18.10.10 实验吧----逆向观察

原创

xiaoyuyulala 于 2018-10-10 11:35:39 发布 395 收藏
分类专栏： RE_WP 文章标签： 逆向观察 实验吧

这题难度是简单，也不知道真的假的，休息一下

```
aris@ubuntu:~/CTF_test/实验吧/RE$ ./rev50 xiaoyuyu
Bad ! password
                                        https://blog.csdn.net/qq_42192672
```

开始找密码的游戏

gdb动态调试，在main函数中比较函数的地方直接设置断点，会看到栈中压入了正确的密码

1.显示main函数的汇编代码：disassemble main

2.对strmp函数设置断点

3.给args参数

```
──────────────────────────────[ DISASM ]──────────────────────────────
► 0x4006df <main+146>    call   strcmp@plt <0x400530>
        s1: 0x7fffffffe1db ◂— 'xiaoyuyu'
        s2: 0x400804 ◂— 0x7000363534333231 /* '123456' */

  0x4006e4 <main+151>    test   eax, eax
  0x4006e6 <main+153>    jne    main+213 <0x400722>

  0x4006e8 <main+155>    mov    eax, dword ptr [rbp - 0x64]
  0x4006eb <main+158>    cdqe
  0x4006ed <main+160>    lea    rdx, [rax*8]
  0x4006f5 <main+168>    lea    rax, [rip + 0x202984] <0x603080>
  0x4006fc <main+175>    mov    rdx, qword ptr [rdx + rax]
  0x400700 <main+179>    lea    rax, [rbp - 0x50]
  0x400704 <main+183>    mov    rsi, rdx
  0x400707 <main+186>    mov    rdi, rax
──────────────────────────────[ STACK ]──────────────────────────────
00:0000│ rsp  0x7fffffffdc90 —▸ 0x7fffffffddf8 —▸ 0x7fffffffe1b4 ◂— 0x72612f656d6f682f ('/home/ar')
01:0008│      0x7fffffffdc98 ◂— 0x200000000
02:0010│      0x7fffffffdca0 ◂— 0xff
03:0018│      0x7fffffffdca8 ◂— 0x0
04:0020│      0x7fffffffdcb0 ◂— 'mercedes'
05:0028│      0x7fffffffdcb8 ◂— 0x0
06:0030│      0x7fffffffdcc0 ◂— 'mercedes'
07:0038│      0x7fffffffdcc8 ◂— 0xff0000000000
──────────────────────────────[ BACKTRACE ]──────────────────────────────
► f 0           4006df main+146
  f 1     7ffff7a2d830 __libc_start_main+240
                                                  https://blog.csdn.net/qq_42192672
```