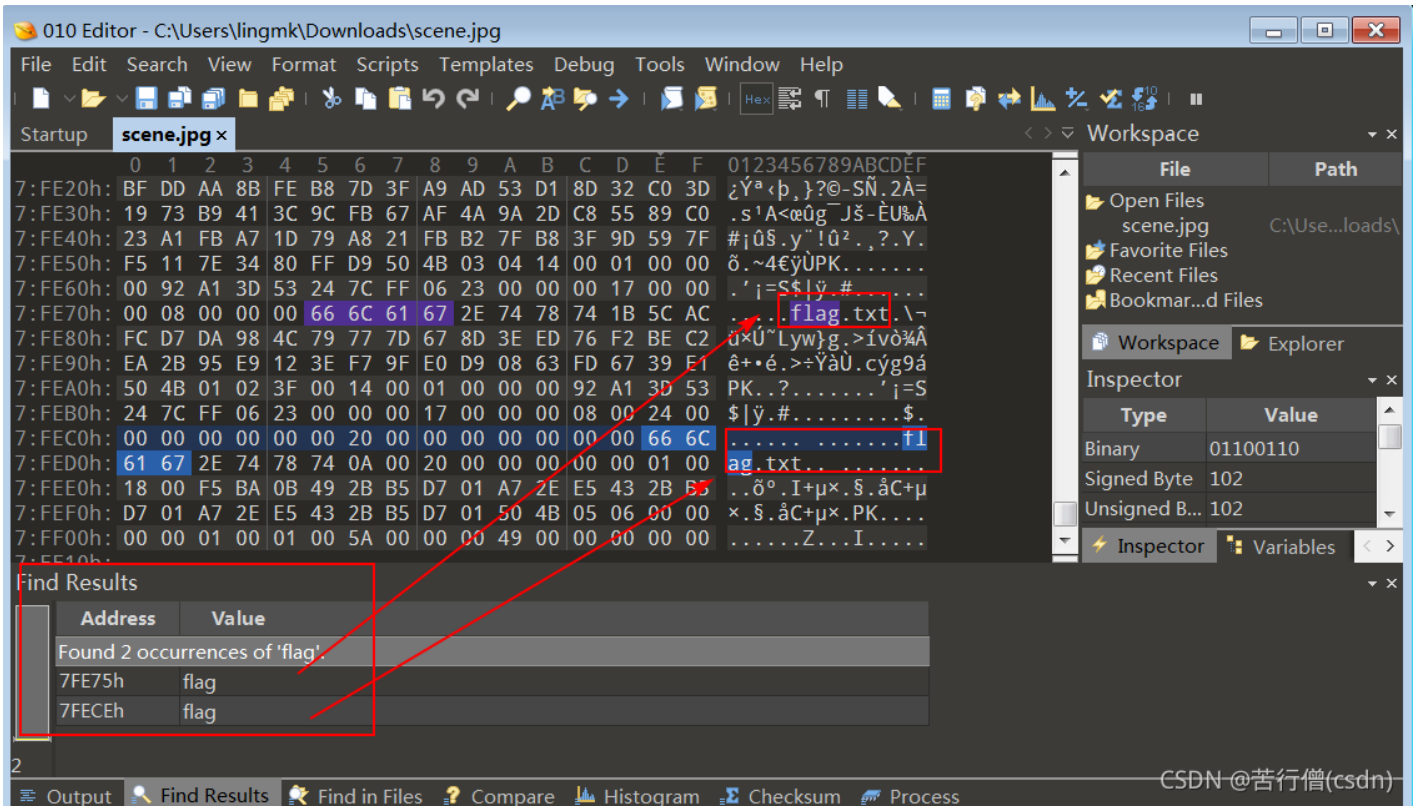
题目描述：隐写

附件下载：

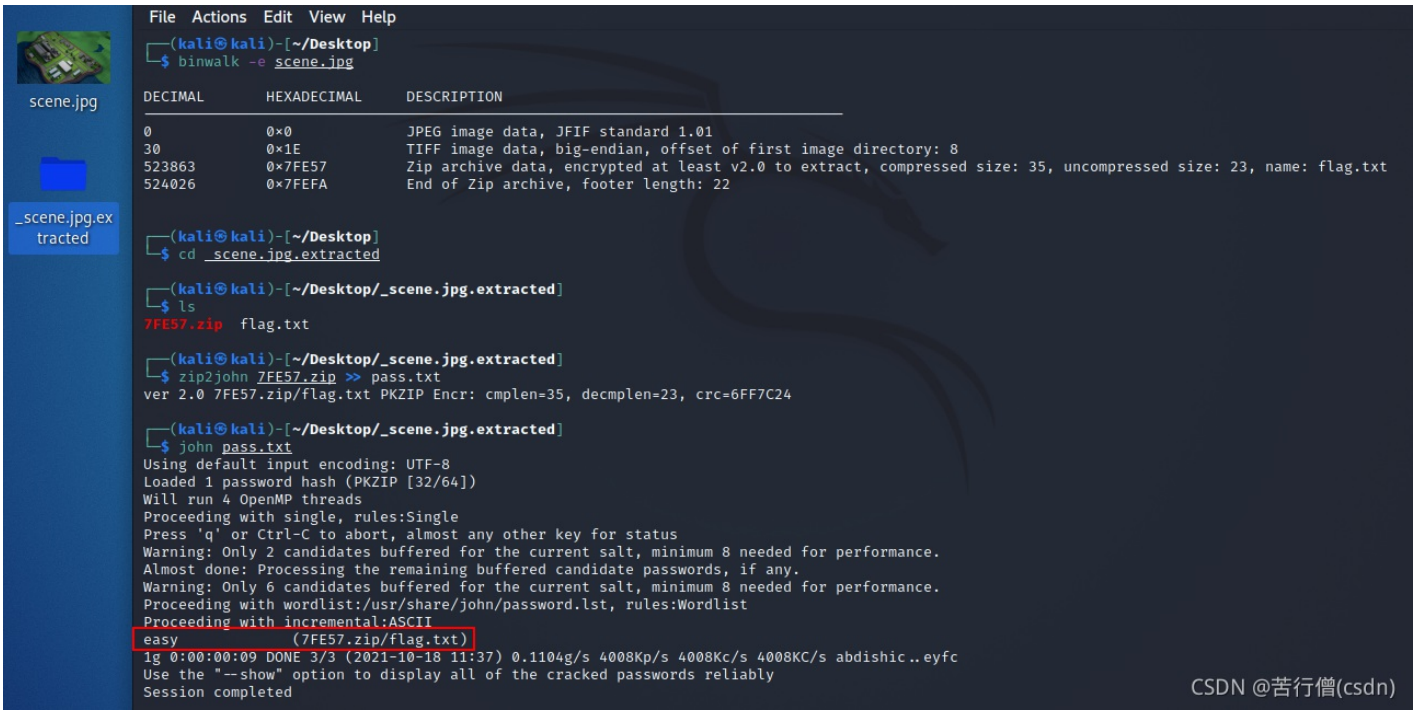
2021-10-12T15_44_19.174914+00_00scene.jpg.zip-网络攻防文档类资源-CSDN下载



先用 010Editor 查看这个图片，能直接看到图片的头部是否完整正常，能直接看到是否隐藏了flag。使用 Stegsolve 逐个图层看，没有发现异常，尝试用 binwalk 搞定。




```
binwalk -e scene.jpg
cd _scene.jpg.extracted
zip2john 7FE57.zip >> pass.txt
john pass.txt
```



发现图片里隐藏的压缩包 7FE57.zip，使用 john 工具暴力破解，发现压缩包的密码是easy。解压缩得到 flag.txt，里面就是 flag{hide_1n@_Picture} 。