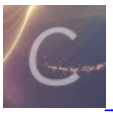
[BUUCTF]REVERSE——[ACTF新生赛2020]rome

原创

Angel~Yan 于 2020-11-26 17:50:46 发布 438 收藏 2

分类专栏： BUUCTF刷题记录 REVERSE

本文链接：https://blog.csdn.net/mcmuyanga/article/details/110196934


BUUCTF刷题记录 同时被 2 个专栏收录

198 篇文章 14 订阅

订阅专栏


REVERSE

75 篇文章 1 订阅

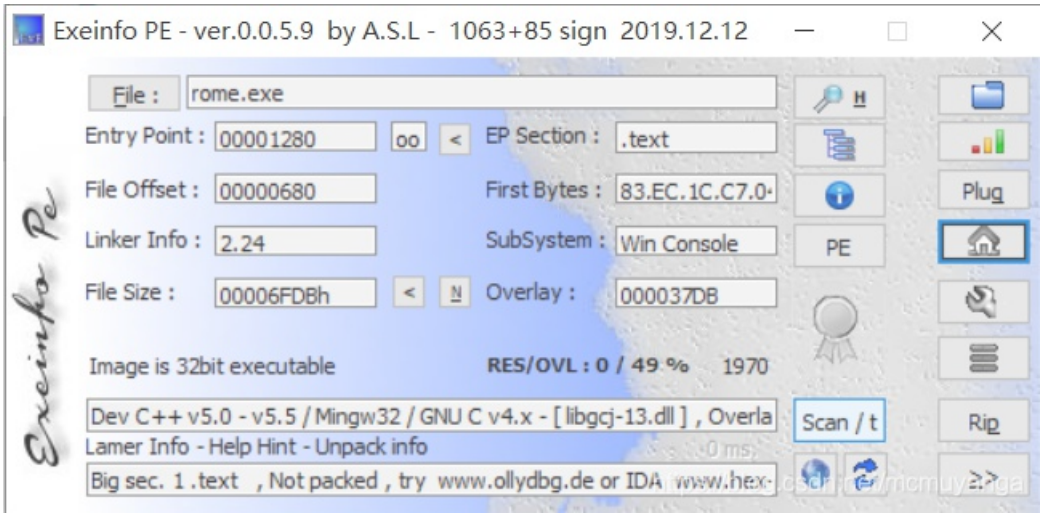
订阅专栏

[ACTF新生赛2020]rome

附件

步骤

1. 无壳，32位程序



2. 32位ida载入，根据提示字符串“You are correct！”，找到关键函数func

```
v15 = 'Q';
 v16 = 's';
 v17 = 'w';
 v18 = '3';
 v19 = 's';
 v20 = 'j';
 v21 = '_';
 v22 = 'l';
 v23 = 'z';
 v24 = '4';
```

```
  v25 = '_';
  v26 = 'U';
  v27 = 'j';
  v28 = 'w';
  v29 = '@';
  v30 = 'l';
  v31 = '\0';
  printf("Please input:");
  scanf("%s", &v5);
  result = v5;
  if ( v5 == 65 )
  {
    result = v6;
    if ( v6 == 67 )
    {
      result = v7;
      if ( v7 == 84 )
      {
        result = v8;
        if ( v8 == 70 )
        {
          result = v9;
          if ( v9 == 123 )
          {
            result = v14;
            if ( v14 == 125 )
            {
              v1 = v10;
              v2 = v11;
              v3 = v12;
              v4 = v13;
              for ( i = 0; i <= 15; ++i )
              {
                if ( *((_BYTE *)&v1 + i) > 64 && *((_BYTE *)&v1 + i) <= 90 )// 大写字母
                  *((_BYTE *)&v1 + i) = (*((char *)&v1 + i) - 51) % 26 + 65;
                if ( *((_BYTE *)&v1 + i) > 96 && *((_BYTE *)&v1 + i) <= 122 )// 小写字母
                  *((_BYTE *)&v1 + i) = (*((char *)&v1 + i) - 79) % 26 + 97;
              }
              for ( i = 0; i <= 15; ++i )
              {
                result = (unsigned __int8)*(&v15 + i);
                if ( *((_BYTE *)&v1 + i) != (_BYTE)result )
                  return result;
              }
              result = printf("You are correct!");
            }
          }
        }
      }
    }
  }
  return result;
}
```

3. 程序很简单，就是让我们输入一个字符串，然后判断大小写，进行相应的运算，最后得到了程序开头的数组 v15= [‘Q’,‘s’,‘w’,‘3’,‘s’,‘j’, ‘’,‘l’,‘z’,‘4’,’’,‘U’,‘j’,‘w’,’@’,‘l’]

由于加密运算里的那个%运算的逆运算很神奇，所以我就采取了最简单值观的暴力破解

```python
v15= [ 'Q','s','w','3','s','j', '_','l','z','4','_','U','j','w','@','l' ]
flag=""

for i in range(16):
    for j in range(128):#ascii表上有127个字符，一个一个试吧
        x=j
        if chr(x).isupper():
            x=(x-51)%26+65
        if chr(x).islower():
            x=(x-79)%26+97
        if chr(x)==v15[i]:
            flag+=chr(j)

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

```
C:\Users\Chrome.py
flag{Cae3ar_th4_Gre@t}
>>>
```