攻防世界 四（进阶篇）catch-me

原创

chan3301 于 2019-06-13 23:54:47 发布 1093 收藏

分类专栏： 逆向题目练习 文章标签： 攻防世界 逆向

本文链接：https://blog.csdn.net/sjt670994562/article/details/91909582

逆向题目练习 专栏收录该内容

16 篇文章 1 订阅

订阅专栏

后来做题速度完全掉了下去，主要是因为基础太差，不管是c、python语言基础，还是汇编基础，还是linux使用，shell脚本的编写，都差太多，所以经过这几天的冲刺，我打算从基础开始，不急于求成，题会做，但不会那么着急了，太急了学的东西也是没用的，这是这几天卡在这道题上，以及同学对我的一些批评总结出来的一些观点。

catch-me

分析，不是elf不是exe，扔到C32Asm，看到头文件 FD 37 7A 58，这里是看到网上的方法，可以用python的magic函数，这里补上连接

https://blog.csdn.net/diyiday/article/details/80571179

```
>>> magic.from_file("Catch__Me")
'XZ compressed data'
```

xz文件

通过tar -Jxf linux-3.12.tar.xz（其实这里直接windows换zip扩展名就行）

经过两次解压，就出来了我们要分析的文件，扔到ida，这一次分析，我真正的认识到了自己的不足，所以后面还需要再学习。

从尾部看起吧，发现haystck是关键，如果条件不满足，其最终的值会变成假flag，bad

```
if ( _mm_cvtsi128_si32(_mm_add_epi32(v14, _mm_srli_si128(v14, 4))) != 2388 )
{
  *(_DWORD *)haystack = '_dab';
  *(_DWORD *)&haystack[4] = '_dab';
  *(_DWORD *)&haystack[8] = '_dab';
  *(_DWORD *)&haystack[12] = '_dab';
  *(_QWORD *)&xmmword_601290 = '_dab_dab';
  BYTE7(xmmword_601290) = 0;
}
printf("Flag: ASIS{%s}\n", haystack);
if ( strstr(haystack, "bad_") )
  puts("this flag is absolutely fake ");
return 0LL;
}
```


这一处，经过汇编一步一步的看，就是对变化了的haystack与xmmword_601290里面以字节为单位全部都相加起来，对haystack没影响，继续往上看。这里将haystack进行了变化，并且是byte_6012A8八位一循环。

```
do
{
```

```
    haystack[v4] ^= byte_6012A8[v4 & 7];
    ++v4;
  }
  while ( v4 != 33 );
```

下面是异或的几个值，就是我们要求的几个关键的值，求出他们来，就ok了，前四位通过调试可以比较容易的出来是主要是6012AC这一个未知值，需要我们设置变量

```
byte_6012A8[0] = HIBYTE(v3);
byte_6012A9 = BYTE2(v3) & 0xFD;
byte_6012AA = BYTE1(v3) & 0xDF;
byte_6012AB = v3 & 0xBF;
```

```
dword_6012AC = *
```

这里用到了一个函数getenv，这个是获取环境字符串，ASIS与CTF是相应的环境变量，这里我们在linux里面用export对环境变量进行设置，创建这两个变量。根据下面这个式子，我们可以得出ASIS&&CTF的值是0x4ff2da0a

```
if ( getenv("ASIS") && (*(_DWORD *)getenv("CTF") ^ v3) != 0xFEEBFEEB )
```

```
a=0xFEEBFEEB^0xB11924E1
print(hex(a))
```

然后设置环境变量，运行，flag就出来啦

```
export ASIS="$(printf "\x0a\xda\xf2\x4f")"    #注意参数是从低位到高位的
export CTF="$(printf "\x0a\xda\xf2\x4f")"
```

```
root@kali:~/ida# export ASIS="$(printf "\x0a\xda\xf2\x4f")"
root@kali:~/ida# export CTF="$(printf "\x0a\xda\xf2\x4f")"
root@kali:~/ida# ./linux_server64
IDA Linux 64-bit remote debug server(ST) v1.22. Hex-Rays (c) 2004-2017
Listening on 0.0.0.0:23946...
=============================================================
[1] Accepting connection from 192.168.30.1...
Flag: ASIS{600d_j0b_y0u_4r3_63771n6_574r73d}
```

这道题难度不大，但是因为之前做题对wp依赖性太大以至于有了拐棍，再加上基础不牢，就做了很长时间，所以后面做题速度要减慢，好好研究基础，明白原理，脱离拐棍，才能有真的提高