2021第一届网刃杯网络安全大赛-藏在s7里的秘密

原创

夜白君 于 2021-09-13 10:40:27 发布 1269 收藏 1

分类专栏： 2021第一届网刃杯网络安全大赛 文章标签： 网络安全 python unctf 网刃杯

本文链接：https://blog.csdn.net/qq_43264813/article/details/120262297

2021第一届网刃杯网络安全大赛 专栏收录该内容

4 篇文章 2 订阅

订阅专栏

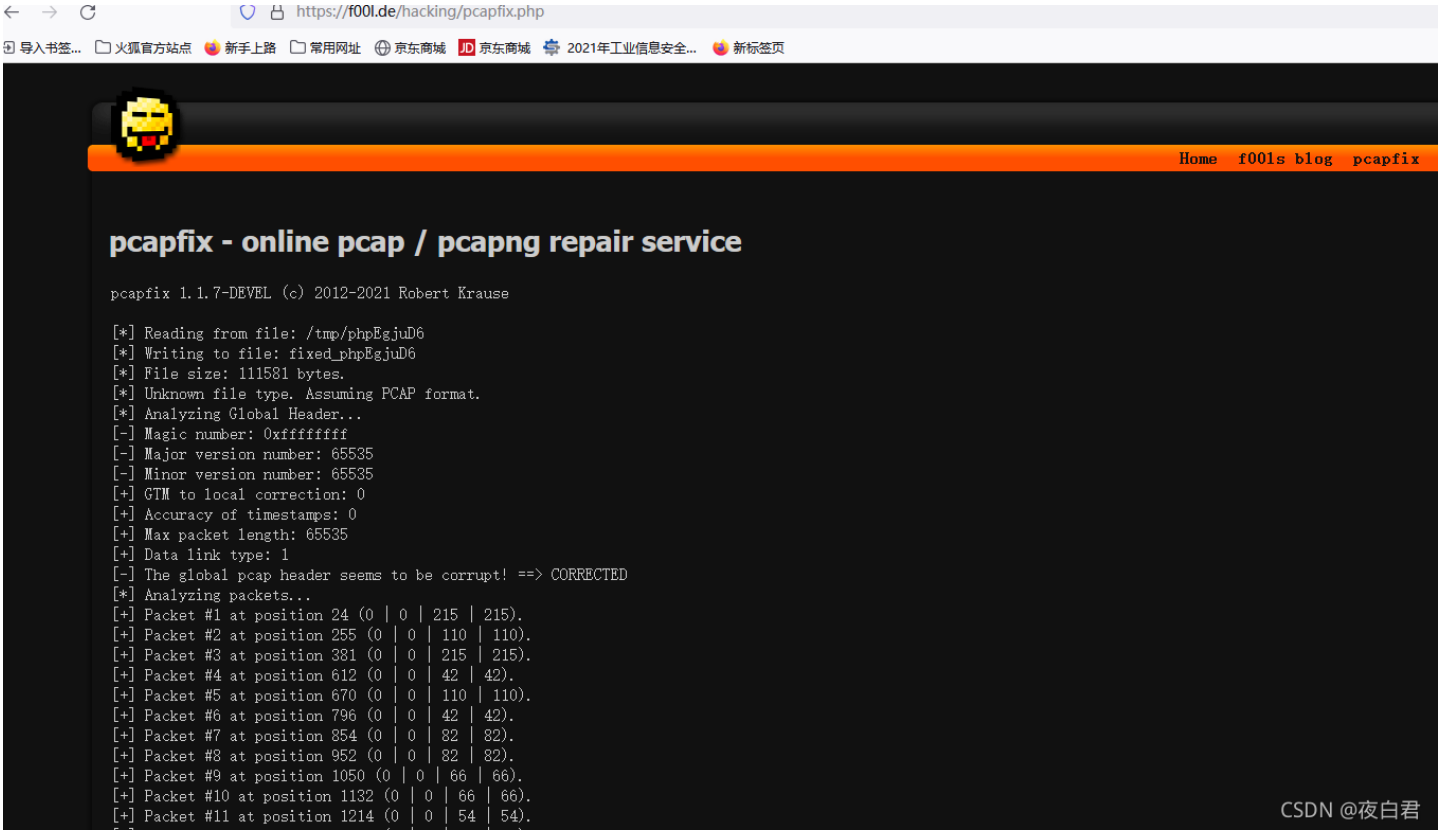
2021第一届网刃杯网络安全大赛-藏在s7里的秘密

难度系数：3.0

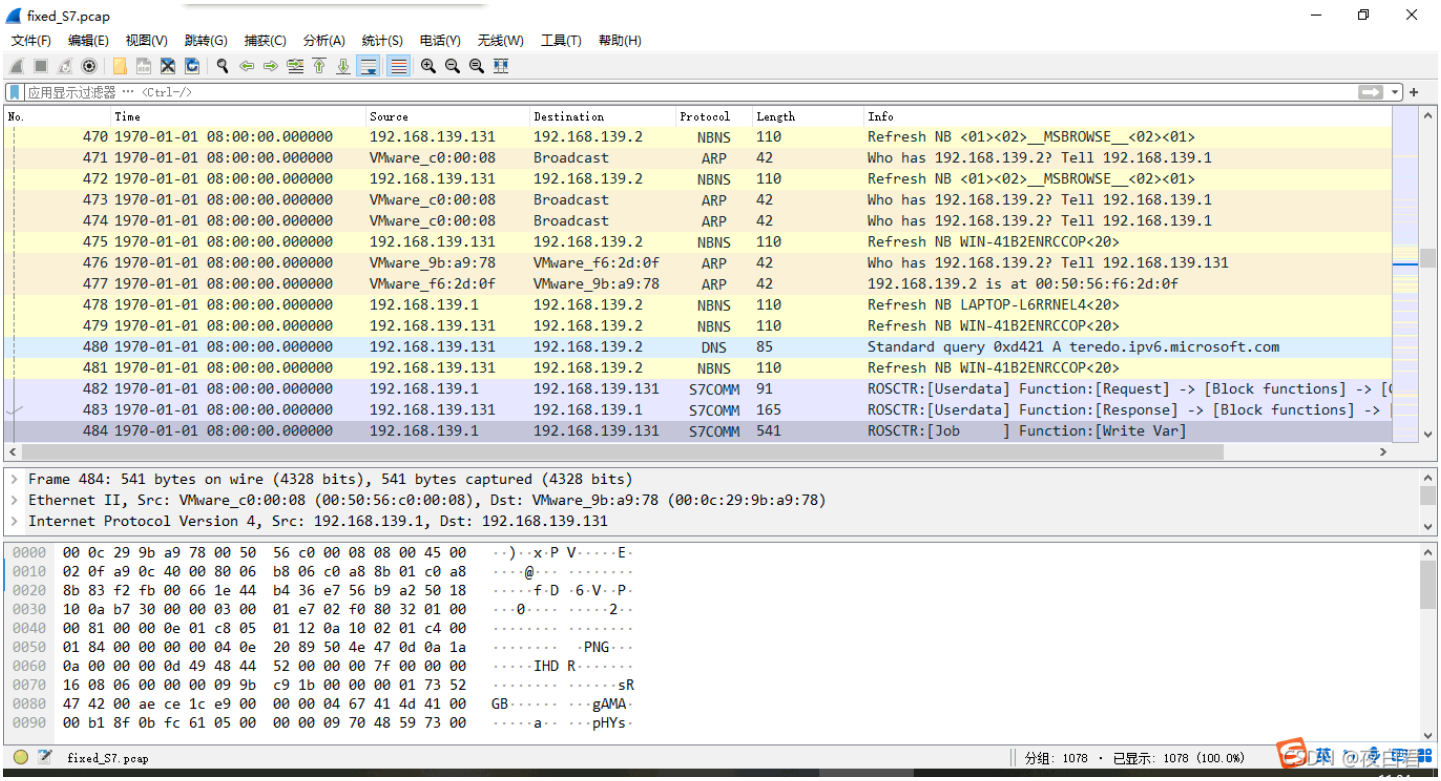
题目描述：某工厂的安全设备捕获了攻击者向PLC中写入恶意数据的数据包，你能分析出并找到其中隐藏的数据吗？

解题思路：

下载查看流量包发现无法打开，尝试对流量包进行修复



分析流量发现存在一个png图



将图片导出并查看发现图片长度缺失，使用010打开发现提升CRC校验有问题，疑是需要爆破图片真实高度，使用网络上的脚本进行爆破

```
import zlib
import struct
import  binascii


file = 'aaaa.png'
fr = open(file,'rb').read()
data = bytearray(fr[12:29])

#crc32key = eval(str(fr[29:33]).replace('\\x','').replace("b'","0x").replace("'",''))
crc32key = struct.unpack('>I',fr[29:33])[0]&0xffffffff
# print(hex(fr[29:33]))
#data = bytearray(b'\x49\x48\x44\x52\x00\x00\x01\xF4\x00\x00\x01\xF1\x08\x06\x00\x00\x00')
n = 4096
for w in range(n):
    width = bytearray(struct.pack('>i', w))
    for h in range(n):
        height = bytearray(struct.pack('>i', h))
        for x in range(4):
            data[x+4] = width[x]
            data[x+8] = height[x]
            #print(data)
        crc32result = zlib.crc32(data)
        if crc32result == crc32key:
            print(crc32key)
            print(width,height)
            print(data)
            newpic = bytearray(fr)
            for x in range(4):
                newpic[x+16] = width[x]
                newpic[x+20] = height[x]
            fw = open(file.split('.')[0]+'_cracked'+'.png','wb')
            fw.write(newpic)
            fw.close
```

将爆破出的高度修改查看拿到flag