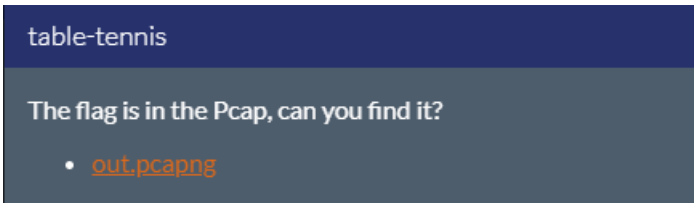
BSidesSF 2019 部分writeup

原创

TuudOp 于 2019-03-06 19:26:05 发布 2092 收藏
分类专栏： ctf 文章标签： BSidesSF 2019

forensics：

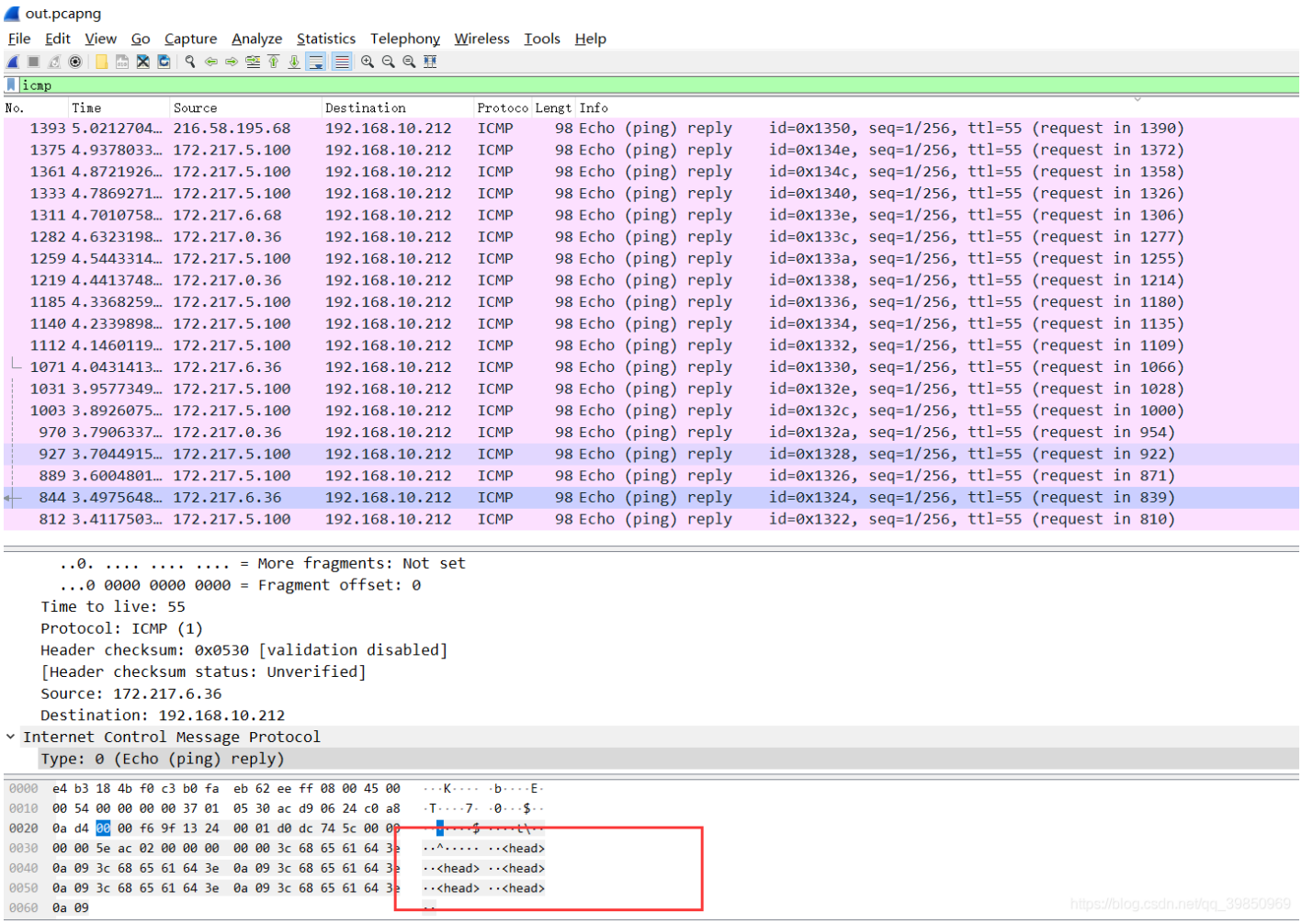
table-tennis



给了一个流量包，使用wireshark打开，通过查找字符串和跟踪TCP数据流并没有发现什么，以我的水平，基本上到这里就结束了。

后面查看了其他人写的writeup，跟着复现了一下。

这个流量包中除了大量的加密的TLS和TCP数据流，还有一些ICMP数据包，发现里面有HTML数据。



这里要将这些HTML数据提取出来，照着大佬使用python scapy模块写的脚本提取数据，我也依样画瓢谢了一下并且理解了脚本的意思，脚本比较简单：

```
from scapy.all import *

packets = rdpcap('out.pcapng')    #rdpcap()读取pcapng文件

for packet in packets:            #遍历每一个数据包
    if packet.haslayer(ICMP):            #haslayer()判断数据包的类型，此处为ICMP
        if packet[ICMP].type == 0:       #每一个ICMP的type值为0的包
            print packet[ICMP].load[-8:],      #打印每个数据包的最后8位，因为前面数据是重复的
```

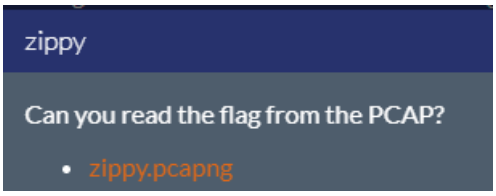
提取出来的数据：

```
root@kali:~/桌面# python pcap.py
<html>
        <head>
        <title>  I <3 Cor gi </tit le>
           <s cript>
d ocument. write(at ob('Q1RG e0p1c3RB UzBuZ0Fi MHV0UDFu Z1Awbmd9 '));
           < /script>

        </hea d>

        <bo dy>

           < h1> Woof !! </h1>

        </bod y>

</ht
```

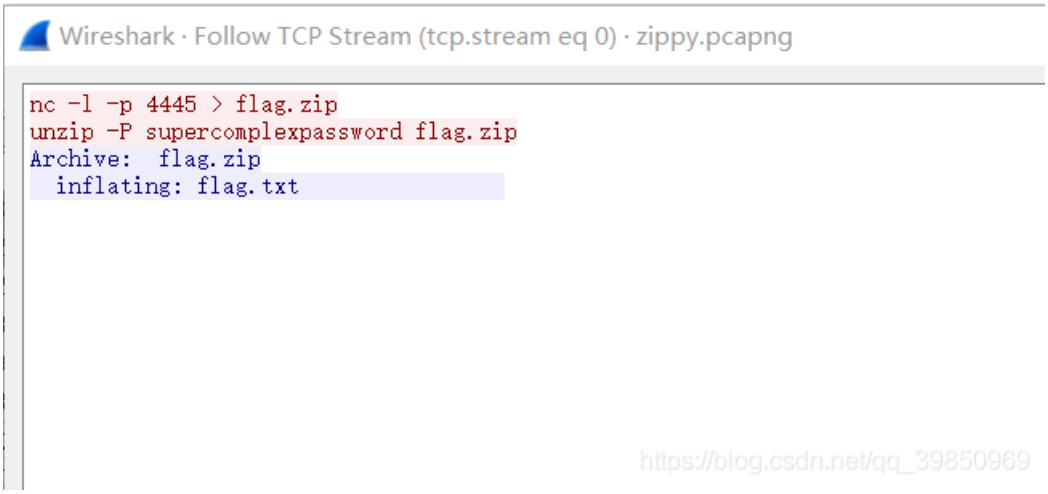

将这段base64加密的数据空格合并 并解密：

```
root@kali:~/桌面# echo Q1RGe0p1c3RBUzBuZ0FiMHV0UDFuZ1Awbmd9 | base64 -d
CTF{JustAS0ngAb0utP1ngP0ng}root@kali:~/桌面#
```

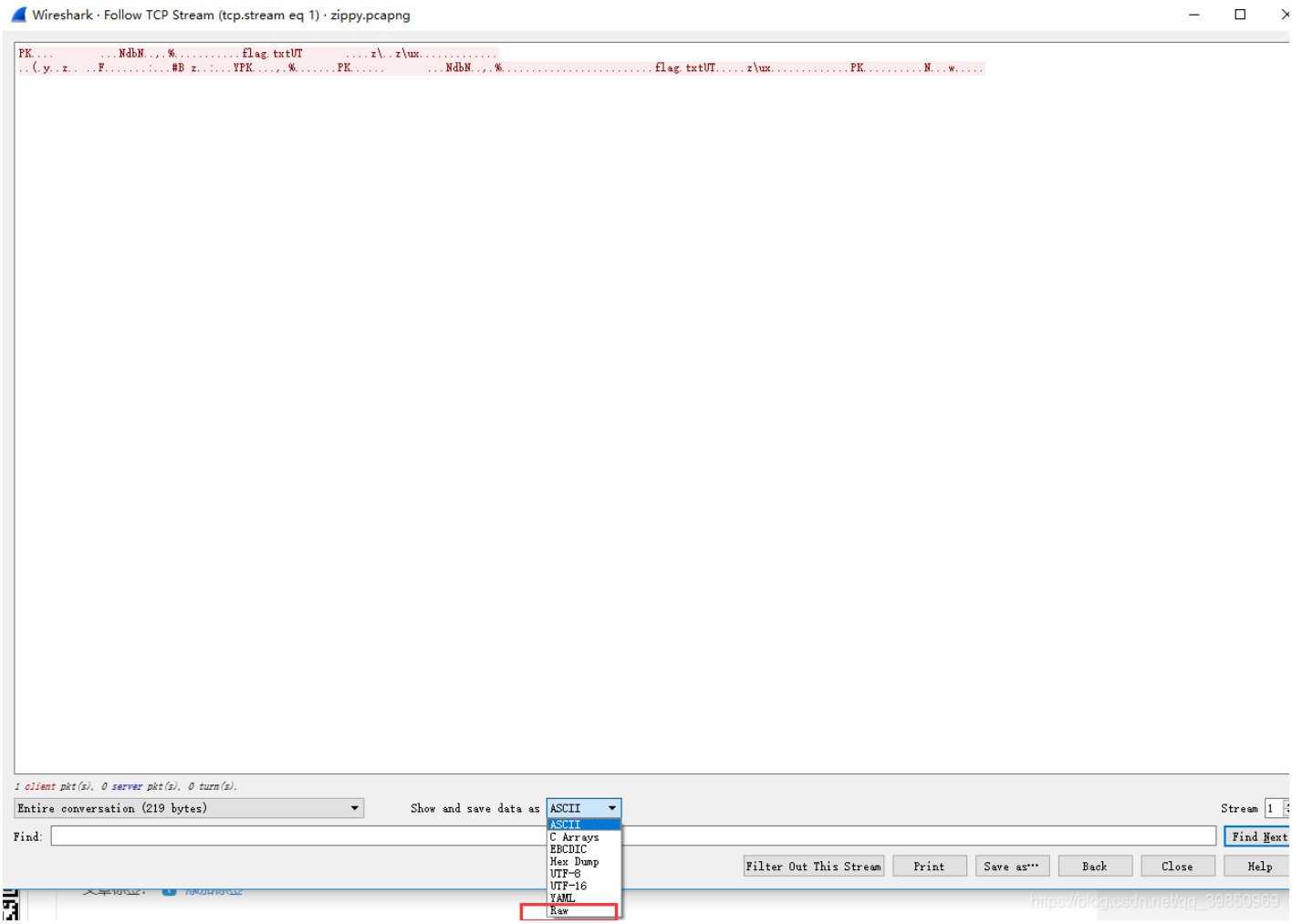
Zippy



也是给了一个pcapng文件，打开之后，跟踪一个TCP数据流



应该是正在发送一个加了密的zip文件，找到这个加密文件的数据流



然后以原始数据保存为zip文件

使用密码解压就可以得到flag

```
root@kali:~/桌面# unzip -P supercomplexpassword flag.zip
Archive:  flag.zip
  inflating: flag.txt
```

```
root@kali:~/桌面# cat flag.txt
CTF{this_flag_is_your_flag}
```

SlashSlash

给了一个flag.zip文件，解压得到flag.aes128cbc文件，同时还有一个字符串，应该是密码

```
root@kali:~/桌面# unzip flag.zip
Archive:  flag.zip
SevenPinLock0123456
 extracting: flag.aes128cbc
```

使用 openssl 即可解密

```
openssl enc -d -aes-128-cbc -pass pass:SevenPinLock0123456 -in flag.aes128cbc
```

```
root@kali:~/桌面# openssl enc -d -aes-128-cbc -pass pass:SevenPinLock0123456 -in flag.aes128cbc
CTF{always_add_comments}
root@kali:~/桌面# openssl enc -d -aes-128-cbc -in flag.aes128cbc
enter aes-128-cbc decryption password:
CTF{always_add_comments}
```