来猜谜了

发表于 2021-03-05 更新于 2021-03-15 分类于 Challenge ， 2020 ， SWPU CTF 2020 ， Misc
Challenge | 2020 | SWPU CTF 2020 | Misc | 来猜谜了

点击此处获得更好的阅读体验

WriteUp来源

官方WP

题目考点

- *LSB隐写*
- *USB协议分析*

解题思路

压缩包打开后是一个 png 图片

关键信息：老色批，首字母是lsp，应该可以联想到lsb隐写，用stegslove将数据提取出来。

从文件头可以看出隐写进去的是zip文件，直接保存为zip就行了。不过也有师傅是直接用binwalk分离出来，然后将文件修补好的。

分离出的压缩包打开后有一个 mi.jpg 和一个流量数据包。

用wireshark打开流量包可以看到是usb协议，且leftover capture data域的数据长度为八个字节，所以可以判断出是键盘流量包。在kali中用tshark命令将leftover capture data域的数据提取出来。

然后就可以直接用键盘流量分析的脚本把敲击了哪些键分析出来，网上这种脚本很多，我就这不发了，嘿嘿

得到的字符串是： `AG DX AG DX AG DX`

这是一串用ADFGX编码方式加密的字符串

通过对照表就可以得到明文: `gogogo`

然后就剩mi.jpg了，flag是隐写在mi.jpg中的，隐写方式是outguess隐写，gogogo就是密钥。其实题目名和题目说明都有猜，这就是在提示隐写方式。直接用工具把flag分离出来就行了

Flag

```
flag{0ut9uEsS_1S_V4rY_e4sy}
```

- ***本文作者：*** *CTFHub*

- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/SWPU-CTF-2020/Misc/hJ5uqoDjN9cf5dPGi3nHET.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Misc # SWPU CTF 2020
耗子尾汁
套娃