# 攻防世界 echo-server writeup



#### 攻防世界 echo-server writeup

- 一. 知识点
- (1) 花指令
- (2) IDA出现"sp-analysis failed"
- 二. 解题步骤

### 一.知识点

### (1) 花指令

0x01 概念

花指令是,由设计者特别构思,希望使反汇编的时候出错,让破解者无法清楚正确地反汇编程序的内容,迷失方向。经典的是,目标位置是另一条指令的中间,这样在反汇编的时候便会出现混乱。花指令有可能利用各种指令: jmp, call, ret的一些堆栈技巧,位置运算,等等。

#### 0x02 常见花指令

| 机器码 | 汇编语言   |
|-----|--|
| 9A  | CALL immed32                                     |
| E8  | CALL immed16                                     |
| E9  | JMP immed16                                      |
| EB  | JMP immed8 https://blog.csdn.net/weizin_45225586 |

0x03 如何去除花指令

第一步:

• 识别哪些是有用的数据,哪些是垃圾数据。

第二步**:** 

• 把垃圾数据用nop(0x90h)填充。

### (2) IDA出现"sp-analysis failed"

#### IDA官网解释:

Problem: Failed to trace the value of the stack pointer

Description: The value of the stack pointer at the end of the function is different from its value at the start of the function. IDA checks for the difference only if the function is ended by a "return" instruction. The most probable cause is that stack tracing has failed. This problem is displayed in the disassembly listing with the "sp-analysis failed" comment. What to do: 1. Examine the value of stack pointer at various locations of the function and try to find out why the stack tracing has failed. Usually, it fails because some called function changed the stack pointer (by purging the input parameters, for example) 2. If you have found the offending function, change its attributes (namely, number of bytes purged upon return). 3. Another way is to specify manually how the stack pointer is modified. See Change stack pointer command

大意是ida检测到,IDA有栈跟踪的功能,它在函数内部遇到ret(retn)指令时会做判断:栈指针的值在函数的开头/结尾是否一致,如果不一致就会在函数的结尾标注"sp-analysis failed"。一般编程中,不同的函数调用约定(如stdcall&\_cdcel call)可能会出现这种情况;另外,为了实现代码保护而加入代码混淆(特指用push/push+ret实现函数调用)技术也会出现这种情况。

#### 二.解题步骤

(1)拖进IDA反编译,查看伪代码,可以看到这里的函数调用很奇怪

| 💱 IDA - echo-server D:\课程学习\大三上 | _\RE\攻防世界\echo-server |
|---------------------------------|-----------------------|
|---------------------------------|-----------------------|

| 文件(E) 编辑(E) 跳转(」) 搜索(H) 视图(Ⅴ) 认 | 周试器 选工 | 页( <u>O</u> ) | 窗口( <u>W</u> ) 帮助           |      |        |               |          |      |                |
|---------------------------------|--------|---------------|-----------------------------|------|--------|---------------|----------|------|----------------|
| 📂 🔒 🗢 🕶 🕶 🏪 🐴 🗛 🗎               | 🔬 🔺    | 0             | at at at -st = st 🖬 🤇       | X    |        | ■ 无调试器        | •        | *c d | P 🗊 🕈 🏠        |
| 店运数 📕 常振运数 📕 北人 🔲 数根            | + /m   | 月 立17 夕       | <b>本日</b>                   |      |        | •             |          |      |                |
| □ 厍函数 ■ 帛规函数 ■ 指令 ■ 数据 ■        |        | 外部在           | 寸方                          |      | -      | かしたす          | _        | _    |                |
| 回困奴図ロ                           |        |               | IDA View-A                  | ×    |        | 仍代码           | ×        | Q    | 十六进制视图-1       |
| 函数名称                            | 段      | 1             | intcdecl main()             |      |        |               |          |      |                |
| <b>f</b> _init_proc             | .init  | 2             | {                           |      |        |               |          |      |                |
| f sub_8048570                   | .plt   | • 3           | <pre>setbuf(stdin, 0)</pre> | ;    |        |               |          |      |                |
| $f$ _setbuf                     | .plt   | • 4           | setbuf(stdout, 0            | );   |        |               |          |      |                |
| fgmon_start                     | .plt   | • 5           | dword_804A088 =             | 1;   |        |               |          |      |                |
| f_putchar                       | .plt   | 6 🔍           | puts("                      |      | ****   | *********\n   |          |      | Echo Server 0. |
| <u>J</u> _memset                | . p1t  | • 7           | <pre>((void (*)(void)</pre> | )((c | char * | )&loc_80487C1 | + 3))(); |      |                |
| f read                          | .prt   | 8 ●           | return 0;                   |      |        |               |          |      |                |
| f fflush                        | .pit   | 9             | }                           |      |        |               |          |      |                |
| f_strlen                        | .plt   |               |                             |      |        |               |          |      |                |
| f_printf                        | .plt   |               |                             |      |        |               |          |      |                |
| f_puts                          | .plt   |               |                             |      |        |               |          |      |                |
| f_strncmp                       | .plt   |               |                             |      |        |               |          |      |                |
| f_exit                          | .plt   |               |                             |      |        |               |          |      |                |
| f start                         | .text  |               |                             |      |        |               |          |      |                |
| J SUD_8048690                   | .text  |               |                             |      |        |               |          |      |                |
| f sub_8048710                   | . text |               |                             |      |        |               |          |      |                |

(2) 跟去这个函数,发现汇编代码很乱,有花指令插入

程序本应该跳转到loc\_80487C1+3处,但这里并没有显示出来,由此判断程序被混淆,混入了花指令,需要去除花指令。

| .text:080487B8 |              | call | _putchar                    |   |
|----------------|--------------|------|-----------------------------|---|
| .text:080487BD |              | jz   | short near ptr              | loc_80487C1+1                                   |
| .text:080487BF |              | jnz  | short near ptr              | loc_80487C1+1                                   |
| .text:080487C1 |              |      |                             |   |
| .text:080487C1 | loc_80487C1: |      |                             | ; CODE XREF: sub_804875D+60↑j                   |
| .text:080487C1 |              |      |                             | ; sub_804875D+62↑j                              |
| .text:080487C1 |              | call | near ptr <mark>915A4</mark> | B8Fh  |
| .text:080487C1 | sub_804875D  | endp | ; sp-analysis fai           | led   |
| .text:080487C1 |              |      |                             |   |
| .text:080487C6 |              |      |                             |   |
| .text:080487C6 | loc_80487C6: |      |                             | ; DMA page register 74LS612:                    |
| .text:080487C6 | _            | in   | eax, 81h                    | ; Channel 2 (diskette DMA) (address bits 16-23) |
| .text:080487C8 |              | in   | al, dx                      |   |
| .text:080487C9 |              | mov  | [eax], al                   |   |

(3) 将汇编代码转换成数据,发现0x80487C1处的字节是0xE8.

coll

| .text:080487BD |                  | jz                   | short near  | r ptr un            | k_80487C2                                     |
|----------------|------------------|----------------------|-------------|---------------------|---|
| .text:080487BD | sub_804875D      | endp ; s             | sp-analysis | <pre>failed</pre>   |   |
| .text:080487BD |                  |                      |             |                     |   |
| .text:080487BF |                  | jnz                  | short near  | <sup>,</sup> ptr un | k_80487C2                                     |
| .text:080487BF | ;                |                      |             |                     |   |
| .text:080487C1 |                  | db <mark>0E8h</mark> |             |                     |   |
| .text:080487C2 | unk_80487C2      | <b>db</b> 0C9h       |             | ;                   | CODE XREF: sub_804875D+60↑j                   |
| .text:080487C2 |                  |                      |             | ;                   | .text:080487BF↑j                              |
| .text:080487C3 |                  | db 0C3h              |             |                     |   |
| .text:080487C3 | ; } // starts at | 804875               | C           |                     |   |
| .text:080487C4 | ;unwind {        |                      |             |                     |   |
| .text:080487C4 |                  | <b>db</b> 55h        | ; U         | ;                   | CODE XREF: main+49↓p                          |
| .text:080487C5 |                  | <b>db</b> 89h        |             |                     |   |
| .text:080487C6 | ;                |                      |             |                     |   |
| .text:080487C6 |                  |                      |             |                     |   |
| .text:080487C6 | loc_80487C6:     |                      |             | ;                   | DMA page register 74LS612:                    |
| .text:080487C6 |                  | in                   | eax, 81h    | ;                   | Channel 2 (diskette DMA) (address bits 16-23) |
| .text:080487C8 |                  | in                   | al, dx      |                     |   |
| .text:080487C9 |                  | mov                  | [eax], al   |                     |   |
| .text:080487C9 | ;                |                      |             |                     | https://blog.csdn.net/weixin_45225566         |

(4)使用IDA把它patch为0x90,转换为代码,汇编代码显示正常

.text:080487BF ; -----------.text:080487C1 db 0x90 .text:080487C2 ; -----.text:080487C2 .text:080487C2 locret\_80487C2: ; CODE XREF: sub\_804875D+601j .text:080487C2 ; sub\_804875D+621j .text:080487C2 leave .text:080487C3 retn .text:080487C3 ; } // starts at 804875D .text:080487C4 ; -----.text:080487C4 ; \_\_unwind { .text:080487C4 ebp ; CODE XREF: main+49↓p push .text:080487C5 mov ebp, esp esp, 88h .text:080487C7 sub eax, large gs:14h .text:080487CD mov .text:080487D3 [ebp-0Ch], eax mov .text:080487D6 eax, eax xor .text:080487D8 mov dword ptr [esp+8], 14h .text:080487E0 dword ptr [esp+4], 0 mov eax, [ebp-70h] .text:080487E8 lea .text:080487EB mov [esp], eax .text:080487EE call \_memset .text:080487F3 .text:080487F3 loc\_80487F3: ; CODE XREF: .text:loc\_80487F3^j .text:080487F3 short near ptr loc\_80487F3+1 jmp .text:080487F3 ; ----rsch.met/web.th =45225568 (5)在上图中可以看到,0x080487F3处汇编代码也存在花指令,转换成数据后出现0xEB,也常被用于混淆

| text:080487F8    | lea eax [ebn-70b]                      |
|------------------|--|
| toxt:000407ED    |  |
| .LEX1.00040/ED   | llov [esp], eax                        |
| .text:080487EE   | call _memset                           |
| .text:080487EE ; |  |
| .text:080487F3   | db <mark>ØEBh</mark>                   |
| .text:080487F4   | db ØFFh                                |
| .text:080487F5   | db 0C0h                                |
| .text:080487F6   | db 48h ; H                             |
| .text:080487F7   | db 0C7h                                |
| .text:080487F8   | db 44h ; D                             |
| .text:080487F9   | db 24h ; \$                            |
| .text:080487FA   | db 8                                   |
| .text:080487FB   | db 14h                                 |
| .text:080487FC   | db bps://blog.csdn.net/weixin_45225566 |

(6)将0xEBpatch为0x90,汇编代码恢复为nop,但下方又出现一出标红。但是标红代码的上两行代码是无条件跳转指令,所以没有影响。

| nd - echo-server D:\课程学习\大    | 三上\RE\攻防世界\ec                      | cho-server  |                  |                | -  | o ×                  |    |
|-------------------------------|------------------------------------|---|------------------|----------------|--|----------------------|----|
| 文件(E) 编辑(E) 跳转(J) 搜索(H) 视     | 图(V)调试器 选项(C                       | 2)窗口(W)帮助   |                  |                |  |                      |    |
|                               | 🛸 🖊 🛌 🔍                            | 📼 🖬 A' 5' * 🗶 🕨 U   | ┃ 上调试器           | • •            |  |                      |    |
| 📕 库函数 📕 常规函数 📕 指令 🔜 🤅         | 数据 🔳 未知 🔲 外音                       | 18符号  |                  |                |  |                      |    |
| ☑函数窗口                         | □ # × [                            | IDA View-A  | ■       十六ì      | #制视图-1         | <ul> <li>G 结构体</li> <li>G 枚举</li> </ul>                                      |                      |    |
| 函数名称                          | 段                                  | .text:080487C2  | 1                | leave          |  |                      | ^  |
| f init proc                   | . init                             | .text:080487C3  |                  | retn           |  |                      |    |
| f sub_8048570                 | .plt                               | .text:080487C3  | ; } // starts at | 804875D        |  |                      |    |
| $f_{\text{setbuf}}$           | .plt                               | .text:080487C4  | ;                |                |  |                      |    |
| fgmon_start                   | .plt                               | .text:080487C4  |                  |                |  |                      |    |
| f MD5                         | .prt                               | .text:080487C4  | Loc_80487C4:     |                | ; CODE XREF: main+49↓p   |                      |    |
| f_memset                      | .plt                               | .text:080487C4  | ;unwina {        |                |  |                      |    |
| <u>f</u> libc_start_main      | .plt                               | .text:080487C4  | -                | ousn e         |  |                      |    |
| f_read                        | .plt                               | text:080487C7   | 1                | ub e           | up, csp  |                      |    |
| f strlen                      | . pit                              | text:080487CD   | -                | 10V e          | ax, large gs:14h   |                      |    |
| f_printf                      | .plt                               | .text:080487D3  |                  | nov [          | ebo-OChl.eax   |                      |    |
| fstack_chk_fail               | .plt                               | .text:080487D6  | ,                | kor e          |  |                      |    |
| f_puts                        | .plt                               | .text:080487D8  | n                | nov d          | word ptr [esp+8], 14h  |                      |    |
| f_strncmp                     | .plt                               | .text:080487E0  | n                | nov d          | word ptr [esp+4], 0  |                      |    |
| f start                       | . text                             | <ul> <li>.text:080487E8</li> </ul>  | 1                | lea e          | ax, [ebp-70h]  |                      |    |
| f sub_8048690                 | . text                             | <ul> <li>text:080487EB</li> </ul>   | n                | nov [          | esp], eax  |                      |    |
| f sub_80486A0                 | . text                             | <pre>.text:080487EE</pre>   | <u> </u>         | all _          | memset   |                      |    |
| f sub_8048710                 | . text                             | .text:080487F3  | r                | пор            |  |                      |    |
| f sub_8048750                 | . text                             | .text:080487F4  | i                | inc e          | ax   |                      |    |
| f main                        | . text                             | .text:080487F6  | c                | lec e          | ax   |                      |    |
| f init                        | .text                              | .text:08048/F/  | r<br>T           | nov d          | word ptr [esp+8], 14h  |                      |    |
| f fini                        | . text                             | .LEXL:080487FF  | -                | iea e          | ax, [epp-/on]  |                      |    |
| f_term_proc                   | . 1111                             | text:08048806   |                  | lov [<br>hov d | espress, eas   |                      |    |
| f putchar                     | exter                              | text:0804880D   |                  | all            | read   |                      |    |
| ₹ MD5                         | exter                              | .text:08048812  | ,                | or e           | ax. eax  |                      |    |
| f memset                      | exter                              | .text:08048814  | -                | iz s           | hort loc 804881D   |                      |    |
| flibc_start_main              | exter                              | .text:08048816  |                  | ,<br>jmp n     | ear ptr 6F448961h  |                      |    |
| f fflush                      | exter                              | .text:08048816  | ;                |                |  |                      |    |
| f strlen                      | exter                              | .text:0804881B  | c                | ib 41h;        | A  |                      |    |
| f printf                      | exter                              | .text:0804881C  | c                | ib 0           |  |                      |    |
| fstack_chk_fail               | exter                              | .text:0804881D  | ;                |                |  |                      |    |
| f strnemp                     | exter                              | .text:0804881D  |                  |                |  |                      |    |
| f exit                        | exter                              | .text:0804881D  | Loc_804881D:     |                | ; CODE XREF: .text:080488141j  |                      |    |
| 7gmon_start                   | exter                              | .text:0804881D  | п                | nov d          | word ptr [esp+8], 5  |                      |    |
|                               |                                    | .text:08048825  | r                | nov a          | word ptr [esp+4], 804881/n   |                      |    |
|                               |                                    | toxt:0004002D   |                  | iea e          |  |                      |    |
|                               |                                    | text:08048833   | "                | all [          | syl, cax   |                      |    |
|                               |                                    | text:08048838   | 1                | est e          |  |                      |    |
|                               |                                    | .text:0804883A  |                  | inz s          | hopt loc 80488A3   |                      |    |
|                               |                                    | .text:0804883C  | -                | nov d          | word ptr [esp], offset aYouAreVervClos : "You are very close! Now patch me~" |                      |    |
| <                             | >                                  |   |                  |                |  |                      |    |
| 行 21/40                       |                                    | 000007F3 080487F3:  | text:080487F3    |                |  |                      | ~  |
| ■输出窗口                         |                                    |   |                  |                |  |                      | ×  |
| IDAPython v1.7.0 final (ser   | 1a⊥ 0) (c) The                     | IDAPython Team <idapython@g< td=""><td>pogiegroups.com&gt;</td><td></td><td></td><td></td><td>^</td></idapython@g<> | pogiegroups.com> |                |  |                      | ^  |
| Dependenting type information |                                    |   |                  |                |  |                      |    |
| Fropagating type information  | n                                  | pagatod   |                  |                |  |                      |    |
| The initial autoanalysis has  | on nas veen pro<br>s been finished | haBaren   |                  |                |  |                      | ~  |
| Duthon                        | s seen rinished                    | •   |                  |                |  |                      | -  |
| All: idlo 向下 磁舟: 1350P        |                                    |   |                  |                |  |                      |    |
| NO. 1016 Pd P. WEM. 1990D     |                                    |   |                  |                | https://city.com/  | In networkin, 469265 | 12 |

(7)继续向下运行,eax被赋值为5,然后跳进loc\_80488A3,进去后发现每次eax会减一,因此这是个循环,读输入的前5个字

| .text:080488A3 |      |             |      |    | loc_80488A3: |      |                | ; ( | CODE | XREF: | .text:08048 | 83A↑j |
|----------------|------|-------------|------|----|--------------|------|----------------|-----|------|-------|-------------|-------|
| .text:080488A3 | 8D 4 | 45 <u>9</u> | 0    |    |              | lea  | eax, [ebp-70h] |     |      |       |             |       |
| .text:080488A6 | 89 🤅 | <u>34</u> 2 | 4    |    |              | mov  | [esp], eax     |     |      |       |             |       |
| .text:080488A9 | E8 5 | 52 F        | D FF | FF |              | call | _strlen        |     |      |       |             |       |
| .text:080488AE | 83 E | 8 0         | 1    |    |              | sub  | eax, 1         |     |      |       |             |       |
| .text:080488B1 | 89 4 | 14 2        | 4 04 |    |              | mov  | [esp+4], eax   |     |      |       |             |       |
| .text:080488B5 | 8D 4 | 45 <u>9</u> | 0    |    |              | lea  | eax, [ebp-70h] |     |      |       |             |       |
| .text:080488B8 | 89 ( | <u>34</u> 2 | 4    |    |              | mov  | [esp], eax     |     |      |       |             |       |
| .text:080488BB | E8 9 | ƏD F        | E FF | FF |              | call | sub_804875D    |     |      |       |             |       |
|                |      |             |      |    |              |      |                |     |      |       |             |       |

(8)回去将下面的标红代码改为nop,发现如果0x0804884F行不执行,函数就会陷入死循环。

xor eax, eax的结果一直为0,jz结果为0时跳转

-

| .text:0804881D |       |      |      |             |    |           |          | loc_804881D: |      | ; CODE XREF: .text:08048814↑j  |
|----------------|-------|------|------|-------------|----|-----------|----------|--------------|------|--|
| .text:0804881D | C7 44 | 24 6 | 98 ( | <b>95</b> ( | 90 | 00        | 00       |              | mov  | dword ptr [esp+8], 5   |
| .text:08048825 | C7 44 | 24 6 | 94 : | 17 8        | 88 | 04        | <u> </u> |              | mov  | dword ptr [esp+4], 8048817h  |
| .text:0804882D | 8D 45 | 90   |      |             |    |           |          |              | lea  | eax, [ebp-70h]   |
| .text:08048830 | 89 04 | 24   |      |             |    |           |          |              | mov  | [esp], eax   |
| .text:08048833 | E8 08 | FE F | F    | FF          |    |           |          |              | call | _strncmp   |
| .text:08048838 | 85 CØ |      |      |             |    |           |          |              | test | eax, eax   |
| .text:0804883A | 75 67 |      |      |             |    |           |          |              | jnz  | short loc_80488A3  |
| .text:0804883C | C7 04 | 24 E | 0    | 39 (        | 94 | <b>08</b> |          |              | mov  | <pre>dword ptr [esp], offset aYouAreVeryClos ; "You are very close! Now patch me~"</pre> |
| .text:08048843 | E8 E8 | FD F | F    | FF          |    |           |          |              | call | _puts  |
| .text:08048848 | A1 88 | A0 6 | 94 ( | 98          |    |           |          |              | mov  | eax, ds:dword_804A088  |
| .text:0804884D | 85 CØ |      |      |             |    |           |          |              | test | eax, eax   |
| .text:0804884F | 74 15 |      |      |             |    |           |          |              | jz   | short loc_8048866  |
| .text:08048851 |       |      |      |             |    |           |          |              |      |  |
| .text:08048851 |       |      |      |             |    |           |          | loc_8048851: |      | ; CODE XREF: .text:08048857↓j  |
| .text:08048851 | 66 B8 | EB 6 | 95   |             |    |           |          |              | mov  | ax, 5EBh   |
| .text:08048855 | 31 CØ |      |      |             |    |           |          |              | xor  | eax, eax   |
| .text:08048857 | 74 F9 |      |      |             |    |           |          |              | jz   | short near ptr loc_8048851+1   |
| .text:08048859 | 90    |      |      |             |    |           |          |              | nop  |  |
| .text:0804885A | C7 04 | 24 6 | 91 ( | 90 (        | 90 | 00        |          |              | mov  | dword ptr [esp], 1   |
| .text:08048861 | E8 EA | FD F | F    | FF          |    |           |          |              | call | _exit https://biog.csdn.net/web/n_45225566   |

(9) eax的值是根据dword\_804A088的值来决定,按x查看交叉引用,看下dword\_804A088这个地址的值是哪来的

| - | <table-cell-rows> xre</table-cell-rows> | fs t   | to dword_804A0            | 88         |                          |                          |              |         |         | $\times$               |
|---|---|--------|---------------------------|------------|--------------------------|--------------------------|--------------|---------|---------|------------------------|
| - | 方向                                      | 봋      | 地址                        | 文本         |                          |                          |              |         |         |                        |
|   | <u>課</u><br>い                           | r<br>w | .text:08048848<br>main+33 | mov<br>mov | eax, ds:dw<br>ds:dword_8 | ord_804A088<br>04A088, 1 |              |         |         |                        |
| - | <i>4</i> = 1 / 2                        |        |                           | 确定         | 取消                       | 搜索                       | 帮助           |         |         | ,                      |
|   | 15 1/2<br>08048                         | 85     |                           | 1:         |                          |                          | : CODE XREE: | .text:0 | 8048857 | 45225568<br><b>J T</b> |

(10)只有一个地方,跟过去看下,发现dword\_804A088这个地址的值是在main函数中硬编码的1

| text:0804890B<br>text:0804890E<br>text:08048913<br>text:0804891D  | mov<br>cal<br>mov<br>mov          | <pre>[esp], eax ; stream 1 _setbuf ds:dword_804A088, 1 dword ptr [esp], offset s ; "</pre>  |
|---|-----------------------------------|---|
| (11)由此可知eax的值为1,需要把jz指令patch  | 为jmp                              |   |
| 15312 冉马坦异归木乃令, 桃儿口 (令你心)且1,  |                                   |   |
| test eax,eax  |                                   |   |
| 当eax=0时,置z标志位为1,jz跳转,jnz不跳转   |                                   |   |
| 当eax=1时,置z标志位为0,jz不跳转,jnz跳转   |                                   |   |
| .text:08040836 05 07<br>.text:0804883A 75 67<br>.text:0804883C C7 04 24 E0 89 04 08<br>.text:08048843 E8 E8 FD FF FF<br>.text:08048848 A1 88 A0 04 08<br>.text:0804884D 85 C0 | jnz<br>mov<br>call<br>mov<br>test | <pre>short loc_80488A3 dword ptr [esp], offset aYouAreVeryClos ; "You are very close! Now patch me~" _puts eax, ds:dword_804A088 eax, eax</pre> |
| .text:0804884F EB 15  | jmp                               | short loc_8048866 https://bloa.csdn.net/weixin_4522556  |

(12) F5生成伪代码,可以看出就是比较输入的字符串的前五个字符与loc\_8048816+1处是否相同

```
IDA View-A
                                       伪代码
  ×
                                                         0
                                                               十六进制视
                        1unsigned int sub 80487C4()
    2 {
t
    3
       size_t v0; // eax
    4
       unsigned __int8 *v1; // ST14_4
    5
       size t v2; // eax
       char s; // [esp+18h] [ebp-70h]
    6
    7
       BYTE v5[3]; // [esp+19h] [ebp-6Fh]
       unsigned int v6; // [esp+7Ch] [ebp-Ch]
    8
    9
       v6 = readgsdword(0x14u);
 0 10
       memset(&s, 0, 0x14u);
 11
       read(0, &s, 0x14u);
 012
 • 13
       if ( !strncmp(&s, (const char *)&loc 8048816 + 1, 5u) )
   14
       {
 • 15
         puts("You are very close! Now patch me~");
         v0 = strlen(\&s);
  16 🔍
t
         v1 = (unsigned int8 *)MD5(v5, v0, 0);
 17
t
         sub_804875D(v1, 0x10u);
t
 18
t
   19
       }
t
   20
       else
t
t
   21
       {
  22
        v2 = strlen(\&s);
         sub 804875D((unsigned int8 *)&s, v2 - 1);
  23
t
       }
   24
t
i
 25
       fflush(stdout);
       return __readgsdword(0x14u) ^ v6;
1
 26
1
 27
```

(13)回去发现是我们第(6)步没有管的花指令,按D转化成数据,发现是在代码段里存了一段数据。这里不要直接改机器码,改了之后会发现找不到字符串地址。

| . LEXL. 00040000 | EO LE FU FF FF |   | Call                   | _reau                                 |
|------------------|----------------|---|------------------------|---------------------------------------|
| .text:08048812   | 33 CØ          |   | xor                    | eax, eax                              |
| .text:08048814   | 74 07          |   | jz                     | short loc_804881D                     |
| .text:08048814   |                | ; |                        |                                       |
| .text:08048816   | E9             |   | db 0 <mark>E9</mark> h |                                       |
| .text:08048817   | 46             |   | db 46h                 | ; F                                   |
| .text:08048818   | 31             |   | <b>db</b> 31h          | ; 1                                   |
| .text:08048819   | 40             |   | <b>db</b> 40h          | ; @                                   |
| .text:0804881A   | 67             |   | <b>db</b> 67h          | ; g                                   |
| .text:0804881B   | 41             |   | db 41h                 | ; A                                   |
| .text:0804881C   | 00             |   | db 0                   |                                       |
| .text:0804881D   |                | : |                        | https://blog.csdn.net/weixin_45225566 |

(14)点击编辑->修补文件->修补程序应用到输入文件,一定要保存!!!不然前面白干了。然后运行程序,输入字符 串"F1@gA",得到flag。

## root@ubuntu:/home/shiyin# ./echo-server \*\*\*\*\*\*\*\*\*\*\* Echo Server 0.3 ALPHA

\*\*\*\*\*\*\*\*\*\*

## F1@gA You are very close! Now patch me~ F8C60EB40BF66919A77C4BD8&D45DEFe4weixin\_45225566

(15)运行报错解决

如果报错 libcrypto.so.1.0.0: cannot open shared object file: No such file or directory 是因为没有 libcrypto.so.1.0.0, 我的系统有 64 位 libcrypto.so.1.0.0 但是没有 32 位的,因此需要安装 32 位的共享库。libssl 中带了 libcrypto。 命令行输入下面的指令即可

sudo apt-get install libssl1.0.0:i386

不过有的虚拟机可以,有的不行。我在kali输完还是不能运行,搞了一个多小时,试了网上各种方法都没用,换了个乌班图虚拟 机这样就行了。有懂的童鞋可以告诉一下我。



创作打卡挑战赛 赢取流量/现金/CSDN周边激励大奖