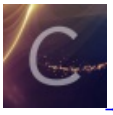
HITCON Training Lab1 Writeup

原创

人而已 于 2021-06-28 19:43:40 发布 32 收藏 1
分类专栏： CTF



对于这个程序，首先尝试运行：

```
$ ./sysmagic

Give me maigc :123
```

显然没有任何回显。

利用checksec对文件进行初步的分析：

下面对文件进行反汇编，利用IDA的反编译，可以看到这里将输入与一个随机数进行了比较：

```
  fd = open("/dev/urandom", 0);
  read(fd, &buf, 4u);
  printf("Give me maigc :");
  __isoc99_scanf("%d", &v2);
  if ( buf == v2 )
  {
    for ( i = 0; i <= 0x30; ++i )
      putchar((char)(*(&v5 + i) ^ *((_BYTE *)&v54 + i)));
  }
  return *MK_FP(__GS__, 20) ^ v67;
}
```

对应的位置如下：

```
.text:0804871A                mov     edx, [ebp+buf]
.text:0804871D                mov     eax, [ebp+var_7C]
.text:08048720                cmp     edx, eax
.text:08048722                jnz     short loc_8048760
.text:08048724                mov     [ebp+var_78], 0
.text:0804872B                jmp     short loc_8048758
```

看来如果要得到flag，必须跳过这个比较。

利用gdb来修改它：

```
[ Legend: Modified register | Code | Heap | Stack | String ]

$eax   : 0x7b
$esp   : 0xbfffef50  →  0x0804a020  →  0xb7e65370  →  <setvbuf+0> push ebp
$ebx   : 0x0
$edi   : 0xb7fb8000  →  0x001b2db0
$esi   : 0xb7fb8000  →  0x001b2db0
$eip   : 0x08048720  →  <get_flag+389> cmp edx, eax
$edx   : 0xed051dcc
$ebp   : 0xbfffefd8  →  0xbfffefe8  →  0x00000000
$eflags: [carry PARITY adjust zero SIGN trap INTERRUPT direction overflow resume
$ecx   : 0x1
$cs: 0x0073 $fs: 0x0000 $gs: 0x0033 $es: 0x007b $ss: 0x007b $ds: 0x007b

0xbfffef50|+0x0000: 0x0804a020  →  0xb7e65370  →  <setvbuf+0> push ebp   ←$esp
0xbfffef54|+0x0004: 0xb7fe98a2  →  <_dl_fixup+194> mov edi, eax
0xbfffef58|+0x0008: 0xed051dcc
0xbfffef5c|+0x000c: 0x0000007b ("{"?)
0xbfffef60|+0x0010: 0xb7fb8d60  →  0xfbad2887
0xbfffef64|+0x0014: 0x00000003
0xbfffef68|+0x0018: 0x193b07c8
0xbfffef6c|+0x001c: 0x3d100b02

    0x8048717 <get_flag+380>   add    esp, 0x10
    0x804871a <get_flag+383>   mov    edx, DWORD PTR [ebp-0x80]
    0x804871d <get_flag+386>   mov    eax, DWORD PTR [ebp-0x7c]
●→  0x8048720 <get_flag+389>   cmp    edx, eax
    0x8048722 <get_flag+391>   jne    0x8048760 <get_flag+453>
    0x8048724 <get_flag+393>   mov    DWORD PTR [ebp-0x78], 0x0
    0x804872b <get_flag+400>   jmp    0x8048758 <get_flag+445>
    0x804872d <get_flag+402>   lea    edx, [ebp-0x6f]
    0x8048730 <get_flag+405>   mov    eax, DWORD PTR [ebp-0x78]

[#0] Id 1, Name: "sysmagic", stopped 0x8048720 in get_flag (), reason: BREAKPOIN

[#0] 0x8048720 →get_flag()
[#1] 0x804879e →main()
[#2] 0xb7e1d647 →__libc_start_main(main=0x8048774 <main>, argc=0x1, argv=0xbfff
08c)
[#3] 0x80484c1 →_start()

gef➤
```


可以看到此时eax=0x7b，edx=0xed051dcc,将edx改为与eax相同的值，此时就可以得到flag：

```
gef➤ c
Continuing.
CTF{debugger_1s_so_p0werful_1n_dyn4m1c_4n4lySis!}
```