2021年中国工业互联网安全大赛核能行业赛道writeup之usb流量分析

原创

苦行僧(csdn) 于 2021-10-24 14:00:00 发布 67 收藏
分类专栏： 信息安全 文章标签： CTF 流量分析 MISC 键盘鼠标

本文链接：https://blog.csdn.net/qpeity/article/details/120896413

目录

附件题：usb流量分析

题目描述：

> 具体描述忘记了o(╯□╰)o
>
> 大概意思是有个U盘插到电脑上，然后经过一些操作导致该电脑重启了。找到这个过程中的flag。

附件下载：

2021-10-12T15_49_10.808949+00_00usb流量分析.zip-网络攻防文档类资源-CSDN下载CTF附件题——usb流量分析USB是UniversalSerialBus（通用串行总线）的缩更多下载资源、学习资料请访问CSDN下载频道。
https://download.csdn.net/download/qpeity/33676446

一、USB协议

先引用一段对USB协议的解释

> USB是 UniversalSerial Bus（通用串行总线）的缩写，是一个外部总线标准，用于规范电脑与外部设备的连接和通讯，例如键盘、鼠标、打印机、磁盘或网络适配器等等。通过对该接口流量的监听，我们可以得到键盘的击键记录、鼠标的移动轨迹、磁盘的传输内容等一系列信息。
>
> USB有三种方式：USB UART，USB HID，USB Memory
>
> UART或者Universal Asynchronous Receiver/Transmitter。这种方式下，设备只是简单的将USB用于接受和发射数据，除此之外就再没有其他通讯功能了。
> HID是人性化的接口。这一类通讯适用于交互式，有这种功能的设备有：键盘，鼠标，游戏手柄和数字显示设备。
> USB Memory，或者说是数据存储。External HDD, thumb drive / flash drive，等都是这一类的。

因此通过流量分析，特别是 USB HID 得到键盘击键记录、鼠标移动轨迹等信息来获得flag。

二、键盘流量

> 键盘流量的特点：
>
> 键盘数据包的数据长度一般为8个字节，击键信息集中在第3个字节，每次击键都会产生一个数据包。如果看到给出的数据包中的信息并且只有第3个字节不为00， 那么可以猜测是一个键盘流。

第三字节，键盘的对应关系，查看 10 Keyboard / Keypad Usage（0x07）https://www.usb.org/sites/default/files/documents/hut1_12v2.pdf

第一个字节，每个bit都代表一个控制按键，如果看到这个数据包中第一个字节是 20 或者 02，那么可以认为是按住了 Shift切换。比如，0200040000000000，就是 Left Shift + a，就是大写 A。

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
Right GUI	Right Alt	Right Shift	Right Ctrl	Left GUI	Left Alt	Left Shift	Left Ctrl

提取敲击键盘的记录，就可能得到flag

三、鼠标流量

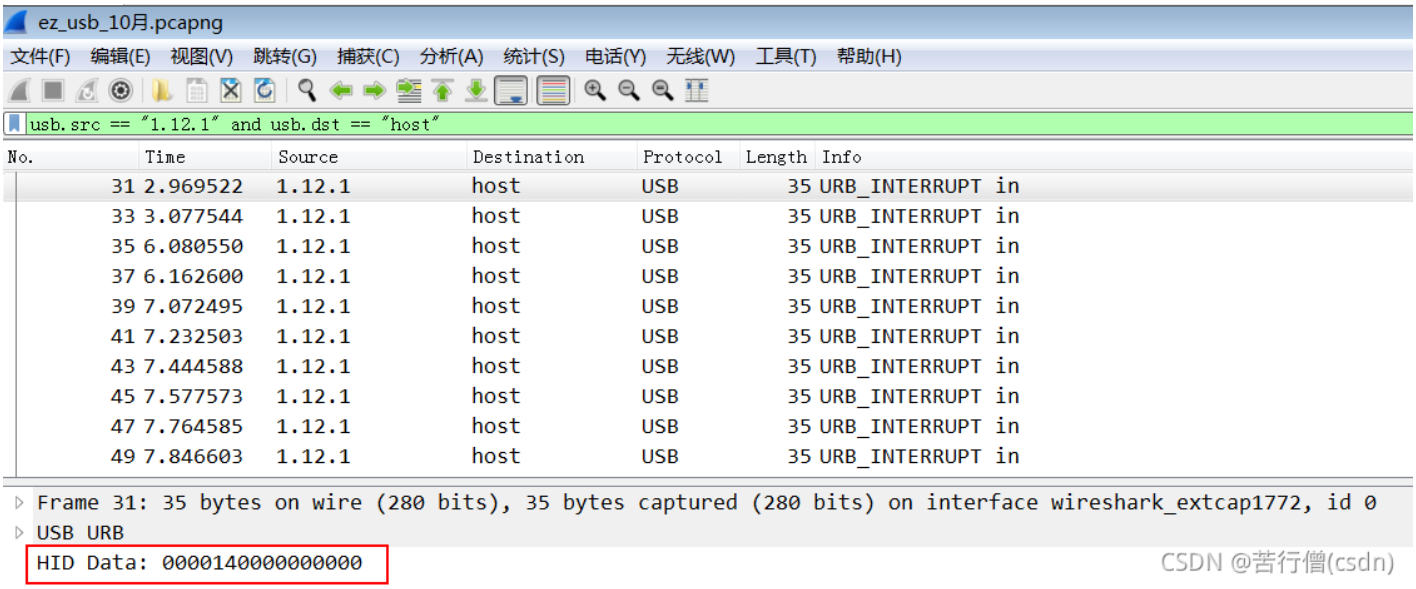
> 鼠标流量
> USB协议鼠标数据一般为四个字节
>
> 第一个字节， 代表按键。
> 当取0× 00时,代表没有按键
> 当取0× 01 时,代表按左键
> 当取0× 02时,代表当前按键为右键。
>
> 第二个字节，可看作为signed byte类型，其最高位为符号位。
> 当值为正时， 代表鼠标右移像素位；
> 值为负时， 代表鼠标左移像素位。
>
> 第三个字节， 代表垂直上下移动的偏移。
> 当值为正时， 代表鼠标上移像素位；
> 值为负时， 代表鼠标下移像素位。

提取鼠标轨迹，并用绘图工具画出来图像，即可能得到flag

四、writeup

附件解压缩得到一个加密的 flag.docx 文件和 一个ez_usb_10月.pcapng 包。需要分析流量包得到密码，打开文件 flag.docx 就能拿到flag了。

wireshark 打开 ez_usb_10月.pcapng 包，筛选 usb.src == "1.12.1" and usb.dst == "host"，发现每个发送给host的数据包，都是8个字节，且第3个字节不是00，认定是敲击键盘。



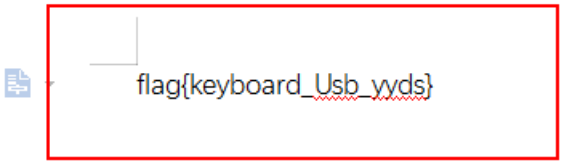
把所有第三个字节提取出来

```
14, 1a, 08, 15, 17, 28, 1e, 1f, 20, 04, 16, 07, 28, 21, 22, 23
```

再对照键盘的对应关系就得到密码 qwert123asd456。

```
q，w，e，r，t，return，1，2，3，a，s，d，return，4，5，6
```

用密码打开flag.docx就得到 —— flag{keyboard_Usb_yyds}



提取的办法也可以用 kali 里的工具 tshark。

- -r 输入文件
- -T 设置解码结果输出的格式， 默认为text
- -e 如果 -T fields选项指定， -e用来指定输出哪些字段，这里就输出 HID 部分

```
tshark -r ez_usb.pcapng -T fields -e usbhid.data | sed '/^\s*$/d' > keyboard.txt
```