攻防世界 Reverse高手进阶区 2分题 secret-galaxy-300

原创

思源湖的鱼 于 2020-12-08 13:25:17 发布 189 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 reverse

本文链接：https://blog.csdn.net/weixin_44604541/article/details/110871100

前言

继续ctf的旅程

攻防世界Reverse高手进阶区的2分题

本篇是secret-galaxy-300的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

PE查壳

扔进IDA

不断跟踪

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
```

```
  __main();
  fill_starbase(&starbase);
  print_starbase(&starbase);
  return 0;
}
```

```
void __cdecl fill_starbase(int a1)
{
  signed int i; // [esp+8h] [ebp-10h]
  int v2; // [esp+Ch] [ebp-Ch]

  v2 = 0;
  for ( i = 0; i <= 4; ++i )
  {
    *(_DWORD *)(a1 + 24 * i) = galaxy_name[i];
    *(_DWORD *)(24 * i + a1 + 4) = rand();
    *(_DWORD *)(24 * i + a1 + 8) = 0;
    *(_DWORD *)(24 * i + a1 + 12) = 0;
    *(_DWORD *)(24 * i + a1 + 16) = 24 * (i + 1) + a1;
    *(_DWORD *)(a1 + 24 * i + 20) = v2;
    v2 = 24 * i + a1;
  }
}
```



```
int __cdecl print_starbase(int a1)
{
  int result; // eax
  const char *v2; // edx
  signed int i; // [esp+1Ch] [ebp-Ch]

  puts("--------------GALAXY DATABASE-------------");
  printf("%10s | %s | %s\n", "Galaxy name", "Existence of life", "Distance from Earth");
  result = puts("------------------------------------------");
  for ( i = 0; i <= 4; ++i )
  {
    if ( *(_DWORD *)(24 * i + a1 + 8) == 1 )
      v2 = "INHABITED";
    else
      v2 = "IS NOT INHABITED";
    result = printf("%11s | %17s | %d\n", *(_DWORD *)(24 * i + a1), v2, *(_DWORD *)(24 * i + a1 + 4));
  }
  return result;
}
```



```
.data:00409000                 public _galaxy_name
.data:00409000 _galaxy_name    dd offset aNgs2366       ; DATA XREF: _fill_starbase+30↑r
.data:00409000                                         ; "NGS 2366"
.data:00409004 off_409004      dd offset aAndromeda     ; DATA XREF: ___libc_csu_gala+36↑r
.data:00409004                                         ; ___libc_csu_gala+60↑r ...
.data:00409004                                         ; "Andromeda"
.data:00409008 off_409008      dd offset aMessier       ; DATA XREF: ___libc_csu_gala+52↑r
.data:00409008                                         ; ___libc_csu_gala+7C↑r ...
.data:00409008                                         ; "Messier"
.data:0040900C off_40900C      dd offset aSombrero      ; DATA XREF: ___libc_csu_gala+AD↑r
.data:0040900C                                         ; "Sombrero"
.data:00409010 off_409010      dd offset aTriangulum    ; DATA XREF: ___libc_csu_gala+44↑r
.data:00409010                                         ; ___libc_csu_gala+EC↑r ...
.data:00409010                                         ; "Triangulum"
.data:00409014 off_409014      dd offset aDarkSecretGala
.data:00409014                                         ; DATA XREF: ___libc_csu_gala+D↑r
.data:00409014                                         ; "DARK SECRET GALAXY"
.data:00409018                 public __CRT_glob
.data:00409018 __CRT_glob      dd 2                     ; DATA XREF: __mingw32_init_mainargs+B↑r
.data:00409018                                         ; __setargv+9↑r ...
.data:0040901C                 public __fmode
.data:0040901C ; int _fmode
.data:0040901C __fmode         dd 4000h                 ; DATA XREF: ___mingw_CRTStartup+59↑w
.data:0040901C                                         ; ___mingw_CRTStartup+9A↑r
.data:00409020 _p_1784         dd offset dword_408654   ; DATA XREF: ___do_global_dtors↑r
.data:00409020                                         ; ___do_global_dtors+12↑r ...
.data:00409024 _fpi_3794       db  40h ; @              ; DATA XREF: ___pformat_cvt+84↑o
```



```
int __libc_csu_gala()
{
  int result; // eax
```

```
  sc[0] = off_409014;
  sc[3] = &byte_40DAC0;
  sc[1] = 31337;
  sc[2] = 1;
  byte_40DAC0 = off_409004[0][8];
  byte_40DAC1 = off_409010[0][7];
  byte_40DAC2 = off_409008[0][4];
  byte_40DAC3 = off_409004[0][6];
  byte_40DAC4 = off_409004[0][1];
  byte_40DAC5 = off_409008[0][2];
  byte_40DAC6 = 95;
  byte_40DAC7 = off_409004[0][8];
  byte_40DAC8 = off_409004[0][3];
  byte_40DAC9 = off_40900C[0][5];
  byte_40DACA = 95;
  byte_40DACB = off_409004[0][8];
  byte_40DACC = off_409004[0][3];
  byte_40DACD = off_409004[0][4];
  byte_40DACE = off_409010[0][6];
  byte_40DACF = off_409010[0][4];
  byte_40DAD0 = off_409004[0][2];
  byte_40DAD1 = 95;
  byte_40DAD2 = off_409010[0][6];
  result = *((unsigned __int8 *)off_409008[0] + 3);
  byte_40DAD3 = off_409008[0][3];
  byte_40DAD4 = 0;
  return result;
}
```


前面main里的两个函数没什么用

但是跟踪发现DARK SECRET GALAXY没有打印

继续跟踪

发现一个形似flag的东西

拼接一下得到`aliens_are_around_us`

是flag

结语

关键在于找到这个函数