

攻防世界 reverse之 elrond32

原创

qq_42728977 于 2020-03-18 14:36:39 发布 1134 收藏 1

分类专栏: [reverse](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_42728977/article/details/104944014

版权



[reverse](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

elrond32

难度系数: 1

题目来源: [tinyctf-2014](#)

思路:

因为题目很简单直接放进IDA32里面

```
1 int __cdecl main(int a1, char **key)
2 {
3     if ( a1 > 1 && sub_8048414(key[1], 0) )
4     {
5         puts("Access granted");
6         sub_8048538((int)key[1]);
7     }
8     else
9     {
10        puts("Access denied");
11    }
12    return 0;
13 }
```

https://blog.csdn.net/qq_42728977

进入sub_8048414函数瞅瞅

```
1 signed int __cdecl sub_8048414(_BYTE *key, int a2)
2 {
3     signed int result; // eax
4
5     switch ( a2 )
6     {
7     case 0:
8         if ( *key == 105 )
9             goto LABEL_19;
10        result = 0;
11        break;
12    case 1:
13        if ( *key == 101 )
14            goto LABEL_19;
15        result = 0;
16    }
```

```

16     break;
17 case 3:
18     if ( *key == 110 )
19         goto LABEL_19;
20     result = 0;
21     break;
22 case 4:
23     if ( *key == 100 )
24         goto LABEL_19;
25     result = 0;
26     break;
27 case 5:
28     if ( *key == 97 )
29         goto LABEL_19;
30     result = 0;
31     break;
32 case 6:
33     if ( *key == 103 )
34         goto LABEL_19;
35     result = 0;
36     break;

```

00000414 sub_8048414:1 (8048414)

https://blog.csdn.net/qq_42728977

```

25     result = 0;
26     break;
27 case 5:
28     if ( *key == 97 )
29         goto LABEL_19;
30     result = 0;
31     break;
32 case 6:
33     if ( *key == 103 )
34         goto LABEL_19;
35     result = 0;
36     break;
37 case 7:
38     if ( *key == 115 )
39         goto LABEL_19;
40     result = 0;
41     break;
42 case 9:
43     if ( *key == 114 )
44 LABEL_19:
45     result = sub_8048414(key + 1, 7 * (a2 + 1) % 11);
46     else
47     result = 0;
48     break;
49 default:
50     result = 1;
51     break;
52 }
53 return result;
54 }

```

https://blog.csdn.net/qq_42728977

分析出题目的大致思路就是验证key然后打印flag

重点在如何确定key，通过分析，key是根据a2再在case里确定，所以先确定a2.

```

>>> for i in range(9):
...     a2=7*(a2+1)%11
...     print a2
...
7
1
3
6

```

快捷
链接
自定
插入

```
5 , 7 * ( 2 + 1 ) % 11);
9
4
2
10
```

https://blog.csdn.net/qq_42728977

由于case只有12345679，其余的就default，return1，所以a2有10个值，再看flah输出函数，可以看到，只需要前8个，所以我们手动根据case找到前八个，

```
>>> key=[105,115,101,110,103,97,114,100]
```

```
1 int __cdecl sub_8048538(int a1)
2 {
3     int v2[33]; // [esp+18h] [ebp-A0h]
4     int i; // [esp+9Ch] [ebp-1Ch]
5
6     memcpy(v2, &unk_8048760, sizeof(v2));
7     for ( i = 0; i <= 32; ++i )
8         putchar(v2[i] ^ *(char *)(a1 + i % 8));
9     return putchar(10);
10 }
```

https://blog.csdn.net/qq_42728977

直接写出对应的python代码即可

```
key=[105,115,101,110,103,97,114,100]
v2=[0x0F,0x1F,0x04,0x09,0x1C,0x12,0x42,0x09,0x0C,0x44,0x0D,0x07,0x09,0x06,0x2D,0x37,0x59,0x1E,0x00,0x59,0x0F,0x08,0x1C,0x23,0x36,0x07,0x55,0x02,0x0C,0x08,0x41,0x0A,0x14]
a=''
for i in range(33):
    a+=chr(v2[i]^key[(i%8)])
print(a)
```

得到flag

flag{s0me7hing_S0me7hinG_t0lki3n}



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)