


3-1 攻防世界

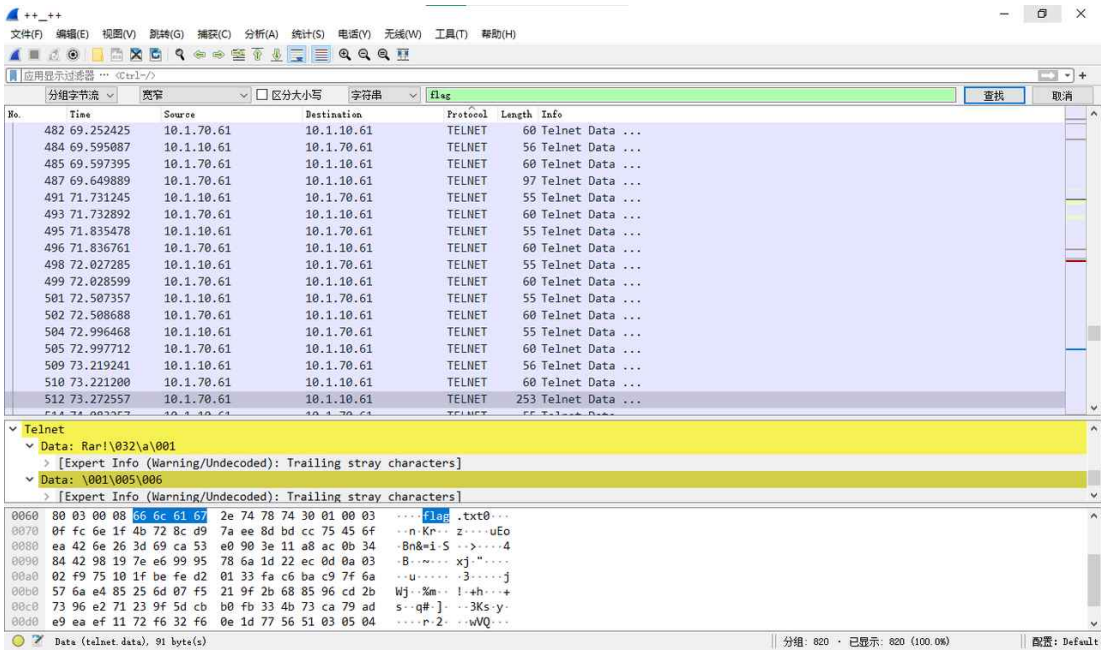
 3分

题目描述

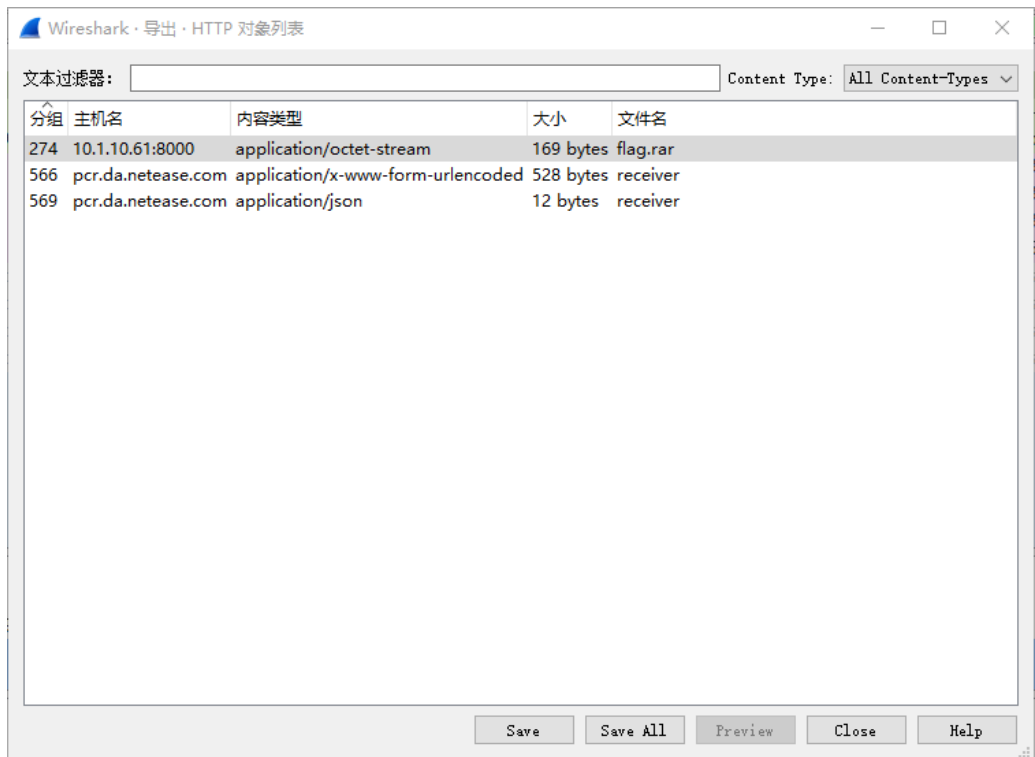
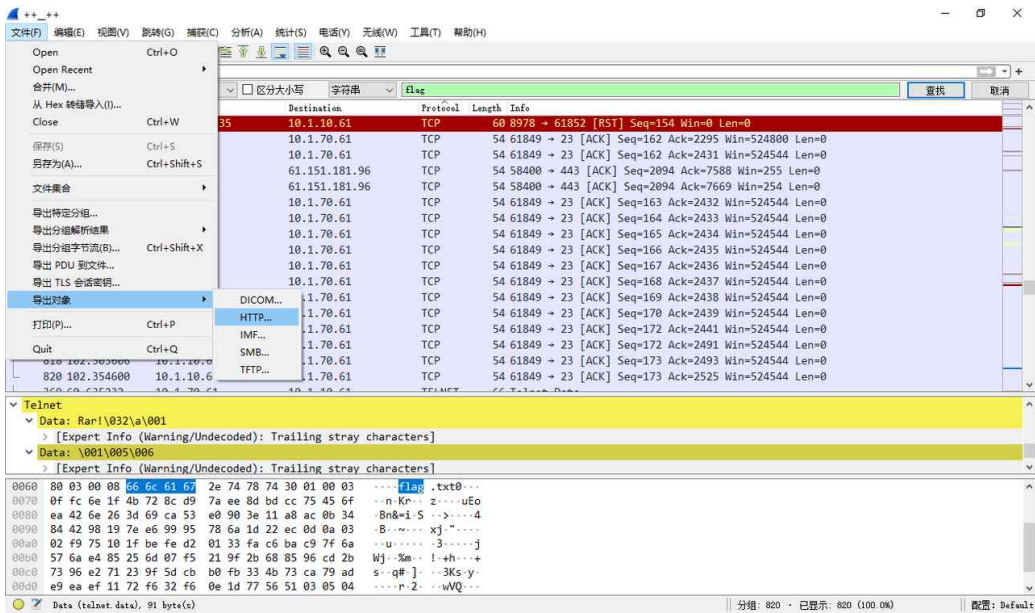
题目给了一个没有后缀的文件

解题

用 010 Editor 查看发现是流量包，用wireshark分析



发现有 flag.rar flag.txt 等文件。导出这几个文件，操作如下：



rar 压缩包解压需要密码。

继续分析，寻找密码，追踪TCP流，重点关注 流6 ，SSH远程访问

```
[root@localhost wireshark]# llss
1 2 3 test
```

wireshark 文件夹下有 1, 2, 3, test 四个文件

test 中文本

```
[root@localhost wireshark]# ccaatt tteesstt  
zhu  
ni  
cheng  
gong
```

1 是一个压缩包，经比对，是 flag.rar

```
[root@localhost wireshark]# ccaatt 11  
Rar!....3...  
.....TU..<.....+......flag.txt0.....n.Kr..z....uEo.Bn&=i.S..>....  
4.B..~...xj..".  
...u.....3.....jWj..%m...!.+h...+s..q#.]...3Ks.y.....r.2...wVQ....
```

2 中也是文本，猜测经过base64编码

```
[root@localhost wireshark]# ccaatt 22  
19aaFYsQQKr+hVX6h12smAUQ5a767TsULEUebWSajEo=[root@localhost wireshark]#  
ppiinn gg bbaaiidduu..ccoomm
```

3 中是一段python代码

```

[root@localhost wireshark]# ccaatt 33

# coding:utf-8
.

.
__author__ = 'YFP'
.

.
from Crypto import Random
.
from Crypto.Cipher import AES
.

.
import sys
.
import base64
.

.
IV = 'QWERTYUIOPASDFGH'
.

.
def decrypt(encrypted):
.
    aes = AES.new(IV, AES.MODE_CBC, IV)
.
    return aes.decrypt(encrypted)
.

.
def encrypt(message):
.
    length = 16
.
    count = len(message)
.
    padding = length - (count % length)
.
    message = message + '\0' * padding
.
    aes = AES.new(IV, AES.MODE_CBC, IV)
.
    return aes.encrypt(message)
.

.
str = 'this is a test'
.

.
example = encrypt(str)
.

.
print(decrypt(example))
.

.

```

最终可以通过提供的python程序拿到密码

Python

```
1  # coding:utf-8
2  from Crypto import Random
3  from Crypto.Cipher import AES
4
5  import sys
6  import base64
7
8  IV = 'QWERTYUIOPASDFGH'
9  def decrypt(encrypted):
10     aes = AES.new(IV, AES.MODE_CBC, IV)
11     return aes.decrypt(encrypted)
12
13  def encrypt(message):
14     length = 16
15     count = len(message)
16     padding = length - (count % length)
17
18     message = message + '\0' * padding
19
20     aes = AES.new(IV, AES.MODE_CBC, IV)
21
22     return aes.encrypt(message)
23
24
25
26  # str = 'this is a test'
27
28
29  # example = encrypt(str)
30  example = "19aaFYsQQKr+hVX6hl2smAUQ5a767TsULEUebWSajEo="
31
32  print(decrypt(base64.b64decode(example)))
```

解压即可得到flag