（未完）Writeup of Take the maze (reverse) in BugKu

原创

C0ss4ck 于 2017-12-12 21:47:34 发布 1135 收藏
分类专栏： Reverse_of_CTF 文章标签： bugku reverse wp 逆向 CTF

好题（可惜我还没做出来，只做到一半）

简述一下逻辑吧，首先观察程序，main函数调F5伪代码失败，看看函数尾是不是要修改栈指针。果然，修改栈指针后，跳出了F5伪代码。

观察一下main函数的逻辑：

```
memset(&v8, 0xCCu, 0x10Cu);
v11 = &savedregs ^ __security_cookie;
printf("welcome to zsctf!\n");
printf("show me your key:");
scanf("%s", input);
v3 = fkingantidebugger();                       // antidebug
if ( len(input) == 24 )
{
  input[16] ^= 1u;
  sub_1FC748(input);
  for ( i = 0; i < 24; ++i )
  {
    if ( (input[i] < 48 || input[i] > 57) && (input[i] < 97 || input[i] > 102) )// 16进制
    {
      GG();
      goto LABEL_14;
    }
  }
  if ( j_suspect(v4, input) )
  {
    printf("done!!!The flag is your input\n");
    sub_1FD9C7(4);
    j_paint();
  }
  else
  {
    GG();
  }
}
else
{
  GG();
}
LABEL_14:
sub_1FDC83(&savedregs, &dword_2058C8);
sub_1FDDAA();
return sub_1FC900(v6, v5);
}
```


开头有一个反调试，动调改跳转过了它，接下来进入一个功能不明的函数（猜测为加密函数），然后，动态调试竟然终止了……GG

然后开始静态分析，在输出'succeed'语句前的if条件中有一个函数，进入这个函数观察代码逻辑，发现三个步骤：

首先是5个case，随后是label后的11个case，走后是4个case；

发现一个可疑字符串‘delru0123456789’，且前五个case对应着数字01234，后11个case对应着56789abcdef，但是这11个case之前有个-53的操作，于是这11个case相当于分成了0，1，2，3，4，5，6，7，8，9，10这11种情况（emmm对16进制数字的操作）；

最后4个case每个case下都各自有一个函数，不难发现这四个函数中都藏有若干数组，分析逻辑后依次异或，得到由‘0’与‘1’组成的26*12的数组（应该就是map），再对4个case后所接的数值进行判断，发现惊喜——‘dlru’（down，left，right，up）

于是判断第一层case的5个字符（有个指向可疑数组的‘e’，暂时不知道是什么用途）起到了确定方向的作用，而第二层case的11个字符则是代表着步长，从0道10

```
inpt = key[read1];                // delru0123456789
a1 = inpt - 100;
inpt -= 100;
switch ( inpt )
{
  case 0:                         // rawcnt=100 down
    unk1(&v7, key[read2] - 48);
    continue;
  case 17:                        // rawcnt=117 up
    unk2(&v7, key[read2] - 48);
    continue;
  case 8:                         // rawcnt=108 left
    unk3(&v7, key[read2] - 48);
    continue;
  case 14:                        // rawcnt=114 right
    unk4(&v7, key[read2] - 48);
    continue;
```


成功逆推出走迷宫路径代表的字符串，接下来，就要直面一开始碰到的加密函数了。

```
   [1,  1,  0,  0,  0,  0,  0,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1]
[0,  0,  1,  0,  1,  1,  1,  0,  1,  1,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  1,  1,  1,  1,  1,
 1,  0,  0,  0,  1,  1,  1,  0,  1,  1,  0,  1,  1,  1,  1,  1,  1,  1,  1,  1,  0,  1,  1,  1,  1,  1,
 0,  0,  1,  1,  1,  1,  1,  0,  0,  0,  0,  0,  1,  1,  1,  1,  1,  0,  0,  1,  0,  1,  1,  1,  1,  1,
 1,  0,  0,  1,  1,  1,  1,  1,  1,  1,  1,  0,  1,  1,  1,  1,  1,  1,  0,  1,  1,  1,  1,  1,  1,  1,
 1,  1,  0,  0,  0,  0,  0,  0,  0,  1,  1,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  1,  1,  1,  1,  1,
 1,  1,  1,  1,  0,  1,  1,  1,  0,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  0,  1,  1,  1,  1,  1,
 1,  1,  1,  1,  0,  1,  1,  1,  0,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  0,  1,  1,  1,  1,  1,
 1,  1,  1,  1,  0,  1,  1,  1,  0,  0,  0,  0,  0,  1,  1,  1,  1,  1,  1,  0,  0,  1,  1,  1,  1,  1,
 1,  1,  1,  1,  0,  1,  1,  1,  1,  1,  1,  1,  0,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,
 1,  1,  1,  1,  0,  1,  1,  1,  1,  1,  1,  1,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  1,  1,  1,  1,
[1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  1,  0,  0,  0,  0,  0
```


GG，果然没怼出来。悄悄问了一波学长，学长说硬怼字节码解析什么的太浪费时间（手动滑稽），不如来一发爆破啊（恍然大悟脸）

（复习四级去了，四级考完去爆破）

（未完待·续）