看雪CTF2020 KCTF 秋季赛 签到题

原创

思源湖的鱼 于 2020-12-19 19:23:44 发布 447 收藏 2

分类专栏： ctf 文章标签： ctf reverse 看雪

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109757839

前言

佛系参加看雪CTF2020

最终只水了一个签到题

是个win64的逆向

解题过程

先运行看看

是个输入flag

然后进行判断对不对的小程序

扔进IDA

F5看伪码

顺手按着习惯改了改变量名

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  signed __int64 buf1_len; // rcx
  char *flag_mid_i; // r8
  __int64 buf2_i; // rax
  unsigned int v6; // edx
  char v7; // cl
  char buf_5_8[6]; // [rsp+20h] [rbp-E0h]
  char buf1[256]; // [rsp+30h] [rbp-D0h]
  char buf2[256]; // [rsp+130h] [rbp+30h]

  memset(buf1, 0, 0x100ui64);
  memset(buf2, 0, 0x100ui64);
  printf_wrapper("KCTF 2020!\n");
  printf_wrapper("http://bbs.pediy.com\n");
  printf_wrapper("Please input your flag: ");
  scanf_wrapper("%s", buf1, 256i64);
  buf1_len = -1i64;
  do
    ++buf1_len;
  while ( buf1[buf1_len] );
  if ( (_DWORD)buf1_len == 12
    && buf1[0] == 'f'
    && buf1[1] == 'l'
    && buf1[2] == 'a'
    && buf1[3] == 'g'
    && buf1[4] == '{'
    && buf1[11] == '}' )
  {
    flag_mid_i = buf_5_8;
    buf2_i = 0i64;
    *(_WORD *)&buf_5_8[4] = *(_WORD *)&buf1[9];
    v6 = 0;
    *(_DWORD *)buf_5_8 = *(_DWORD *)&buf1[5];
    while ( (unsigned __int8)(*flag_mid_i - '0') <= 9u )
    {
      ++v6;
      ++flag_mid_i;
      if ( v6 >= 6 )
      {
        buf2[0] = buf1[5];
        buf2[1] = buf1[5] + buf1[6] - 48;
        buf2[2] = buf1[5] + buf1[6] - 48 + buf1[7] - 48;
        buf2[3] = buf2[2] + buf1[8] - 48;
        buf2[4] = buf2[2] + buf1[8] - 48 + buf1[9] - 48;
        buf2[5] = buf2[4] + buf1[10] - 48;
        while ( 1 )
        {
          v7 = buf2[buf2_i++];
          if ( v7 != a2Efi[buf2_i - 1] )
            break;
          if ( buf2_i == 7 )
          {
            printf_wrapper("You are winner!\n");
            return 0;
          }
        }
        break;
      }
    }
  }
  printf_wrapper("Try again!\n");
  return -1;
}
```


需要输入一个 `flag{++++++}` 的字符串

根据输入的6位字符串计算得到buf2要为a2Efi的内容

跟踪看下

```
.rdata:0000000140003268 aTryAgain       db 'Try again!',0Ah,0   ; DATA XREF: main:loc_1400011A4↑o
.rdata:0000000140003274 a2Efi           db '2;=EF',0            ; DATA XREF: main+12F↑o
.rdata:000000014000327B                 align 20h
```

那就跟着做就是了

```
>>> ord(':')+48-ord('2')
57
>>> chr(57)
'9'
>>> ord('=')+48+48-ord('2')-ord('g')
4
>>> ord('=')+48+48-ord('2')-ord('9')
50
>>> chr(50)
'2'
>>> ord('E')+48-ord('=')
56
>>> chr(56)
'8'
>>> ord('F')+48+48-ord('8')-ord('=')
49
>>> chr(49)
'1'
>>> ord('I')+48-ord('F')
51
>>> chr(51)
'3'
>>>
```


于是得到flag

```
flag{292813}
encryted: 2;=EFI
```

结语

简单的逆向