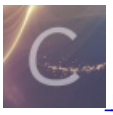
攻防世界 reverse之 elrond32

原创

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

分类专栏： reverse

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



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

```
int __cdecl main(int a1, char **key)
{
  if ( a1 > 1 && sub_8048414(key[1], 0) )
  {
    puts("Access granted");
    sub_8048538((int)key[1]);
  }
  else
  {
    puts("Access denied");
  }
  return 0;
}
```


进入sub_8048414函数瞅瞅

```
signed int __cdecl sub_8048414(_BYTE *key, int a2)
{
  signed int result; // eax

  switch ( a2 )
  {
    case 0:
      if ( *key == 105 )
        goto LABEL_19;
      result = 0;
      break;
    case 1:
      if ( *key == 101 )
        goto LABEL_19;
      result = 0;
```

```
      break;
    case 3:
      if ( *key == 110 )
        goto LABEL_19;
      result = 0;
      break;
    case 4:
      if ( *key == 100 )
        goto LABEL_19;
      result = 0;
      break;
    case 5:
      if ( *key == 97 )
        goto LABEL_19;
      result = 0;
      break;
    case 6:
      if ( *key == 103 )
        goto LABEL_19;
      result = 0;
      break;
```

00000414 sub_8048414:1 (8048414)


```
      result = 0;
      break;
    case 5:
      if ( *key == 97 )
        goto LABEL_19;
      result = 0;
      break;
    case 6:
      if ( *key == 103 )
        goto LABEL_19;
      result = 0;
      break;
    case 7:
      if ( *key == 115 )
        goto LABEL_19;
      result = 0;
      break;
    case 9:
      if ( *key == 114 )
LABEL_19:
        result = sub_8048414(key + 1, 7 * (a2 + 1) % 11);
      else
        result = 0;
      break;
    default:
      result = 1;
      break;
  }
  return result;
}
```


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
```

```
5
9
4
2
10
```


由于case只有12345679，其余的就defult，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   qmemcpy(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 }
```


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,0x0
8,0x1C,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}