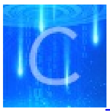
CG-CTF Misc Writeup--Remove Boyfriend

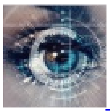
原创

周无争 于 2018-04-17 17:12:17 发布 1438 收藏
分类专栏： CTF # MISC

本文链接：https://blog.csdn.net/hamletal/article/details/79975951
版权



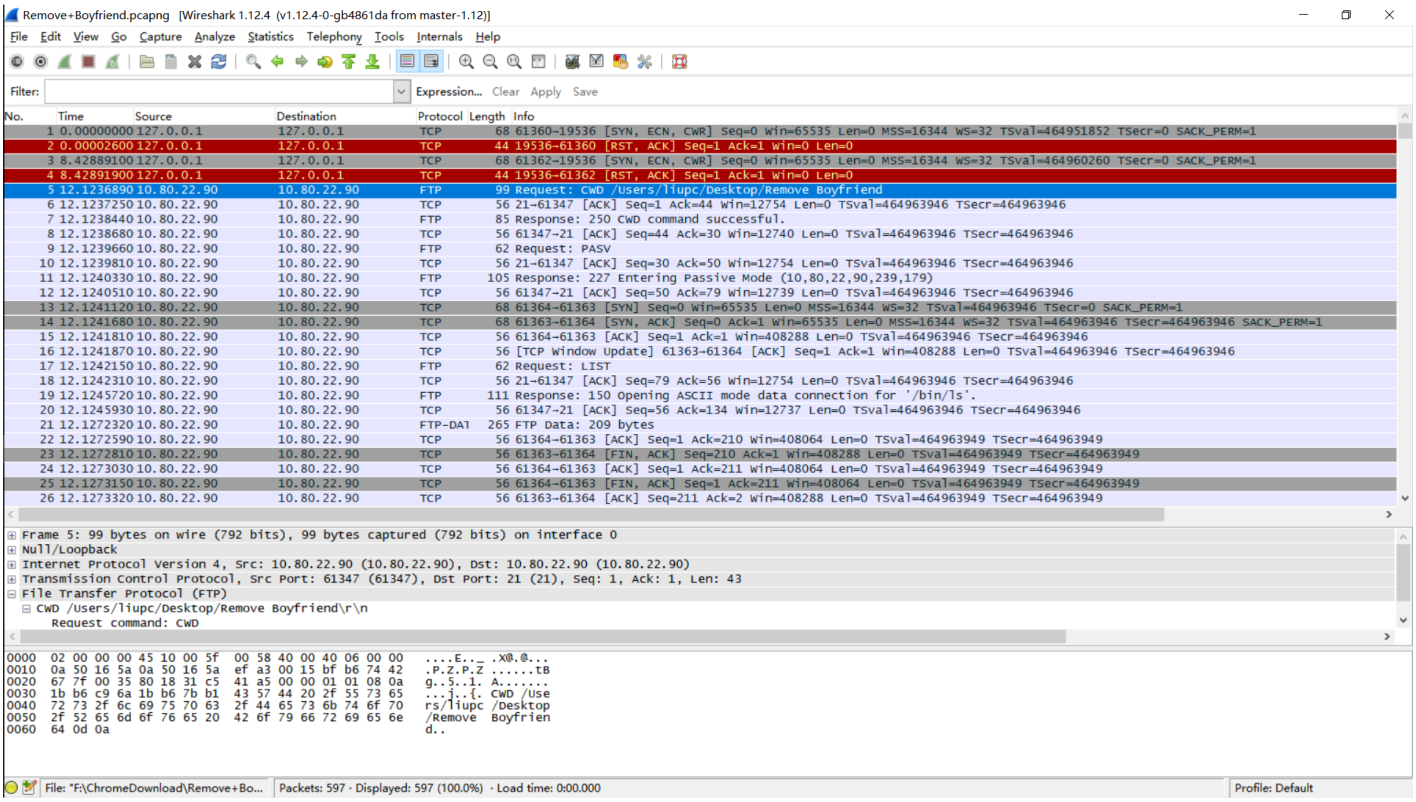
CTF 同时被 2 个专栏收录
1 篇文章 0 订阅
订阅专栏



MISC
1 篇文章 0 订阅
订阅专栏

最近在刷题，发现这道题竟然没有writeup，只好硬磕。好在出题人比较厚道，没有挖更多的坑，最后解决后还是很有成就感的（小白在进步）。

按照题目下载网盘文件：Remove+Boyfriend.pcapng。用wireshark打开，是这样的：



Remove+Boyfriend.pcapng [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time       Source       Destination  Protocol Length Info
   1 0.00000000 127.0.0.1    127.0.0.1    TCP        68 61360→19536 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=16344 WS=32 TSval=464951852 TSecr=0 SACK_PERM=1
   2 0.00002600 127.0.0.1    127.0.0.1    TCP        44 19536→61360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   3 8.42889100 127.0.0.1    127.0.0.1    TCP        68 61362→19536 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=16344 WS=32 TSval=464960260 TSecr=0 SACK_PERM=1
   4 8.42891900 127.0.0.1    127.0.0.1    TCP        44 19536→61362 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   5 12.1236890 10.80.22.90  10.80.22.90  FTP        99 Request: CWD /Users/liupc/Desktop/Remove Boyfriend
   6 12.1237250 10.80.22.90  10.80.22.90  TCP        56 21→61347 [ACK] Seq=1 Ack=44 Win=12754 Len=0 TSval=464963946 TSecr=464963946
   7 12.1238440 10.80.22.90  10.80.22.90  FTP        85 Response: 250 CWD command successful.
   8 12.1238680 10.80.22.90  10.80.22.90  TCP        56 61347→21 [ACK] Seq=44 Ack=30 Win=12740 Len=0 TSval=464963946 TSecr=464963946
   9 12.1239660 10.80.22.90  10.80.22.90  FTP        62 Request: PASV
  10 12.1239810 10.80.22.90  10.80.22.90  TCP        56 21→61347 [ACK] Seq=30 Ack=50 Win=12754 Len=0 TSval=464963946 TSecr=464963946
  11 12.1240330 10.80.22.90  10.80.22.90  FTP       105 Response: 227 Entering Passive Mode (10,80,22,90,239,179)
  12 12.1240510 10.80.22.90  10.80.22.90  TCP        56 61347→21 [ACK] Seq=50 Ack=79 Win=12739 Len=0 TSval=464963946 TSecr=464963946
  13 12.1241120 10.80.22.90  10.80.22.90  TCP        68 61364→61363 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=32 TSval=464963946 TSecr=0 SACK_PERM=1
  14 12.1241680 10.80.22.90  10.80.22.90  TCP        68 61363→61364 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=32 TSval=464963946 TSecr=464963946 SACK_PERM=1
  15 12.1241810 10.80.22.90  10.80.22.90  TCP        56 61364→61363 [ACK] Seq=1 Ack=1 Win=408288 Len=0 TSval=464963946 TSecr=464963946
  16 12.1241870 10.80.22.90  10.80.22.90  TCP        56 [TCP Window Update] 61363→61364 [ACK] Seq=1 Ack=1 Win=408288 Len=0 TSval=464963946 TSecr=464963946
  17 12.1242150 10.80.22.90  10.80.22.90  FTP        62 Request: LIST
  18 12.1242310 10.80.22.90  10.80.22.90  TCP        56 21→61347 [ACK] Seq=79 Ack=56 Win=12754 Len=0 TSval=464963946 TSecr=464963946
  19 12.1245720 10.80.22.90  10.80.22.90  FTP       111 Response: 150 Opening ASCII mode data connection for '/bin/ls'.
  20 12.1245930 10.80.22.90  10.80.22.90  TCP        56 61347→21 [ACK] Seq=56 Ack=134 Win=12737 Len=0 TSval=464963946 TSecr=464963946
  21 12.1272320 10.80.22.90  10.80.22.90  FTP-DAT   265 FTP Data: 209 bytes
  22 12.1272590 10.80.22.90  10.80.22.90  TCP        56 61364→61363 [ACK] Seq=1 Ack=210 Win=408064 Len=0 TSval=464963949 TSecr=464963949
  23 12.1272810 10.80.22.90  10.80.22.90  TCP        56 61363→61364 [FIN, ACK] Seq=210 Ack=1 Win=408288 Len=0 TSval=464963949 TSecr=464963949
  24 12.1273030 10.80.22.90  10.80.22.90  TCP        56 61364→61363 [ACK] Seq=1 Ack=211 Win=408064 Len=0 TSval=464963949 TSecr=464963949
  25 12.1273150 10.80.22.90  10.80.22.90  TCP        56 61364→61363 [FIN, ACK] Seq=1 Ack=211 Win=408064 Len=0 TSval=464963949 TSecr=464963949
  26 12.1273320 10.80.22.90  10.80.22.90  TCP        56 61363→61364 [ACK] Seq=211 Ack=2 Win=408288 Len=0 TSval=464963949 TSecr=464963949
```

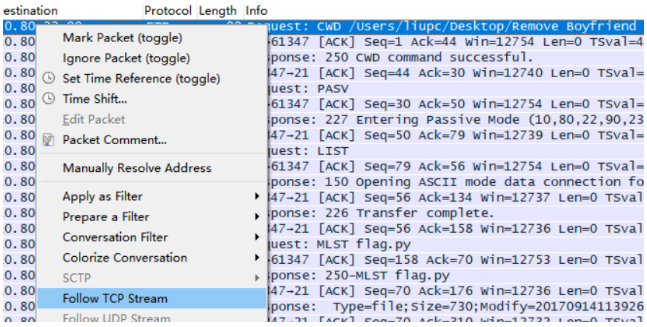
```
⊞ Frame 5: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface 0
⊞ Null/Loopback
⊞ Internet Protocol Version 4, Src: 10.80.22.90 (10.80.22.90), Dst: 10.80.22.90 (10.80.22.90)
⊞ Transmission Control Protocol, Src Port: 61347 (61347), Dst Port: 21 (21), Seq: 1, Ack: 1, Len: 43
⊟ File Transfer Protocol (FTP)
  ⊟ CWD /Users/liupc/Desktop/Remove Boyfriend\r\n
      Request command: CWD
```

```
0000  02 00 00 00 45 10 00 5f  00 58 40 00 40 06 00 00   ....E.._ .X@.@...
0010  0a 50 16 5a 0a 50 16 5a  ef a3 00 15 bf b6 74 42   .P.Z.P.Z ......tB
0020  67 7f 00 35 80 18 31 c5  41 a5 00 00 01 01 08 0a   g..5..1. A.......
0030  1b b6 c9 6a 1b b6 7b b1  43 57 44 20 2f 55 73 65   ...j..{. CWD /Use
0040  72 73 2f 6c 69 75 70 63  2f 44 65 73 6b 74 6f 70   rs/liupc /Desktop
0050  2f 52 65 6d 6f 76 65 20  42 6f 79 66 72 69 65 6e   /Remove  Boyfrien
0060  64 0d 0a                                           d..
```

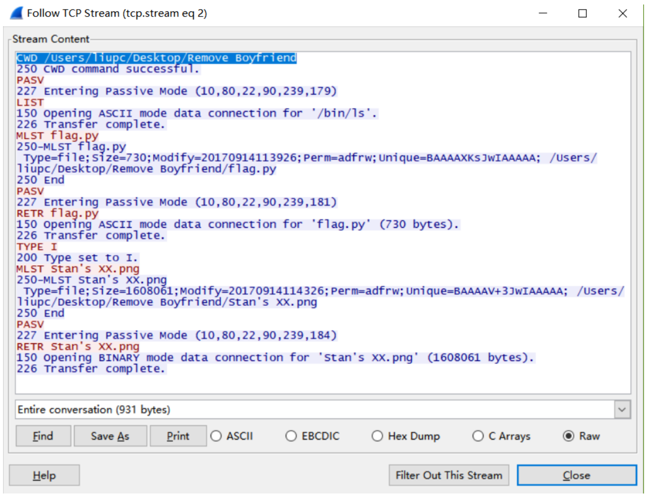
File: "F:\ChromeDownload\Remove+Bo... Packets: 597 · Displayed: 597 (100.0%) · Load time: 0:00.000 Profile: Default

可能会有点乱，从头开始看，第5行有条操作命令：CWD /Users/liupc/Desktop/Remove Boyfriend

CWD是Raw FTP commands，右击--Follow TCP Stream，得到一个命令列表：



```
estination          Protocol Length  Info
0.80                             uest: CWD /Users/liupc/Desktop/Remove Boyfriend
0.80                             61347 [ACK] Seq=1 Ack=44 Win=12754 Len=0 TSval=4
0.80                             ponse: 250 CWD command successful.
0.80                             47→21 [ACK] Seq=44 Ack=30 Win=12740 Len=0 TSval=
0.80                             uest: PASV
0.80                             61347 [ACK] Seq=30 Ack=50 Win=12754 Len=0 TSval=
0.80                             ponse: 227 Entering Passive Mode (10,80,22,90,23
0.80                             47→21 [ACK] Seq=50 Ack=79 Win=12739 Len=0 TSval=
0.80                             uest: LIST
0.80                             61347 [ACK] Seq=79 Ack=56 Win=12754 Len=0 TSval=
0.80                             ponse: 150 Opening ASCII mode data connection fo
0.80                             47→21 [ACK] Seq=56 Ack=134 Win=12737 Len=0 TSval
0.80                             ponse: 226 Transfer complete.
0.80                             47→21 [ACK] Seq=56 Ack=158 Win=12736 Len=0 TSval
0.80                             uest: MLST flag.py
0.80                             61347 [ACK] Seq=158 Ack=70 Win=12753 Len=0 TSval
0.80                             ponse: 250-MLST flag.py
0.80                             47→21 [ACK] Seq=70 Ack=176 Win=12736 Len=0 TSval
0.80                             ponse:  Type=file;Size=730;Modify=20170914113926
```



```
CWD /Users/liupc/Desktop/Remove Boyfriend
250 CWD command successful.
PASV
227 Entering Passive Mode (10,80,22,90,239,179)
LIST
150 Opening ASCII mode data connection for '/bin/ls'.
226 Transfer complete.
MLST flag.py
250-MLST flag.py
 Type=file;Size=730;Modify=20170914113926;Perm=adfrw;Unique=BAAAAXKsJwIAAAAA; /Users/
liupc/Desktop/Remove Boyfriend/flag.py
250 End
PASV
227 Entering Passive Mode (10,80,22,90,239,181)
RETR flag.py
150 Opening ASCII mode data connection for 'flag.py' (730 bytes).
226 Transfer complete.
TYPE I
200 Type set to I.
MLST Stan's XX.png
250-MLST Stan's XX.png
 Type=file;Size=1608061;Modify=20170914114326;Perm=adfrw;Unique=BAAAAV+3JwIAAAAA; /Users/
liupc/Desktop/Remove Boyfriend/Stan's XX.png
250 End
PASV
227 Entering Passive Mode (10,80,22,90,239,184)
RETR Stan's XX.png
150 Opening BINARY mode data connection for 'Stan's XX.png' (1608061 bytes).
226 Transfer complete.
```

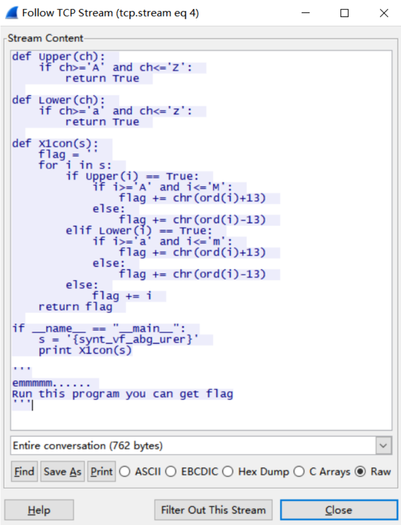
Entire conversation (931 bytes)

可以看出传输了两个文件：flag.py和Stan's xx.png

我们把这两个文件找到保存：

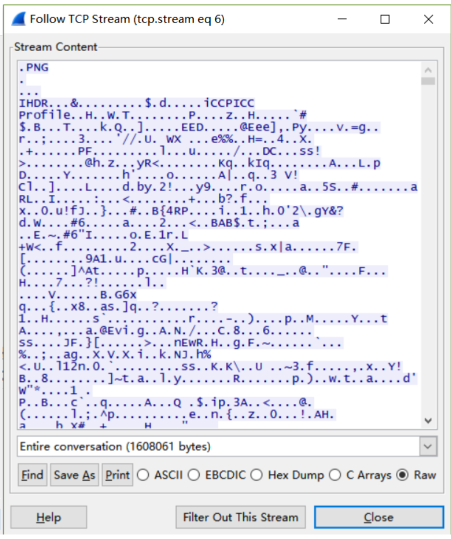
在第50行右击--Follow TCP Stream，可得到flag.py中的代码，

保存，运行到得：{flag_is_not_here}。显然不是。继续，
在82行右击--Follow TCP Stream,可得到一个PNG文件，保存为图片。



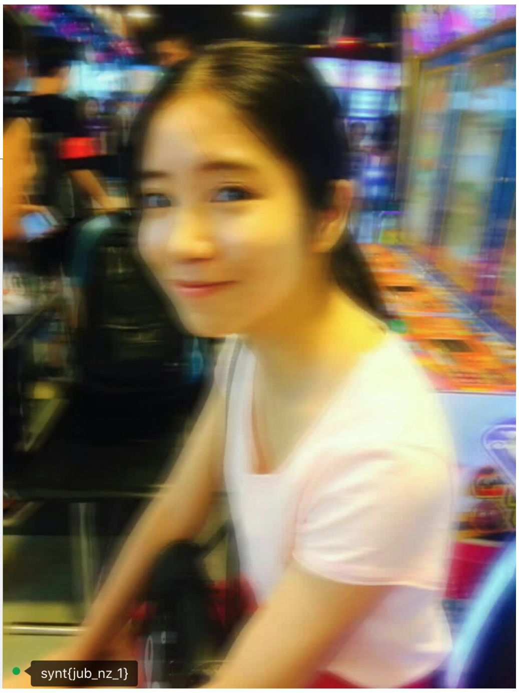
```
def Upper(ch):
    if ch>='A' and ch<='Z':
        return True

def Lower(ch):
    if ch>='a' and ch<='z':
        return True

def X1con(s):
    flag = ''
    for i in s:
        if Upper(i) == True:
            if i>='A' and i<='M':
                flag += chr(ord(i)+13)
            else:
                flag += chr(ord(i)-13)
        elif Lower(i) == True:
            if i>='a' and i<='m':
                flag += chr(ord(i)+13)
            else:
                flag += chr(ord(i)-13)
        else:
            flag += i
    return flag

if __name__ == "__main__":
    s = '{synt_vf_abg_urer}'
    print X1con(s)

'''
emmmmm......
Run this program you can get flag
'''
```

Entire conversation (762 bytes)



```
.PNG
.
...
IHDR...&.........$.d.....iCCPICC
Profile..H..W.T........P....Z..H.....`#
$.B...T....k.Q..]....EED.....@Eee],.Py....V.=g..
r..;....3....'//.U. WX ...e%%..H=..4..X.
.+......PF.........l...u..../...DC...ss!
>........@h.z...yR<.........Kq..kIq.........A...L.p
D.....Y.......h'....o......A|..q..3 V!
Cl..]....L....d.by.2!...y9....r.o.....a..5S..#.......a
RL..I.....:...<........+...b?.f...
x..O.u!fJ..}...#..B{4RP....i..1..h.O'2\.gY&?
d.W....#6.....a....2...<..BAB$.t.;...a
..E.~.#6"I.....o.E.1r.L
+W<..f..........2....X._..>......s.x|a......7F.
[........9A1.u....cG|........
(......]^At.....p.....H`K.3@..t...._..@.."....F...
H....7...?!......l..
....V......B.G6x
q...{..x8..as.]q..?.......?
1..H......s`...........r....-..)....p..M.....Y...t
A....,...a.@Evi.g..A.N./...C.8...6......
SS....JF.}[......>...nEWR.H..g.F.~......`...
%..;..ag..X.V.X.i..k.NJ.h%
<.U..l12n.O.`..........SS..K.K\..U ..~3.f......,.x..Y!
B..8........]~t.a..l.y.......R.......p.)..w.t..a....d'
W"*....1 .
P..B...C`..q.....A...Q .$.ip.3A..<....@.
(......l.;.^p..........e..n.{..z..O...!.AH.
```

Entire conversation (1608061 bytes)



图片左下角有信息：synt{jub_nz_1}

修改python代码运行，得到flag，提交成功。