XCTF-elrond32

原创

Lu1u~ 于 2021-06-24 16:32:50 发布 56 收藏 1

分类专栏： CTF-RE练习

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_52974719/article/details/118190782

版权

CTF-RE练习 专栏收录该内容

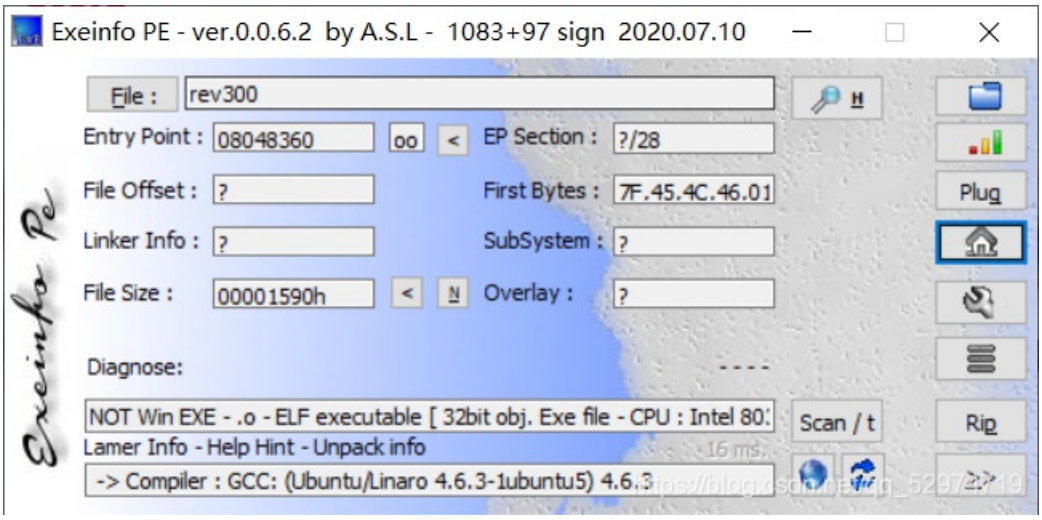
9 篇文章 2 订阅

订阅专栏

XCTF-elrond32

1、查壳

无壳，**32位ELF文件**



2、ida静态分析

```
int __cdecl main(int a1, char **a2)
{
  if ( a1 > 1 && sub_8048414(a2[1], 0) )        // 获得key
  {
    puts("Access granted");
    sub_8048538((int)a2[1]);                    // 处理函数
  }
  else
  {
    puts("Access denied");
  }
  return 0;
}
```

https://blog.csdn.net/qq_52974719

主要由两个函数组成，**sub_8048414**用来验证**key**，**sub_8048538**函数用来进行与**key**的的异或加密。

sub_8048141函数:


```
        goto LABEL_19;
      result = 0;
      break;
    case 4:
      if ( *a1 == 100 )
        goto LABEL_19;
      result = 0;
      break;
    case 5:
      if ( *a1 == 97 )
        goto LABEL_19;
      result = 0;
      break;
    case 6:
      if ( *a1 == 103 )
        goto LABEL_19;
      result = 0;
      break;
    case 7:
      if ( *a1 == 115 )
        goto LABEL_19;
      result = 0;
      break;
    case 9:
      if ( *a1 == 114 )
LABEL_19:
        result = sub_8048414(a1 + 1, 7 * (a2 + 1) % 11);// 递归调用
      else
        result = 0;
      break;
    default:
      result = 1;
      break;
  }
  return result;
```

https://blog.csdn.net/qq_52974719

一开始传入一个二维数组的行指针和**0**，里面直接进行一个**switch**和**case**的判断，由**0**进入则可以知道***a1==105**即**key**的第一个元素的**ASCII**码为**105**，之后跳转到**label19**处，传入**a1+1**和一个生产关键码的运算。

```python
a2=0
for i in range(7):
    a2 = 7 * (a2 + 1) % 11
    print(a2,end=' ')
#最终遍历顺序为0 7 1 3 6 5 9 4
print()
key=[105,115,101,110,103,97,114,100]
```

根据这个生产关键码的算法依次得到key的每个元素。

提取密文获得flag

sub_8048538函数

```
1 int __cdecl sub_8048538(int a1)
2 {
3   int v2[33]; // [esp+18h] [ebp-A0h] BYREF
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);
0 }
```

https://blog.csdn.net/qq_52974719

主要内容是将unk_8048760字符串的值存到v2里，依次与key异或。可知密文字符串每个元素为字符型，占一个字节，而v2开辟的是int型的数组，所以其中3个字节会用0来填充，写脚本提出就好。

```
.rodata:08048748                    align 20h
.rodata:08048760 unk_8048760        db  0Fh                 ; DATA XREF: sub_804
.rodata:08048761                    db    0
.rodata:08048762                    db    0
.rodata:08048763                    db    0
.rodata:08048764                    db  1Fh
.rodata:08048765                    db    0
.rodata:08048766                    db    0
.rodata:08048767                    db    0
.rodata:08048768                    db    4
.rodata:08048769                    db    0
.rodata:0804876A                    db    0
.rodata:0804876B                    db    0
.rodata:0804876C                    db    9
.rodata:0804876D                    db    0
.rodata:0804876E                    db    0
.rodata:0804876F                    db    0
.rodata:08048770                    db  1Ch
.rodata:08048771                    db    0
.rodata:08048772                    db    0
.rodata:08048773                    db    0
.rodata:08048774                    db  12h
.rodata:08048775                    db    0
.rodata:08048776                    db    0
.rodata:08048777                    db    0
.rodata:08048778                    db  42h ; B
.rodata:08048779                    db    0
.rodata:0804877A                    db    0
.rodata:0804877B                    db    0
.rodata:0804877C                    db    9
.rodata:0804877D                    db    0
.rodata:0804877E                    db    0
.rodata:0804877F                    db    0
```

用来填充

https://blog.csdn.net/qq_52974719

```
key=[105,115,101,110,103,97,114,100]
str=[15,   0,   0,   0,  31,   0,   0,   0,   4,   0,
    0,   0,   9,   0,   0,   0,  28,   0,   0,   0,
   18,   0,   0,   0,  66,   0,   0,   0,   9,   0,
    0,   0,  12,   0,   0,   0,  68,   0,   0,   0,
   13,   0,   0,   0,   7,   0,   0,   0,   9,   0,
    0,   0,   6,   0,   0,   0,  45,   0,   0,   0,
   55,   0,   0,   0,  89,   0,   0,   0,  30,   0,
    0,   0,   0,   0,   0,   0,  89,   0,   0,   0,
   15,   0,   0,   0,   8,   0,   0,   0,  28,   0,
    0,   0,  35,   0,   0,   0,  54,   0,   0,   0,
    7,   0,   0,   0,  85,   0,   0,   0,   2,   0,
    0,   0,  12,   0,   0,   0,   8,   0,   0,   0,
   65,   0,   0,   0,  10,   0,   0,   0,  20,   0,
    0,   0]
c=[]
for i in range(len(str)//4):
    c.append(str[4*i])
for i in range(len(c)):
        print(chr(c[i]^key[i%8]),end='')
#flag{s0me7hing_S0me7hinG_t0lki3n}
```

完结线:re弟弟的做题笔记，有时可能会带点稀奇古怪的思路，如有问题还望师傅们指正，专栏内容会随着比赛记录而不断更新哦。爬~