攻防世界 逆向 Shuffle

原创

与日平肩以头抢地 于 2020-02-26 10:23:31 发布 536 收藏

分类专栏： 逆向 文章标签： 安全

本文链接：https://blog.csdn.net/fool_best/article/details/104511153

逆向 专栏收录该内容

12 篇文章 0 订阅

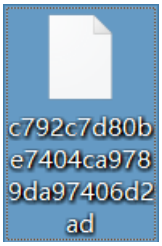
订阅专栏

攻防世界 逆向 Shuffle

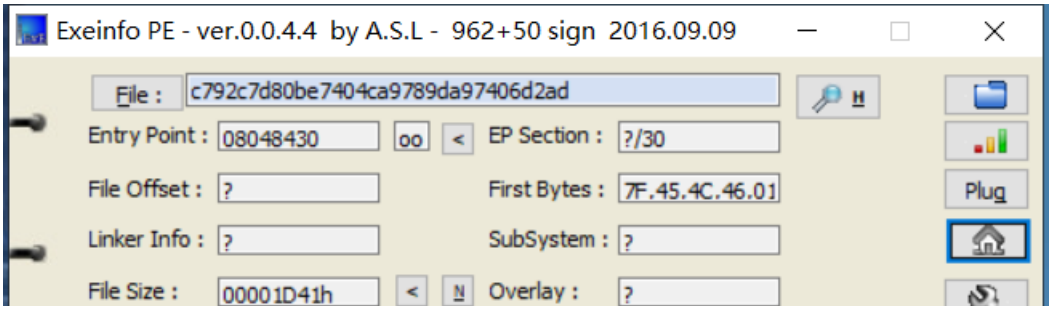
（原创）

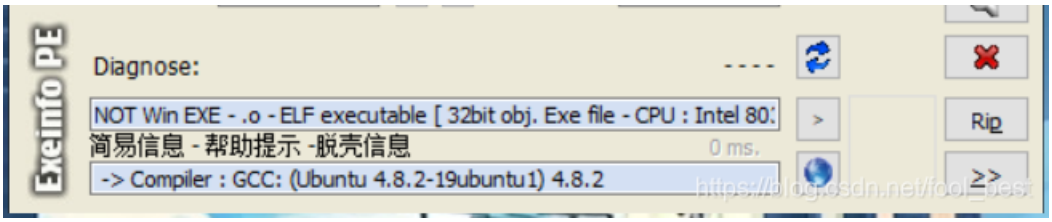
原题如下：

下载文件

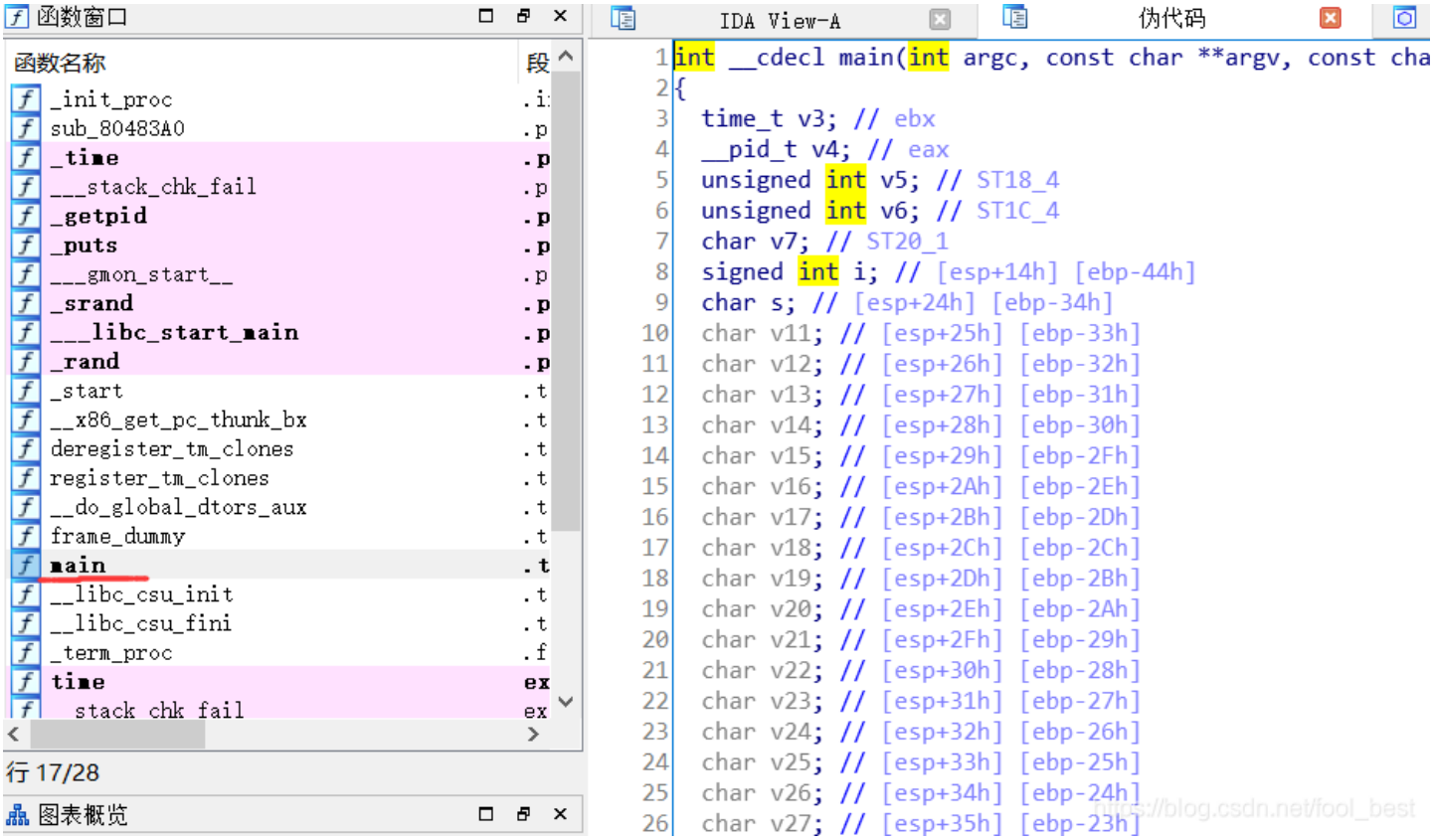


查看脱壳信息





用IDA打开查看main函数



关键源代码如下：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  time_t v3; // ebx
  __pid_t v4; // eax
  unsigned int v5; // ST18_4
  unsigned int v6; // ST1C_4
  char v7; // ST20_1
  signed int i; // [esp+14h] [ebp-44h]
  char s; // [esp+24h] [ebp-34h]
  char v11; // [esp+25h] [ebp-33h]
  char v12; // [esp+26h] [ebp-32h]
  char v13; // [esp+27h] [ebp-31h]
  char v14; // [esp+28h] [ebp-30h]
  char v15; // [esp+29h] [ebp-2Fh]
  char v16; // [esp+2Ah] [ebp-2Eh]
  char v17; // [esp+2Bh] [ebp-2Dh]
  char v18; // [esp+2Ch] [ebp-2Ch]
  char v19; // [esp+2Dh] [ebp-2Bh]
  char v20; // [esp+2Eh] [ebp-2Ah]
  char v21; // [esp+2Fh] [ebp-29h]
  char v22; // [esp+30h] [ebp-28h]
  char v23; // [esp+31h] [ebp-27h]
  char v24; // [esp+32h] [ebp-26h]
  char v25; // [esp+33h] [ebp-25h]
```

```
char v26; // [esp+34h] [ebp-24h]
char v27; // [esp+35h] [ebp-23h]
char v28; // [esp+36h] [ebp-22h]
char v29; // [esp+37h] [ebp-21h]
char v30; // [esp+38h] [ebp-20h]
char v31; // [esp+39h] [ebp-1Fh]
char v32; // [esp+3Ah] [ebp-1Eh]
char v33; // [esp+3Bh] [ebp-1Dh]
char v34; // [esp+3Ch] [ebp-1Ch]
char v35; // [esp+3Dh] [ebp-1Bh]
char v36; // [esp+3Eh] [ebp-1Ah]
char v37; // [esp+3Fh] [ebp-19h]
char v38; // [esp+40h] [ebp-18h]
char v39; // [esp+41h] [ebp-17h]
char v40; // [esp+42h] [ebp-16h]
char v41; // [esp+43h] [ebp-15h]
char v42; // [esp+44h] [ebp-14h]
char v43; // [esp+45h] [ebp-13h]
char v44; // [esp+46h] [ebp-12h]
char v45; // [esp+47h] [ebp-11h]
char v46; // [esp+48h] [ebp-10h]
char v47; // [esp+49h] [ebp-Fh]
char v48; // [esp+4Ah] [ebp-Eh]
char v49; // [esp+4Bh] [ebp-Dh]
unsigned int v50; // [esp+4Ch] [ebp-Ch]

v50 = __readgsdword(0x14u);
s = 83;
v11 = 69;
v12 = 67;
v13 = 67;
v14 = 79;
v15 = 78;
v16 = 123;
v17 = 87;
v18 = 101;
v19 = 108;
v20 = 99;
v21 = 111;
v22 = 109;
v23 = 101;
v24 = 32;
v25 = 116;
v26 = 111;
v27 = 32;
v28 = 116;
v29 = 104;
v30 = 101;
v31 = 32;
v32 = 83;
v33 = 69;
v34 = 67;
v35 = 67;
v36 = 79;
v37 = 78;
v38 = 32;
v39 = 50;
v40 = 48;
v41 = 49;
```

```
  v42 = 52;
  v43 = 32;
  v44 = 67;
  v45 = 84;
  v46 = 70;
  v47 = 33;
  v48 = 125;
  v49 = 0;
  v3 = time(0);
  v4 = getpid();
  srand(v3 + v4);
  for ( i = 0; i <= 99; ++i )
  {
    v5 = rand() % 0x28u;
    v6 = rand() % 0x28u;
    v7 = *(&s + v5);
    *(&s + v5) = *(&s + v6);
    *(&s + v6) = v7;
  }
  puts(&s);
  return 0;
}
```

写出C++源代码。
源字符串即从s，v11，v12到v47，v48。

```cpp
#include<iostream>
#include<string>
using namespace std;

int main()
{
    char arr[40] = { 83, 69, 67, 67, 79, 78, 123, 87, 101, 108, 99, 111, 109, 101, 32, 116, 111, 32,
        116, 104, 101, 32, 83, 69, 67, 67, 79, 78, 32, 50, 48, 49, 52, 32, 67, 84, 70, 33, 125 };
    for(int i = 0;i < 40;i++) {
        cout << arr[i];
    }
    return 0;
}
```


运行得到flag。

```
SECCON{Welcome to the SECCON 2014 CTF!}
```

flag：SECCON{Welcome to the SECCON 2014 CTF!}