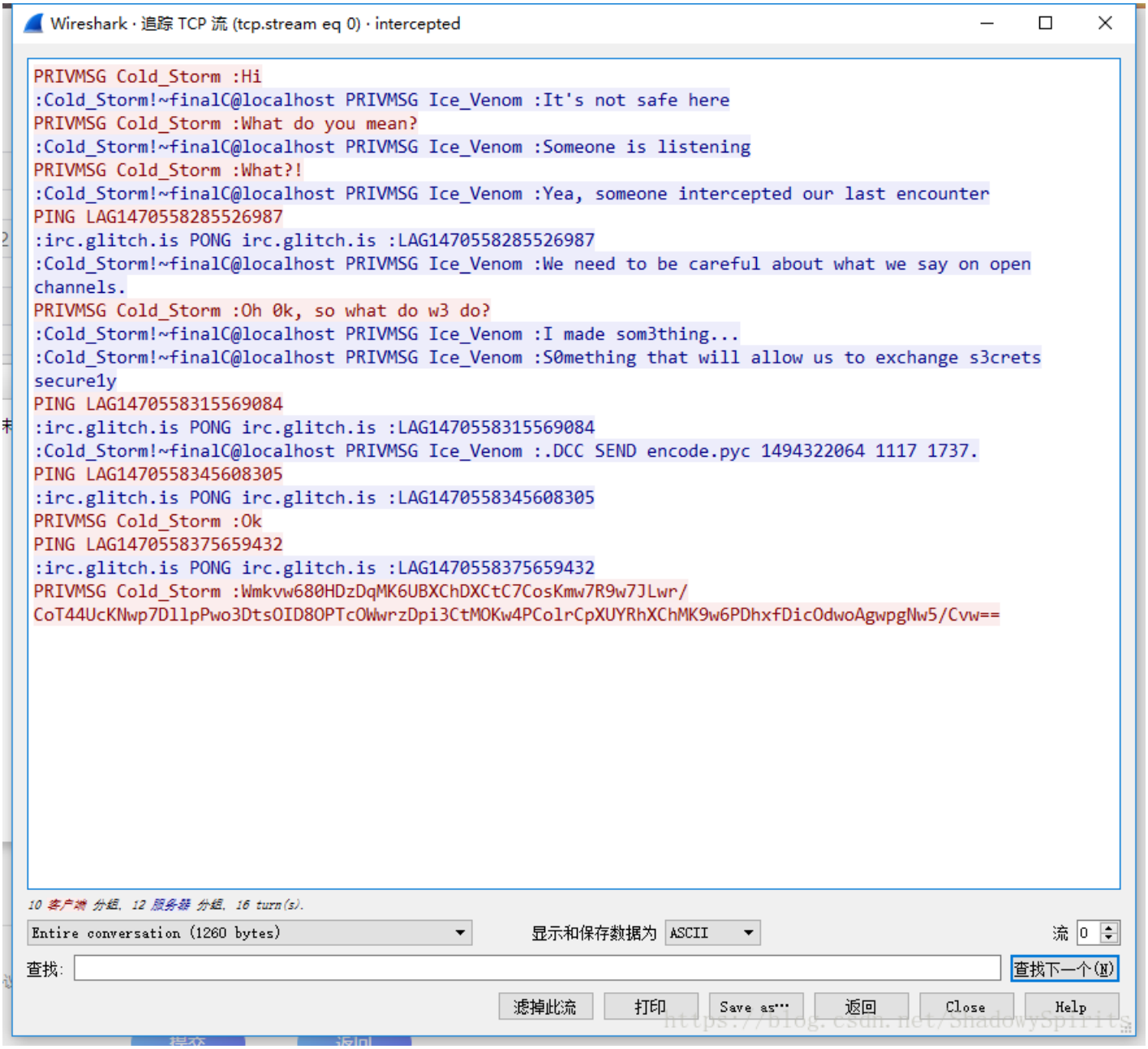
IceCTF - Intercepted Conversations Pt.2 WriteUp

原创

ShadowySpirits 于 2018-09-04 18:33:01 发布 952 收藏

分类专栏： ctf 文章标签： ctf IceCTF i春秋

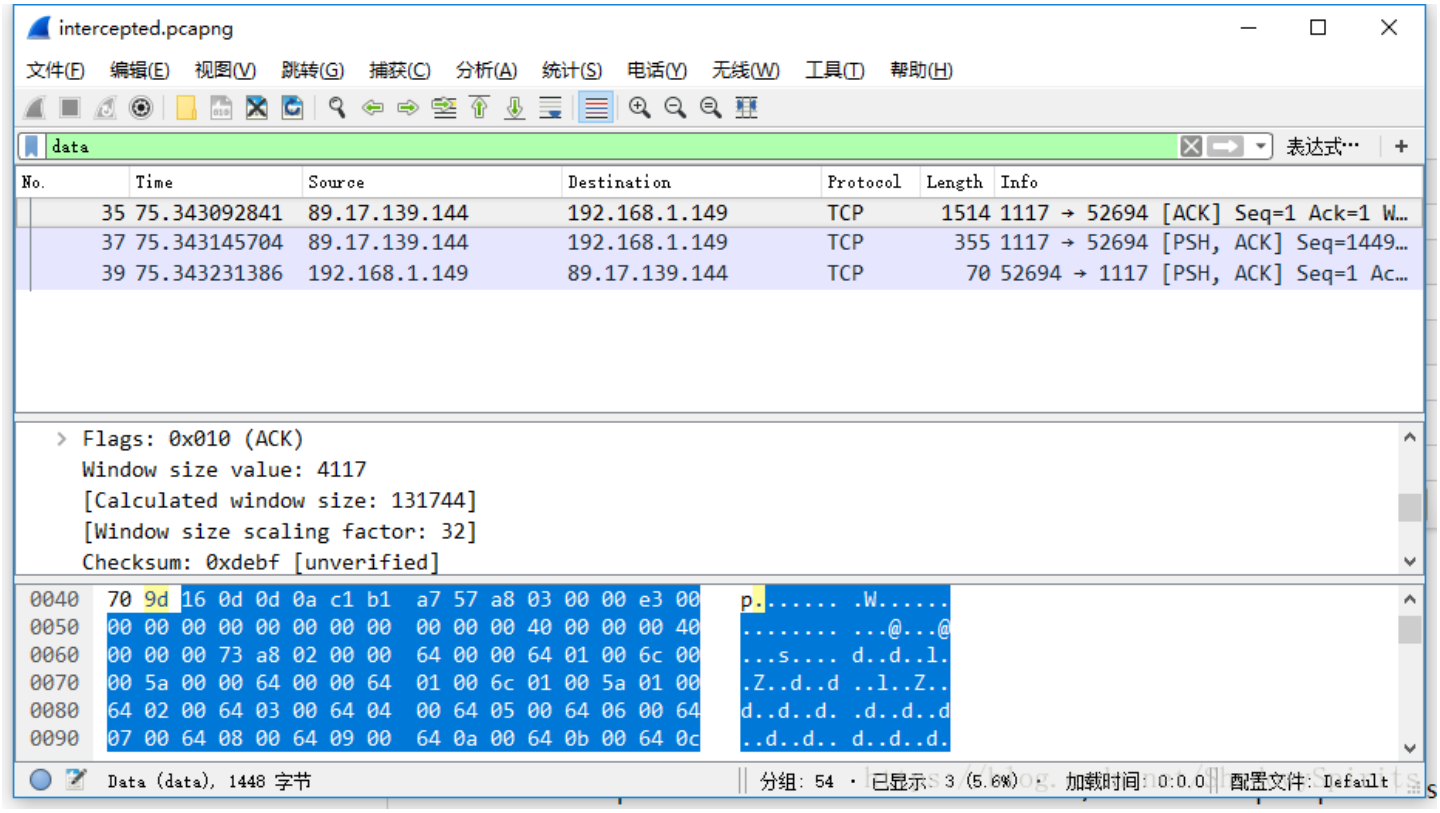
追踪 Protocol 为 IRC 的流，可以得到一段聊天内容



大意是传输了一个 encode.pyc 文件，并用其加密了一段文字,密文如下：
Wmkvw680HDzDqMK6UBXChDXCtC7CosKmw7R9w7JLwr/CoT44UcKNwp7DllpPwo3DtsOID8OPTcOWwrzDpi3CtMOKw4PColrCpXUYRhXChMK9w6PDhxfDicOdwoAgwpgNw5/Cvw==

于是就想办法提取出这个 pyc 文件，pyc 是 python 编译后的文件（pyc pyo 等文件格式的详解：https://blog.csdn.net/willhuo/article/details/49886663 ）

继续检查数据包，在筛选器中筛选 data 可以发现这个包



可以看到它的开头是 16 0d，这是 Python 3.5 编译后的特征码，可以确定这就是我们要找的 encode.pyc（Python 各版本编译后的特征码可以在这查询 https://gist.github.com/delimitry/bad5496b52161449f6de ）

将提取出的 encode.pyc 文件用 uncompyle6 （ https://github.com/rocky/python-uncompyle6 ）反编译如下：

```
# Offsec Research CTF Team
import random, base64, string, sys
P = [27,35,50,11,8,20,44,30,6,1,5,2,33,16,36,64,3,61,54,25,12,21,26,10,57,53,38,56,58,37,43,17,42,47,4,
S = [68,172,225,210,148,172,72,38,208,227,0,240,193,67,122,108,252,57,174,197,83,236,16,226,133,94,104,
#comment these lines if not running under python2
reload(sys)
sys.setdefaultencoding('utf8')
#Get the encoded flag and do the conversions in reverse order
ans = ((base64.b64decode(sys.argv[1])).encode('utf8')).decode('utf8')
#Create a list with length of character in ans (encoded flag)
ans_list = list(ans)
#Create empty inp list
inp = ['' for i in range(len(ans))]
for j in range(0, len(ans), 64):
    for i in range(64):
        #Try every printable ascii character and if the equation is satisfied, we've found one characte
        for c in string.printable:
            if (ans_list[j + P[i] - 1] == unichr(((ord(c) + S[i]) % 256))):
                inp[j + i] = c
inp = ''.join(inp)
print(inp)
```

这里直接给出破解脚本：

```
 import base64
inp = base64.b64decode("Wmkvw680HDzDqMK6UBXChDXCtC7CosKmw7R9w7JLwr/CoT44UcKNwp7DllpPwo3DtsOID8OPTcOWwrz
P = [
27, 35, 50, 11, 8, 20, 44, 30, 6, 1, 5, 2, 33, 16, 36, 64, 3, 61, 54, 25, 12, 21, 26, 10, 57, 53, 38, 5
S = [68, 172, 225, 210, 148, 172, 72, 38, 208, 227, 0, 240, 193, 67, 122, 108, 252, 57, 174, 197, 83, 2

ans = ['' for i in range(len(inp))]
for j in range(0, len(inp), 64):
for i in range(64):
x = ord(inp[j + P[i] - 1]) - S[i]
if x < 0:
x += 256
ans[j + i] = chr(x)

ans = ''.join(ans)
print(ans)
```