XCTF 3rd-GCTF-2017 hackme

原创

pipixia233333 于 2019-05-07 08:42:05 发布 1547 收藏
分类专栏： 逆向之旅

这个题 有字符串 感觉简单了许多

IDA View-A | Pseudocode-A | Strings window | Hex View-1 | Structures | Enums | Imports | Exports

```
18  _BOOL4 flag__re; // [rsp+B8h] [rbp-8h]
19  int i; // [rsp+BCh] [rbp-4h]
20
21  sub_407470("Give me the password: ");
22  sub_4075A0("%s", input, a2);
23  for ( i = 0; input[i]; ++i )                  // len==22
24    ;
25  flag__re = i == 22;
26  v17 = 10;
27  do
28  {
29    v6 = sub_406D90("%s", input, v2, v3, v4, v5);
30    v3 = (v6 % 22);
31    v14 = v6 % 22;
32    v16 = 0;
33    code_ = byte_6B4270[v6 % 22];
34    index_va = input[v6 % 22];
35    index_1 = v6 % 22 + 1;
36    v15 = 0;
37    while ( v15 < index_1 )
38    {
39      ++v15;
40      v16 = 1828812941 * v16 + 12345;
41    }
42    v2 = v16;
43    v10 = v16 ^ index_va;
44    if ( code_ != (v16 ^ index_va) )
45      flag__re = 0;
46    --v17;
47  }
48  while ( v17 );
49  if ( flag__re )
50    v9 = sub_407470("Congras\n");
51  else
52    v9 = sub_407470("Oh no!\n");
53  return 0LL;
54}
```


然后这个题 算法就在这 我们写出来脚本就行

```
#include <stdio.h>
#include<iostream>
#include<iomanip>
#include<stdio.h>
#include<string.h>
#include<algorithm>
#include<vector>
#include<iostream>
#include<map>
#include<time.h>
#include<queue>
#include <Windows.h>
#include "windows.h"
using namespace std;
unsigned char ida_chars[] =
{
  0x5F, 0xF2, 0x5E, 0x8B, 0x4E, 0x0E, 0xA3, 0xAA, 0xC7, 0x93,
  0x81, 0x3D, 0x5F, 0x74, 0xA3, 0x09, 0x91, 0x2B, 0x49, 0x28,
  0x93, 0x67, 0x00, 0x00
};
int main()
{
    int s,temp;
    for(int i=0;i<22;i++)
    {
        s=ida_chars[i];
        temp=0;
        for(int j=0;j<i+1;j++)
        {
            temp = 1828812941 * temp + 12345;
        }
        printf("%c",(temp^s)&0xff);
    }

    return 0;
}
```