“红明谷”杯数据安全大赛 技能场景赛 部分wp

原创

「已注销」 于 2021-04-03 00:00:50 发布 4405 收藏 4

文章标签： 信息安全

本文链接：https://blog.csdn.net/pipidejiahuo/article/details/115409442

文章目录

一、MISC 我的心是冰冰的

bingbing.jpg

bingbing.zip

描述：似乎有信息被隐藏了。

1>.首先，思路是盲猜用图中的信息解压缩包的密码
另一边用zip爆破工具爆破，节省时间，爆破居然先爆破出来了
密码是：gnibgnib

2>.然后分析bingbing.pcapng
打开后发现是usb键盘流量，或者是usb鼠标流量
网上查资料可得，USB协议的数据部分在Leftover Capture Data域之中，右键leftover capture data –> 应用为列，可以将该域的值在主面板上显示，键盘数据包的数据长度为8个字节，击键信息集中在第3个字节，每次key stroke都会产生一个keyboard event usb packet

可以将 leftover capture data单独提取出来，在linux中，具体命令为：tshark -r bingbing.pcap -T fields -e usb.capdata > usbdata.txt

因此，这就是usb键盘流量

3.从得出的userdata.txt文件中过滤出键盘击键相关的流量，并根据映射表，将键盘按键按照对应关系输出出来，查资料找到了网上的脚本

```
#!/usr/bin/env python
import sys
import os

DataFileName = "usbdata.txt"

presses = []
```

```
normalKeys = {"04":"a", "05":"b", "06":"c", "07":"d", "08":"e", "09":"f", "0a":"g", "0b":"h", "0c":"i", "0d":"j"
, "0e":"k", "0f":"l", "10":"m", "11":"n", "12":"o", "13":"p", "14":"q", "15":"r", "16":"s", "17":"t", "18":"u",
"19":"v", "1a":"w", "1b":"x", "1c":"y", "1d":"z","1e":"1", "1f":"2", "20":"3", "21":"4", "22":"5", "23":"6","24"
:"7","25":"8","26":"9","27":"0","28":"<RET>","29":"<ESC>","2a":"<DEL>", "2b":"\t","2c":"<SPACE>","2d":"-","2e":"
=","2f":"[","30":"]","31":"\\","32":"<NON>","33":";","34":"'","35":"<GA>","36":",","37":".","38":"/","39":"<CAP>
","3a":"<F1>","3b":"<F2>", "3c":"<F3>","3d":"<F4>","3e":"<F5>","3f":"<F6>","40":"<F7>","41":"<F8>","42":"<F9>","
43":"<F10>","44":"<F11>","45":"<F12>"}

shiftKeys = {"04":"A", "05":"B", "06":"C", "07":"D", "08":"E", "09":"F", "0a":"G", "0b":"H", "0c":"I", "0d":"J",
 "0e":"K", "0f":"L", "10":"M", "11":"N", "12":"O", "13":"P", "14":"Q", "15":"R", "16":"S", "17":"T", "18":"U", "
19":"V", "1a":"W", "1b":"X", "1c":"Y", "1d":"Z","1e":"!", "1f":"@", "20":"#", "21":"$", "22":"%", "23":"^","24":
"&","25":"*","26":"(","27":")","28":"<RET>","29":"<ESC>","2a":"<DEL>", "2b":"\t","2c":"<SPACE>","2d":"_","2e":"+
","2f":"{","30":"}","31":"|","32":"<NON>","33":"\"","34":":","35":"<GA>","36":"<","37":">","38":"?","39":"<CAP>"
,"3a":"<F1>","3b":"<F2>", "3c":"<F3>","3d":"<F4>","3e":"<F5>","3f":"<F6>","40":"<F7>","41":"<F8>","42":"<F9>","4
3":"<F10>","44":"<F11>","45":"<F12>"}

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 tshark first."
        print "        You can use `sudo apt-get install tshark` to install it"
        print "Author : "
        print "        Angel_Kitty <angelkitty6698@gmail.com>"
        print "        If you have any questions , please contact me by email."
        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 > %s" % (pcapFilePath, DataFileName))

    # read data
    with open(DataFileName, "r") as f:
        for line in f:
            presses.append(line[0:-1])
    # handle
    result = ""
    for press in presses:
        Bytes = press.split(":")
        if Bytes[0] == "00":
            if Bytes[2] != "00":
                result += normalKeys[Bytes[2]]
        elif Bytes[0] == "20": # shift key is pressed.
            if Bytes[2] != "00":
                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()
```

最后结果从 DEL 分段分别解密文， 16进制解码即可
flag值： flag{8f9ed2f933ef14a8d0523d0349e1299c}

总结：挺有劲儿的一题，做了好久，明明答案早已经出来了，开始却没发现那是16进制，辗转了好久，以为是脚本错了，折腾好久，最后才想到答案可能是密文，提交答案时却是第10名提交的，错失前三血呜呜呜

二、签到

MISC 签到
答对8道数据安全知识小竞赛题，得flag

flag值： flag{7e63095d-4310-4f24-a01a-4a858d442fab}

赛后感受：小白做题，难得一批，题目好多不会做，还是很自闭了，感谢队友的辅助，一起加油！