chamd5-wp

Misc-车联网签到

Misc-the secret of car

解题思路

解压，car.pcapng可以解压出来，打开看是一个usb的流量包，老思路直接提取就可以

password1在car.pcapng里面

1.先用：tshark 命令把cap data提取出来tshark -r ./car.pcapng -T fields -e usb.capdata

2.github找个脚本提取下，得到password1：

```
#!/usr/bin/env python


import sys
import os


DataFileName = "usb.dat"


presses = []
```

```
normalKeys = {"04":"a", "05":"b", "06":"c", "07":"d", "08":"e", "09":"f", "0

shiftKeys = {"04":"A", "05":"B", "06":"C", "07":"D", "08":"E", "09":"F", "0a

def main():
    # check argv
    if len(sys.argv) != 2:
        print("Usage : ")
        print("        python UsbKeyboardHacker.py data.pcap")
        print("Tips : ")
        print("        To use this python script , you must install the tsha
        print("        You can use `sudo apt-get install tshark` to install
        print("Author : ")
        print("        WangYihang <wangyihanger@gmail.com>")
        print("        If you have any questions , please contact me by emai
        print("        Thank you for using.")
        exit(1)


    # get argv
    pcapFilePath = sys.argv[1]

    # get data of pcap
    os.system("tshark -r %s -T fields -e usb.capdata 'usb.data_len == 8' > %


    # read data
    with open(DataFileName, "r") as f:
        for line in f:
            presses.append(line[0:-1])
    # handle
    result = ""
    for press in presses:
        if press == '':
            continue
        if ':' in press:
            Bytes = press.split(":")
        else:
            Bytes = [press[i:i+2] for i in range(0, len(press), 2)]
        if Bytes[0] == "00":
            if Bytes[2] != "00" and normalKeys.get(Bytes[2]):
                result += normalKeys[Bytes[2]]
        elif int(Bytes[0],16) & 0b10 or int(Bytes[0],16) & 0b100000: # shift
            if Bytes[2] != "00" and normalKeys.get(Bytes[2]):
                result += shiftKeys[Bytes[2]]
        else:
            print("[-] Unknow Key : %s" % (Bytes[0]))
```

```
    print("[+] Found : %s" % (result))


    # clean the temp data
    os.system("rm ./%s" % (DataFileName))



if __name__ == "__main__":
    main()
```

```
@MacBook-Pro UsbKeyboardDataHacker-master % python UsbKeyboardDataHacker.py ./car.pcapng
nd : password1<SPACE><CAP>v3hicl3_ne7workin9_1s
```

用binwalk再分析下car.pcapng,发现可以分离出来了password2.txt,里面是摩斯加密的秘文:

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
3632540       0x376D9C        Zip archive data, at least v2.0 to extract, compressed size: 47, uncompressed size: 82, name: passwo
rd2.txt
3632689       0x376E31        End of Zip archive, footer length: 22
3632829       0x376EBD        Zip archive data, at least v2.0 to extract, compressed size: 47, uncompressed size: 82, name: passwo
rd2.txt
3632978       0x376F52        End of Zip archive, footer length: 22
```

在线解下:

..--.-/../--/.--./---/.-./-/.-/-./-/..--.-/..---/..--.-/..-/.-.../--/.

加密摩斯密码 解密摩斯密码

_IMPORTANT_2_U&ME

输入passwd解压得到wbs43open.bmp,一听这个名字就是bmp的隐写，直接用wbs43open一把梭就可以:

flag{_1nt3rnet_0f_Vehicles_4_f4n}

Reverse-层层关卡

解题思路

第一段 就是相减

```
f = 'olympics'
for i in range(len(f)):
    print(hex(ord(f[i]))[2:],end='')
print()
```

第二段 四个结果两两组合，试出来

```
f1 = 'in'
for i in range(len(f1)):
    print(chr(ord(f1[i])^33))
    print(chr(ord(f1[i])^32))
```

第三段 base64

flag{6f6c796d70696373_lO_Y2hpbmE=}