2016 华山杯 Writeup

原创

0x4C43 于 2016-09-13 09:40:56 发布 1120 收藏

分类专栏： CTF 逆向工程 文章标签： 华山杯 writeup reverse CTF

Reverse7 移动迷宫

Value: 200
Description: 当赶到的时候发现对方已经提前接头了，但在现场遗留了一个 U 盘并恢复出了一个登陆程序，如何才能拿到密钥？

题目为走迷宫的形式。IDA中F5查看伪代码，程序先将输入的字符串通过locate函数进行变换。

```
printf_s("[*] To get the flag, you need to input a correct string.\n\n");
scanf_s("%s", str, 25);
while ( strlen(str) != 24 )
{
  v3 = __iob_func();
  fflush(v3);
  printf_s("\n[*] Please Input a string with 24 characters!\n\n");
  scanf_s("%s", str, 25);
}
for ( times = 0; times < 4; ++times )
  locate(&str[6 * times], &step[6 * times]);
```

locate函数将输入字符串str的字符与二维数组table中的字符进行匹配，并返回各字符在数组中所在的列号（1,2,3,4），这些整数代表移动方向：1—>up；2–>down；3–>left；4–>right。

```
void __cdecl locate(char *str, char *a)
{
  int col_t; // [sp+0h] [bp-8h]@1
  int row_t; // [sp+4h] [bp-4h]@1

  col_t = 0;
  for ( row_t = 0; row_t < 6; ++row_t )
  {
    while ( col_t < 4 )
    {
      if ( str[row_t] == *(&table[4 * row_t] + col_t) )
      {
        a[row_t] = col_t + 1;
        break;
      }
      ++col_t;
    }
    col_t = 0;
  }
}
```

```
.data:0040E000 ; _BYTE table[24]
.data:0040E000 ?table@@3PAY03DA db '0','A','1','B'     ; DATA XREF: locate(char *,uchar *)+3A↑r
.data:0040E000                  db 'a','2','b','3'
.data:0040E000                  db '4','C','5','D'
.data:0040E000                  db 'c','6','d','7'
.data:0040E000                  db '8','E','9','F'
.data:0040E000                  db 'e','0','f','1'
```

具体移动的逻辑实现如下：根据locate返回的整数序列移动横纵坐标。二维数组route中的字符代表路径：“#”代表通路，“*”代表障碍物，初始位置为（3,0），终点为（9,8）。

```
.data:0040E018 ; char (* route)[10]
.data:0040E018 ?route@@3PAY09DA db '*','*','*','*','*','*','*','*','*','*'
.data:0040E018                                          ; DATA XREF: _main+150↑r
.data:0040E018                  db '*','#','#','#','#','*','*','*','*','*'
.data:0040E018                  db '*','#','*','*','#','*','*','*','*','*'
.data:0040E018                  db '#','#','*','#','#','*','*','*','*','*'
.data:0040E018                  db '*','*','*','#','*','*','*','*','*','*'
.data:0040E018                  db '*','*','*','#','*','#','#','#','#','#'
.data:0040E018                  db '*','*','*','#','#','#','*','*','*','#'
.data:0040E018                  db '*','*','*','*','*','*','*','*','*','#'
.data:0040E018                  db '*','*','*','*','*','*','*','*','*','#'
.data:0040E018                  db '*','*','*','*','*','*','*','*','#','#'
```

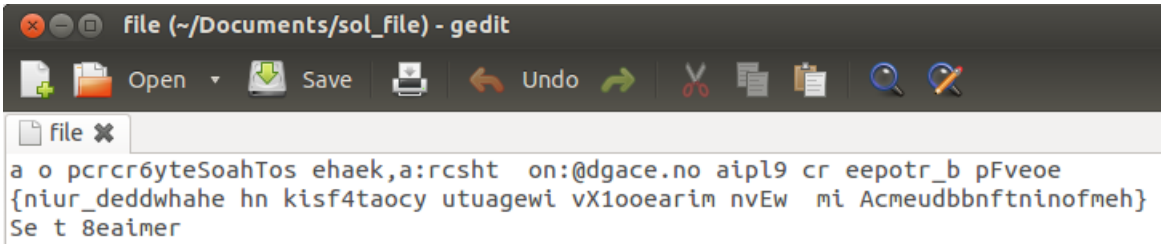
```
33  while ( n < 24 )
34  {
35    switch ( step[n] )
36    {
37      case 1:
38        --row_r;
39        break;
40      case 2:
41        ++row_r;
42        break;
43      case 3:
44        --col_r;
45        break;
46      case 4:
47        ++col_r;
48        break;
49      default:
50        break;
51    }
```

根据以上分析，step数组的值应为4114 4422 3222 4414 4442 2223才能走到终点，映射到table数组中的字符为Ba47F1A256E0B347F1B2C6Ef，所以最终的flag是flag_Xd{hSh_ctf:Ba47F1A256E0B347F1B2C6Ef}。

Misc1 Try Everything

Value:200
Description:
try everything you can to get flag, and DO NOT ASK MANAGER THE FLAG.

解压文件打开能看到一串乱序字符串，其中包含组成flag的“{”“}”等字符。



用binwalk查看可知，file文件由文件名为0~163的164个小文件组成。

```
superlee@ubuntu:~/Documents/sol_file$ binwalk file

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             gzip compressed data, has original file name: "24", from Unix, last modified: 2016-09-10 10:19:40
24            0x18            gzip compressed data, has original file name: "72", from Unix, last modified: 2016-09-10 10:19:40
48            0x30            gzip compressed data, has original file name: "108", from Unix, last modified: 2016-09-10 10:19:40
73            0x49            gzip compressed data, has original file name: "129", from Unix, last modified: 2016-09-10 10:19:40
98            0x62            gzip compressed data, has original file name: "18", from Unix, last modified: 2016-09-10 10:19:40
122           0x7A            gzip compressed data, has original file name: "92", from Unix, last modified: 2016-09-10 10:19:40
146           0x92            gzip compressed data, has original file name: "63", from Unix, last modified: 2016-09-10 10:19:40
170           0xAA            gzip compressed data, has original file name: "162", from Unix, last modified: 2016-09-10 10:19:40
195           0xC3            gzip compressed data, has original file name: "110", from Unix, last modified: 2016-09-10 10:19:40
220           0xDC            gzip compressed data, has original file name: "156", from Unix, last modified: 2016-09-10 10:19:40
245           0xF5            gzip compressed data, has original file name: "132", from Unix, last modified: 2016-09-10 10:19:40
270           0x10E           gzip compressed data, has original file name: "101", from Unix, last modified: 2016-09-10 10:19:40
295           0x127           gzip compressed data, has original file name: "34", from Unix, last modified: 2016-09-10 10:19:40
319           0x13F           gzip compressed data, has original file name: "143", from Unix, last modified: 2016-09-10 10:19:40
344           0x158           gzip compressed data, has original file name: "28", from Unix, last modified: 2016-09-10 10:19:40
368           0x170           gzip compressed data, has original file name: "136", from Unix, last modified: 2016-09-10 10:19:40
393           0x189           gzip compressed data, has original file name: "115", from Unix, last modified: 2016-09-10 10:19:40
418           0x1A2           gzip compressed data, has original file name: "114", from Unix, last modified: 2016-09-10 10:19:40
```

重新排序即得到flag。

```
# binwalk file.gz | awk -F '"' '{print $2}'
offset=[24,72,108,129,18,92,63,162,110,156,132,101,34,143,28,136,115,114,17,14,69,10,7,11,127,55,58,86,

s="a o pcrcr6yteSoahTos ehaek,a:rcsht  on:@dgace.no aipl9 cr eepotr_b pFveoe{niur_deddwhahe hn kisf4tao

result = ''.join([s[offset.index(x)] for x in range(len(s))])
print result
```

```
superlee@ubuntu:~/Documents/sol_file$ python file.py
Since the eavesdropper have obtained our communication key, therefore we have ad
opted a new communication program.This is our new key:flag_Xd{hSh_ctf:4Ea9F16bA8
b@c}
```