HGAME 2020 WRITE UP

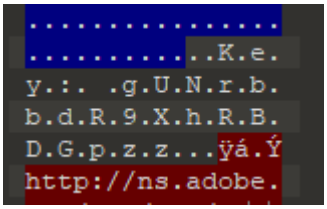
MISC

1. Comos 的午餐

流量分析题，导入 sslkey 文件后，过滤 http，在方法为 PUT 的 Reassembled SSL 中发现压

6103 wetransfer-us-prod-outgoing.s3.amazonaws.com application/x-www-form-urlencoded 1220 kB e418689cfb

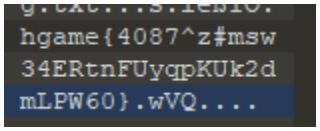
缩包文件头，导出 http 文件，改后缀为 zip，打开得到名为 outguess with key 的图片，010editor 发现 key



，用 outguess 解密得到网址 https://dwz.cn/69rOREdu，打开下载 zip，扫码得到 flag

2. 所见即为假

既然是假的，猜到伪加密，用 010editor 编辑后打开得到图片，同时压缩包 16 进制码末尾有 key 和提示 f5，用 f5-steganography 解密得到一堆 16 进制码，放入 010editor 得到 flag



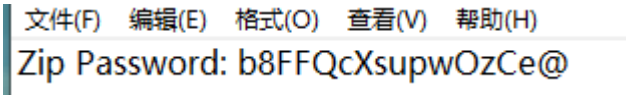
3. 地球上最后的夜晚

感觉是 pdf 隐写，用 Wbstego4.3open 解密得到压缩包密码 Zip Password: OmR#O12#b3b%s*IW，得到 word 文档，使用 zip 方法打开，word 文件夹里发现 secret.xml，打开得到 flag

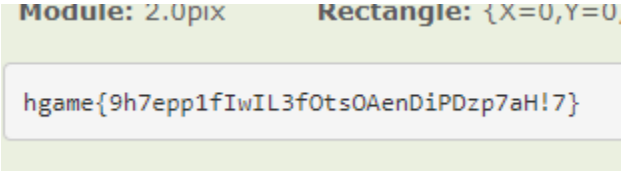
<flag>hgame{mkLbn8hP2g!p9ezPHqHuBu66SeDA13u1}</flag>

4. 玩玩条码

给的条码是日本四州码，解密得到 1087627，mp4 存在隐写，用 hint 给的软件打开，使用插件 MSU_stego_video (hint 里的 ffmpeg 插件不是很清楚用法) 加上之前解密得到的密码，解出 mp4 隐藏的



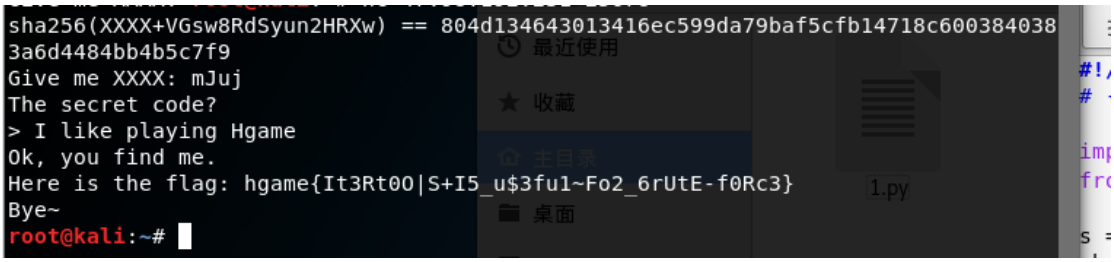
，解开压缩包得到 code128 条码，用 wiki 上提供的在线扫码得到 flag



CRYPTO

1. Verification_code

未知明文前四位，已知加密后的 sha256，范围比较小，写个脚本对应 nc 跑出来，但只有 60 秒的时间得到 flag



2. Remainder

多素数 rsa 和孙子定理，网上找到资料

中国剩余定理：

$$\begin{cases} x \equiv a_1 (\mod m_1) \\ x \equiv a_2 (\mod m_2) \\ \dots \\ x \equiv a_n (\mod m_n) \end{cases}$$

对于这样的同余式我们有一个公式：

$$M : M = \prod_{i=1}^{n} mi$$

$$B_i : \frac{M}{m_i} B_i \equiv 1 (\mod m_i) \{i = 1, 2, \dots n\} 即 B_i 是 \frac{M}{mi} 在模 m_i 下的逆元$$

$$x = \sum_{i=1}^{n} \frac{M}{m_i} \cdot B_i \cdot a_i$$

N 为 p，q，r 乘积，所以

```
N = p * q * r
#M = p * q * r
#Bi = gmpy2.invert(M / mi,mi)
#xi = M / mi * Bi * ci
```

，mi 为 p，q，r，写脚本得到 flag

hgame{CrT_w0Nt+6Oth3R_mE!!!}