2022第二届网刃杯网络安全大赛-Re

原创

夜白君 已于 2022-04-25 11:29:35 修改 2538 收藏 6

分类专栏： 2022第二届网刃杯网络安全大赛 文章标签： 网络安全 Reverse 第二届网刃杯

于 2022-04-25 09:12:36 首次发布

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_43264813/article/details/124396596

版权

2022第二届网刃杯网络安全大赛 专栏收录该内容

4 篇文章 36 订阅

订阅专栏

2022第二届网刃杯网络安全大赛-Re

前言

提示：该内容由夜刃TEOT战队-rootkit师傅原创，禁止抄袭！

一、RE1-ez_algorithm?

难度系数：5.0

题目描述：就是玩！！！

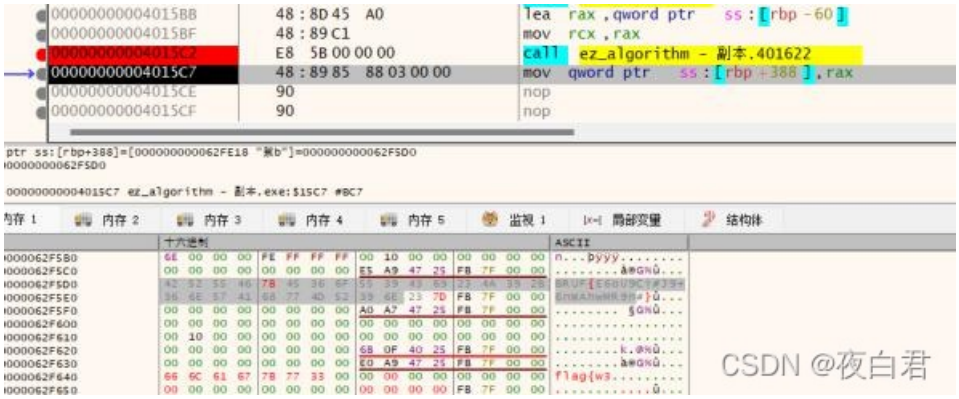
输入经过加密之后进行比较，长度看密文得知是28字节，逆向算法发现条件太多，但是发现：加密的相关因素仅仅和铭文本身和他所在flag中的偏移有关系，可以爆破。 加密函数太复杂，直接在汇编层面爆破 先修改一下程序

添加一个跳转，然后进行爆破。

逆向算法得知，数字和特殊字符和位置没有线性关系，所以先把数字爆出来

（一开始想直接用ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789得到密码表，但是后来发现在字符串的位置会影响加密的结果，尝试之后发现，字母不会变成别的就是字母，大写不变小写，缩短了爆破的困难）

在call下断点，找到rcx所在内存，直接修改成0123456789，得到一一对应的关系，很意外就是转个顺序然后手动复原flag，特殊字符转成下划线，看着就像flag了然后慢慢手动尝试，每次尝试之后，将对的答案直接加再下面的对的内存中，然后慢慢延长flag（用二分法逐渐靠近即可）最后尝试得到flag



但是发现最后一位不对，加密算法里

```
{
  switch ( v15 + rand() % 7 )           // 特殊字符转换
  {
    case 0:
      *REturn = ':';
      break;
```

要不下划线转出别的，要不就是

```
    }
  }
  else if ( *input111 <= '/' || *input111 > '9' )// 花括号不变
  {
    *REturn = *input111;
  }
  else                                  // 数字
```

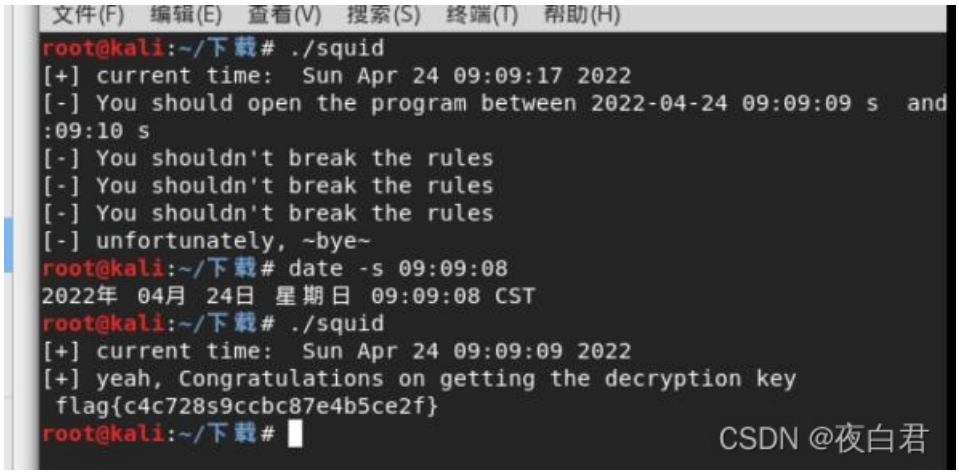
特殊符号不变，所以这里就是特殊符号，原来的符号

flag{w3Lc0mE_t0_3NcrYPti0N:}

二、Re2-定时启动

难度系数：4.0
题目描述：拼手速

直接用2018的kali设置好时间运行程序，得到flag（要删掉出现的readme文件，不然会报错）



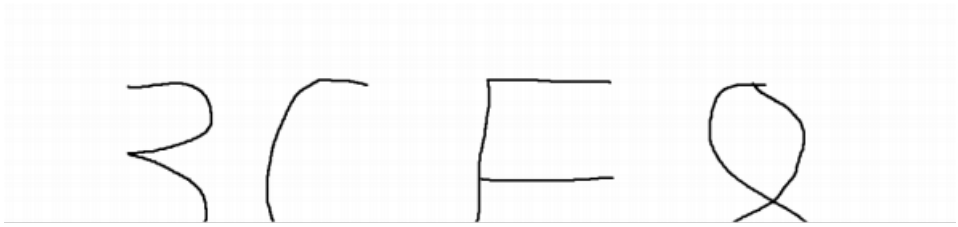
不知道为啥2021.3的kali跑不出来

flag{c4c728s9ccbc87e4b5ce2f}

三、Re3-Re_function

难度系数：4.0
题目描述：你能解出这道“简单”的逆向题目吗？

压缩包密码在旁边的16进制里，生成一个jpg文件，以为是宽高隐写，结果就是只有一半



这是改完宽高之后的图片，在考察什么呢？考察我能不能猜出来密码？考察我的耐心和精力和预测未来 的能力？得到两个文件

elf文件分析就是一个base64的过程，加解密不清楚，先不管，输入来自main的参数 看到exe文件

```
puts("please input flag: ");
v3 = _acrt_iob_func(0);
```

```
fgets(Buffer, 28, v3);
v4 = strlen(Buffer);
for ( i = 0; i < v4; i += 2 )
  Buffer[i] ^= 0x37u;
v6 = 0;
if ( v4 <= 0 )
  goto LABEL_7;
do
{
  v7 = *((_BYTE *)&cmp + v6);
  v8 = Buffer[v6++];
}
while ( v6 < v4 );
if ( v8 == v7 )
  puts("Get!!!");
```

CSDN @夜白君

把jz和下面的一行花指令patch掉就好了，得到清新的反汇编，看到对这些数据的奇数位进行了一个异或，然后进行比较。

```
v10 = 0;
cmp = xmmword_402120;
v11 = 0x72667841;
v12 = 0x4E5E7841;
v13 = 0x3D0E525D;
puts("please input flag: ");
```

异或后的结果是：SqcTSxCxSAwHGm/JvxQrvxiNjR9=

结合刚才elf的提示，直接进行一个变表的base64解密，得到flag

```
import base64
import string

str1 = "SqcTSxCxSAwHGm/JvxQrvxiNjR9="

string1 = "FeVYKw6a0lDIOsnZQ5EAf2MvjS1GUiLWPTtH4JqRgu3dbC8hrcNo9/mxzpXBky7+" string2 = "ABCDEFGHIJKLMNOPQRSTUVWX
YZabcdefghijklmnopqrstuvwxyz0123456789+/"
print (base64.b64decode(str1.translate(str.maketrans(string1,string2))))
```

7. flag{we1come_t0_wrb}

四、Re4-freestyle

难度系数：3.0
题目描述：论数学的重要性。

1. 拿到这个题目呢，非常的高兴和兴奋，感谢平台给我这次参加比赛的机会，我代表我个人和我身上的每一个器官表达由衷的感谢，虽然平台比赛全程我就没进去过几次，但是我还是再一次表达我的感谢。
2. 我诚惶诚恐的把得到的来之不易的文件小心翼翼的拖到ida里面去，然后静静的等待ida解析完这个程序，我用无名指按动F5，得到了我曾经学过的C代码，main函数还是那么的诱人，进去第一个函数，我看到运算，一个困难但是巧妙的if判断中隐藏着惊天的秘密，我拿起铅笔和一张大眼草，飞快的进行运算，终于在30s不到的时间，得到了结果是3327，然后我退出，又来到第二个函数，进行第二次小学5年级运算，是105，我非常的兴奋，然后打开浏览器，输入md5在线加密，进行加密在得到加密的结果的刹那间，我的人生得到了升华，我仿佛想起了王小云院士，想起了图灵，想起了我们的伟大的教员。在经过漫长的等待，等待平台重新开放的时候，我进去提交了这神圣的flag。
3. flag就是md5（3327105）

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖