攻防世界 reverse easy-153

原创

队长啊别开枪了 于 2019-10-08 16:53:16 发布 282 收藏

分类专栏： 逆向 文章标签： CTF reverse

本文链接：https://blog.csdn.net/weixin_41216733/article/details/102395612

逆向 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

1、peid查壳，为UPX壳，放到kali中用upx -d easy-153脱壳

2、ida查看脱壳程序

```
if ( !v7 )
{
  puts("\nOMG!!!! I forgot kid's id");
  write(v6, "6980087614356821435692875 3", 0x1Du);
  puts("Ready to exit     ");
  exit(0);
}
read(v5, &v9, 0x1Du);
__isoc99_scanf("%d", &v8);
if ( v8 == v7 )
{
  if ( (*(_DWORD *)((char *)lol + 3) & 0xFF) == 204 )
  {
    puts(":D");
    exit(1);
  }
  printf("\nYou got the key\n ");
  lol((int)&v9);
}
```

```
char v2; // [sp+15h] [bp-13h]@1
char v3; // [sp+16h] [bp-12h]@1
char v4; // [sp+17h] [bp-11h]@1
char v5; // [sp+18h] [bp-10h]@1
char v6; // [sp+19h] [bp-Fh]@1
char v7; // [sp+1Ah] [bp-Eh]@1
char v8; // [sp+1Bh] [bp-Dh]@1

v2 = 2 * *(_BYTE *)(a1 + 1);
v3 = *(_BYTE *)(a1 + 4) + *(_BYTE *)(a1 + 5);
v4 = *(_BYTE *)(a1 + 8) + *(_BYTE *)(a1 + 9);
v5 = 2 * *(_BYTE *)(a1 + 12);
v6 = *(_BYTE *)(a1 + 18) + *(_BYTE *)(a1 + 17);
v7 = *(_BYTE *)(a1 + 10) + *(_BYTE *)(a1 + 21);
v8 = *(_BYTE *)(a1 + 9) + *(_BYTE *)(a1 + 25);
return printf("flag_is_not_here");
```

程序看的一脸闷逼，发现v2v3v4v5v6v7v8的运算都与a1这个字符串有关，且a1至少有26位，而主程序中正好有一串字符串为
69800876143568214356928753
恰好26位，则

```
a='69800876143568214356928753'
v2=chr(2*ord(a[1]))
v3=chr(ord(a[4])+ord(a[5]))
v4=chr(ord(a[8])+ord(a[9]))
v5=chr(2*ord(a[12]))
v6=chr(ord(a[18])+ord(a[17]))
v7=chr(ord(a[10])+ord(a[21]))
v8=chr(ord(a[9])+ord(a[25]))
print v2,v3,v4,v5,v6,v7,v8
```

运算后
r h e l h e g
但是交上去不对，又看了看别人的writeup，发现是对的，不管了