攻防世界 Reverse高手进阶区 2分题 IgniteMe

原创

思源湖的鱼 于 2020-12-04 13:29:09 发布 101 收藏
分类专栏： ctf 文章标签： ctf 攻防世界 reverse

本文链接：https://blog.csdn.net/weixin_44604541/article/details/110633295

前言

继续ctf的旅程
攻防世界Reverse高手进阶区的2分题
本篇是IgniteMe的writeup

发现攻防世界的题目分数是动态的
就仅以做题时的分数为准了

解题过程

下下来一个exe

PE查壳

扔进IDA

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int result; // eax
  size_t i; // [esp+4Ch] [ebp-8Ch]
  char v5[4]; // [esp+50h] [ebp-88h]
  char v6[28]; // [esp+58h] [ebp-80h]
  char v7; // [esp+74h] [ebp-64h]

  sub_402B30(&unk_446360, "Give me your flag:");
  sub_4013F0(sub_403670);
  sub_401440(v6, 127);
  if ( strlen(v6) < 0x1E && strlen(v6) > 4 )
  {
    strcpy(v5, "EIS{");
    for ( i = 0; i < strlen(v5); ++i )
    {
      if ( v6[i] != v5[i] )
      {
        sub_402B30(&unk_446360, "Sorry, keep trying! ");
        sub_4013F0(sub_403670);
        return 0;
      }
    }
    if ( v7 == 125 )
    {
      if ( (unsigned __int8)sub_4011C0(v6) )
        sub_402B30(&unk_446360, "Congratulations! ");
      else
        sub_402B30(&unk_446360, "Sorry, keep trying! ");
      sub_4013F0(sub_403670);
      result = 0;
    }
    else
    {
      sub_402B30(&unk_446360, "Sorry, keep trying! ");
      sub_4013F0(sub_403670);
      result = 0;
    }
  }
  else
  {
    sub_402B30(&unk_446360, "Sorry, keep trying!");
    sub_4013F0(sub_403670);
    result = 0;
  }
  return result;
}
```


跟踪`sub_4011C0`

```
bool __cdecl sub_4011C0(char *a1)
{
  size_t v2; // eax
  signed int v3; // [esp+50h] [ebp-B0h]
  char v4[32]; // [esp+54h] [ebp-ACh]
  int v5; // [esp+74h] [ebp-8Ch]
  int v6; // [esp+78h] [ebp-88h]
  size_t i; // [esp+7Ch] [ebp-84h]
  char v8[128]; // [esp+80h] [ebp-80h]

  if ( strlen(a1) <= 4 )
    return 0;
  i = 4;
  v6 = 0;
  while ( i < strlen(a1) - 1 )
    v8[v6++] = a1[i++];
  v8[v6] = 0;
  v5 = 0;
  v3 = 0;
  memset(v4, 0, 0x20u);
  for ( i = 0; ; ++i )
  {
    v2 = strlen(v8);
    if ( i >= v2 )
      break;
    if ( v8[i] >= 97 && v8[i] <= 122 )
    {
      v8[i] -= 32;
      v3 = 1;
    }
    if ( !v3 && v8[i] >= 65 && v8[i] <= 90 )
      v8[i] += 32;
    v4[i] = byte_4420B0[i] ^ sub_4013C0(v8[i]);
    v3 = 0;
  }
  return strcmp("GONDPHyGjPEKruv{{pj]X@rF", v4) == 0;
}
```


大小写互换
再做异或

跟踪`sub_4013C0`

```
int __cdecl sub_4013C0(int a1)
{
  return (a1 ^ 0x55) + 72;
}
```

提取`004420B0`

```
004420B0  0D 13 17 11 02 01 20 1D  0C 02 19 2F 17 2B 24 1F
004420C0  1E 16 09 0F 15 27 13 26  0A 2F 1E 1A 2D 0C 22 04
```

那整个流程都在上面了

逆向就是了

```
n = 28
val1 = [0x0D,0x13,0x17,0x11,0x02,0x01,0x20,0x1D,0x0C,0x02,0x19,0x2F,0x17,0x2B,
        0x24,0x1F,0x1E,0x16,0x09,0x0F,0x15,0x27,0x13,0x26,0x0A,0x2F,0x1E,0x1A,
        0x2D,0x0C,0x22,0x04]
v4 = "GONDPHyGjPEKruv{{pj]X@rF"
v8 = ""
flag = ""

for i in range(len(v4)):
    v8 += chr(((ord(v4[i]) ^ val1[i]) - 72) ^ 0x55)

for i in range(len(v8)):
    if ord(v8[i]) >= 97 and ord(v8[i]) <= 122:
        flag += chr(ord(v8[i]) - 32)
    elif ord(v8[i]) >= 65 and ord(v8[i]) <= 90:
        flag += chr(ord(v8[i]) + 32)
    else:
        flag += v8[i]

print('EIS{'+flag+'}')
```

```
1  n = 28
2  val1 = [0x0D,0x13,0x17,0x11,0x02,0x01,0x20,0x1D,0x0C,0x02,0x19,0x2F,0x17,0x2B,
3          0x24,0x1F,0x1E,0x16,0x09,0x0F,0x15,0x27,0x13,0x26,0x0A,0x2F,0x1E,0x1A,
4          0x2D,0x0C,0x22,0x04]
5  v4 = "GONDPHyGjPEKruv{{pj]X@rF"
6  v8 = ""
7  flag = ""
8
9  for i in range(len(v4)):
10     v8 += chr(((ord(v4[i]) ^ val1[i]) - 72) ^ 0x55)
11
12 for i in range(len(v8)):
13     if ord(v8[i]) >= 97 and ord(v8[i]) <= 122:
14         flag += chr(ord(v8[i]) - 32)
15     elif ord(v8[i]) >= 65 and ord(v8[i]) <= 90:
16         flag += chr(ord(v8[i]) + 32)
17     else:
18         flag += v8[i]
19
20 print('EIS{'+flag+'}')
```

```
EIS{wadx_tdgk_aihc_ihkn_pjlm}
```


得到flag

结语

简单逆向