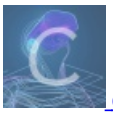
bugkuCTF之逆向入门解题思路

原创

邻家小白 于 2019-08-09 17:33:49 发布 1537 收藏 2

分类专栏： ctf 文章标签： bugkuCTF

本文链接：https://blog.csdn.net/xiaoguiyingxia/article/details/98968651



逆向入门

我们把文件下载得到的exe文件拖入ida。看到有个main主函数。
printf就是输出

```
call    _printf
mov     byte ptr [esp+2Fh], 66h
mov     byte ptr [esp+2Eh], 6Ch
mov     byte ptr [esp+2Dh], 61h
mov     byte ptr [esp+2Ch], 67h
mov     byte ptr [esp+2Bh], 7Bh
mov     byte ptr [esp+2Ah], 52h
mov     byte ptr [esp+29h], 65h
mov     byte ptr [esp+28h], 5Fh
mov     byte ptr [esp+27h], 31h
mov     byte ptr [esp+26h], 73h
mov     byte ptr [esp+25h], 5Fh
mov     byte ptr [esp+24h], 53h
mov     byte ptr [esp+23h], 30h
mov     byte ptr [esp+22h], 5Fh
mov     byte ptr [esp+21h], 43h
mov     byte ptr [esp+20h], 30h
mov     byte ptr [esp+1Fh], 4Fh
mov     byte ptr [esp+1Eh], 4Ch
mov     byte ptr [esp+1Dh], 7Dh
mov     eax, 0
leave
retn
```


然后每一条按下“R”得出结果

```
call    ___main
mov     dword ptr [esp], offset aHiThisI
call    _printf
mov     byte ptr [esp+2Fh], 'f'
mov     byte ptr [esp+2Eh], 'l'
mov     byte ptr [esp+2Dh], 'a'
mov     byte ptr [esp+2Ch], 'g'
mov     byte ptr [esp+2Bh], '{'
mov     byte ptr [esp+2Ah], 'R'
mov     byte ptr [esp+29h], 'e'
mov     byte ptr [esp+28h], '_'
mov     byte ptr [esp+27h], '1'
mov     byte ptr [esp+26h], 's'
mov     byte ptr [esp+25h], '_'
mov     byte ptr [esp+24h], 'S'
mov     byte ptr [esp+23h], '0'
mov     byte ptr [esp+22h], '_'
mov     byte ptr [esp+21h], 'C'
mov     byte ptr [esp+20h], '0'
mov     byte ptr [esp+1Fh], 'O'
mov     byte ptr [esp+1Eh], 'L'
mov     byte ptr [esp+1Dh], 7Dh
mov     eax, 0
leave
retn
```


R，后的字符即可。flag{Re_1s_S0_C0oL}