buuctf Crackme6

原创

20000s 于 2020-05-16 19:23:24 发布 396 收藏 1

分类专栏： buuctf

本文链接：https://blog.csdn.net/qq_37439229/article/details/106161683

buuctf 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

这道题涉及的知识点说实话还是蛮多的。。。

```
.text:0040122A ; ---------------------------------------------------------------------------
.text:0040122A
.text:0040122A loc_40122A:                             ; CODE XREF: .text:loc_401260↓j
.text:0040122A                 mov     edx, [ebp-50h]
.text:0040122D                 add     edx, 1
.text:00401230                 mov     [ebp-50h], edx
.text:00401233
.text:00401233 loc_401233:                             ; CODE XREF: .text:00401228↑j
.text:00401233                 mov     eax, [ebp-50h]
.text:00401236                 cmp     eax, [ebp-4Ch]
.text:00401239                 jge     short loc_401262
.text:0040123B                 mov     ecx, [ebp+0Ch]
.text:0040123E                 add     ecx, [ebp-50h]
.text:00401241                 movsx   edx, byte ptr [ecx]
.text:00401244                 cmp     edx, 30h
.text:00401247                 jl      short loc_401257
.text:00401249                 mov     eax, [ebp+0Ch]
.text:0040124C                 add     eax, [ebp-50h]
.text:0040124F                 movsx   ecx, byte ptr [eax]
.text:00401252                 cmp     ecx, 39h
.text:00401255                 jle     short loc_401260
.text:00401257
.text:00401257 loc_401257:                             ; CODE XREF: .text:00401247↑j
.text:00401257                 mov     dword ptr [ebp-54h], 1
.text:0040125E                 jmp     short loc_401262
.text:00401260 ; ---------------------------------------------------------------------------
.text:00401260
.text:00401260 loc_401260:                             ; CODE XREF: .text:00401255↑j
.text:00401260                 jmp     short loc_40122A
.text:00401262 ; ---------------------------------------------------------------------------
.text:00401262
.text:00401262 loc_401262:                             ; CODE XREF: .text:00401239↑j
.text:00401262                                         ; .text:0040125E↑j
.text:00401262                 cmp     dword ptr [ebp-54h], 0
```


首先是这里的加密

主要是看汇编，不难，yafu一下知道是[2,3,5,7,11,13,17,19,23]

```
a = [2 , 3, 5, 7, 11 ,13,17,19,23]
 b = [0x33,0x21,0x22,0x21,0x35,0x7c,0x62,0x65,0x6e]
 for i in range(9):
    a[i] = a[i] +0x41
    a[i] = a[i] ^b[i]
"".join(chr(a[i]) for i in range(9))
#pediy2016
```

之后进入异常（因为/0,）

```
void __cdecl sub_4013B0(HWND hWnd, char *a2)
{
  int v2; // ST70_4
  char v3; // [esp+64h] [ebp-1029Ch]
  char v4; // [esp+65h] [ebp-1029Bh]
  char v5; // [esp+66h] [ebp-1029Ah]
  char v6; // [esp+67h] [ebp-10299h]
  char v7; // [esp+68h] [ebp-10298h]
  char v8; // [esp+69h] [ebp-10297h]
  char v9; // [esp+6Ah] [ebp-10296h]
  char v10; // [esp+6Bh] [ebp-10295h]
  char v11; // [esp+6Ch] [ebp-10294h]
  char v12; // [esp+6Dh] [ebp-10293h]
  char v13; // [esp+6Eh] [ebp-10292h]
  char v14; // [esp+6Fh] [ebp-10291h]
  char v15; // [esp+70h] [ebp-10290h]
  char v16; // [esp+71h] [ebp-1028Fh]
  char v17; // [esp+72h] [ebp-1028Eh]
  char v18; // [esp+73h] [ebp-1028Dh]
  char v19; // [esp+74h] [ebp-1028Ch]
  char v20; // [esp+75h] [ebp-1028Bh]
  char v21; // [esp+76h] [ebp-1028Ah]
  char v22; // [esp+77h] [ebp-10289h]
  char v23; // [esp+78h] [ebp-10288h]
  char v24; // [esp+79h] [ebp-10287h]
  char v25; // [esp+7Ah] [ebp-10286h]
  char v26; // [esp+7Bh] [ebp-10285h]
  char v27; // [esp+7Ch] [ebp-10284h]
  char v28; // [esp+7Dh] [ebp-10283h]
  char v29; // [esp+7Eh] [ebp-10282h]
  char v30; // [esp+7Fh] [ebp-10281h]
  char v31; // [esp+80h] [ebp-10280h]
```


这里是个虚拟机保护，得慢慢解析每条指令，由于太繁琐了我就简单说一下过程，就不演示了
首先检查是否数量是0x14，之后直接对比字符串，是cool1,最后6个字符，是要解两个方程
（当然，解方程之前把你的ascii码值变成相应数字,比如0x31 变 1）

```
import z3
x = z3.Int('x')
y = z3.Int('y')
z = z3.Int('z')
s = z3.Solver()
s.add(x<=9,x>=0)
s.add(y<=9,y>=0)
s.add(z>=0,z<=9)
s.add(x==1)
s.add(x+y*y*y+z*z*z==0x64+10*y+z)
print(s.model())
# 1 5 3
```

```
import z3
x = z3.Int('x')
y = z3.Int('y')
z = z3.Int('z')
g = z3.Int('g')
s = z3.Solver()
s.add(x<=9,x>=0)
s.add(y<=9,y>=0)
s.add(z>=0,z<=9)
s.add(g<=9,g>=0)
s.add(10*x+y+10*z+g==0x23)
s.add(4*(10*x+y)+2*(10*z+g)==0x5e)
print(s.model())
#2312
```

flag:pediy20161532312