

攻防世界re1

原创

[hello@kitty](#) 于 2020-09-26 15:16:14 发布 118 收藏

分类专栏: [ctf逆向](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/keep_reading/article/details/108482073

版权



[ctf逆向](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

文章目录

攻防世界re1

[先找main函数翻译成伪代码](#)

[分析伪代码找到这个字符串 \(还有下边那个dq\)](#)

攻防世界re1

(dword: 由 4 字节长(32 位整数)的数字表示的数据)

查壳脱壳

先找main函数翻译成伪代码

打开IDA，一般自动定位到start函数
在start，双击定位，找到了一个

```
; Attributes: library function

public start
start proc near

; FUNCTION CHUNK AT 0040132A SIZE 00000117 BYTES
; FUNCTION CHUNK AT 0040146F SIZE 0000000F BYTES

call    sub_4052B4
jmp     loc_40132A
start endp ; sp-analysis failed
```

.....推测这里有main函数线索的可能性比较大，再双击以下试试

```
PerformanceCount= LARGE_INTEGER ptr -14h
SystemTimeAsFileTime= _FILETIME ptr -0Ch
var_4= dword ptr -4

push    ebp |
mov     ebp, esp
sub     esp, 14h
and     [ebp+SystemTimeAsFileTime.dwLowDateTime], 0
and     [ebp+SystemTimeAsFileTime.dwHighDateTime], 0
mov     eax, __security_cookie
push    esi
push    edi
mov     edi, 0BB40E64Eh
mov     esi, 0FFFF0000h
cmp     eax, edi
jz      short loc_4052E4
```

调到了汇编语言的部分，（不太会，把这几行都点开看了看F5，发现mov后边那个比较像.....找到main函数）双击ctrlx再F5

分析伪代码找到这个字符串（还有下边那个dq）

```
.rdata:00413E2C a1qnan          dd  '1#QNHN',0          ; DATA XREF: sub_40102C:10C_
.rdata:00413E33                                     align 4
.rdata:00413E34 xmmword_413E34  xmmword  3074656D30633165577B465443545544h
.rdata:00413E34                                     ; DATA XREF: sub_401000+10↑r
.rdata:00413E44 qword_413E44    dq  7D465443545544h     ; DATA XREF: sub_401000+27↑r
```

16进制大端小端存储