huzai9527
码龄4年 暂无认证

108 原创 | 4万+ 周排名 | 1万+ 总排名 | 9万+ 访问 | 等级
1955 积分 | 108 粉丝 | 254 获赞 | 65 评论 | 1326 收藏
私信 关注
搜博主文章
热门文章
计算机组成原理----思维导图 27514
Webservice调到Client received SOAP Fault from server: 服务器无法处理请求,未将对象引用设置到对象的实例。 17996
操作系统——思维导图 14519
数据分析---十大算法 6599
Ubuntu进入登陆界面，输入密码，登录后黑屏一闪，又跳到登陆界面 3890
分类专栏
CTF 43篇
glibc 8篇
IDA 1篇
Linux内核 12篇
密码学 8篇
ssm框架 3篇
最新评论
vmware 虚拟机共享文件夹没有显示
随迁: 感谢
操作系统——思维导图
子蚊: 麻烦能发我一份源文件吗？ 2711729115@qq.com 谢谢！！
ctf-pwn-patchelf-用题目给的libc运行二...
huzai9527: 这个是由于的改完之后，没有相应的debug的文件，导致的pwngdb用...
ctf-pwn-patchelf-用题目给的libc运行二...
weixin_51805103: 同问， 改了后gdb里面heap bin指令都用不了了，要怎么解决...
ctf-pwn-patchelf-用题目给的libc运行二...
孤勇silly鬼: 师傅，改了之后gdb好些指令用不了，要怎么解决呀
您愿意向朋友推荐"博客详情页"吗？
强烈不推荐 不推荐 一般般 推荐 强烈推荐
最新文章
[_IO_FILE] 原理解析
【tcache stash unlink +】图解
【large bin 】源码解析
2021
11月 4篇 | 09月 2篇 | 08月 3篇 | 07月 3篇
06月 8篇 | 05月 27篇 | 04月 8篇 | 03月 6篇
02月 6篇 | 01月 7篇
2020年 6篇 2019年 9篇
2018年 19篇
广告
你的Mac 可以运行Windows
Mac与Windows融合
Windows 中畅享 Mac 功能。针对 macOS Monterey 和Windows 11/10进行了优化。
parallels.com.cn
打开

目录

一、IDA打开遇到JUMP CS命令
二、使用EDIT --> other --> specify sw...
跳表修复后，F5

IDA修复跳表

原创 huzai9527 2021-11-08 12:03:20 24 收藏 版权
分类专栏： CTF IDA 文章标签： 网络安全
CTF 同时被 2 个专栏收录 0 订阅 43 篇文章 订阅专栏

一、 IDA打开遇到JUMP CS命令

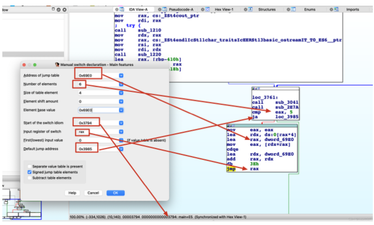
```
void __fastcall main(__int64 a1, char **a2, char **a3)
{
  __int64 v3; // rax
  unsigned int v4; // eax
  __int64 v5; // [rsp-418h] [rbp-418h]
  __int64 v6; // [rsp-2C8h] [rbp-2C8h]
  __int64 v7; // [rsp-178h] [rbp-178h]
  unsigned __int64 v8; // [rsp-20h] [rbp-20h]

  __asm { endbr64 }
  v8 = __readfsqword(0x28u);
  sub_2B96(a1, a2, a3);
  sub_2EDE();
  sub_3A88(&v5);
  sub_4326(&v6);
  sub_4BD4(&v7);
  v3 = sub_1210(&std::cout, "Peppa Pig first~");
  sub_1220(v3, &std::endl<char,std::char_traits<char>>);
  sub_3BEC(&v5);
  while ( 1 )
  {
    sub_3041(&v5);
    v4 = sub_2E7A();
    if ( v4 <= 5 )
      break;
    sub_1290("Invalid...");
  }
JUMPOUT(__CS__, (char *)dword_69E0 + dword_69E0[v4]);
}
```

CSDN @huzai9527

- 这是由于GCC在编译超过5个switch的结构时会用跳表进行优化，变成上面的样子

二、使用EDIT --> other --> specify switch

- 将光标打在JUMP命令上按TAB键切换到汇编，然后才能进行编辑
- 我解释一下各个参数的意义



```
Address of Jump table: 跳表的地址，cmp eax 5，之后跳到的地址，这里就是0x69E0
Number of elements: switch 的个数，先前cmp eax 5，加一个default这里填6
Size of table element: switc j 的 element 的类型，这里eax 可以看出占4个字节
Element shift amount: 这个一般情况下都是零，和跳表计算时的方式有关，比如此题只是单纯的跳
Element base value: 设置为计算跳转地址时给跳表元素加的值，比如此题的计算方法为 &jump_t
Start of the switch idiom: 这个默认就行，就是获取跳表值的语句的地址
Input register of switch: 设置为用于给跳表寻址的寄存器
First(lowest) input value: 就是 switch 的最小值了
Default jump address: 也就是 default 的跳转位置，其实有时候可以不填，但是最好还是填上，
```

跳表修复后，F5

```
12  while ( 1 )
13  {
14    sub_3041(v5, v4);
15    v4 = sub_2E7A();
16    if ( v4 <= 5 )
17    {
18      switch ( (unsigned __int64)off_69E0 + off_69E0[v4] )
19      {
20        case 1uLL:
21          v4 = (void *)v10;
22          v5 = v12;
23          sub_341B(v12, v10);
24          continue;
25        case 2uLL:
26          v4 = (void *)v10;
27          v5 = v12;
28          sub_348E(v12, v10);
29          continue;
30        case 3uLL:
31          v4 = (void *)v10;
32          v5 = v12;
33          sub_3565(v12, v10);
34          continue;
35        case 4uLL:
36          v4 = (void *)v10;
37          v5 = v12;
38          sub_363C(v12, v10);
39          continue;
40        case 5uLL:
41          v11 = sub_31B6();
42          if ( v11 && v11 != v10 )
43          {
44            switch ( v10 )
45            {
46              case 1u:
47                v5 = v12;
48                sub_3B3E(v12);
49                break;
50              case 2u:
51                v5 = v12;
52                sub_43DC(v12);
72
00003802 main:59 (3802)
```

ida 和 ida64 04-10
打开里面对应的exe文件就可以运行
代码逆向（五）&m‐&md‐&md‐switch-case识别技巧提高 姝丝 3296

我们前面为各位读者分别介绍了转成if-else与利用跳转表两种优化模式，但是在最后我隐含着提出了一个...
参与评论
请先 登录 后发表评论~ 抢沙发 评论
IDA实例教程_hnzwx888的专栏 10-30
再来看看这个类的另类脱法。直接运行该程序，DUMP下来,再使用IMPORTREC的IAT AutoSearch功能修复输入...
ida macOS在非英文状态下启动, 快捷键失灵或部分不可用... 10-28
ida macOS在非英文状态下启动, 快捷键失灵修复IDA7.1, IDA7.0)IDA7.1https://github.com/fjh658/IDA7.1_SPIDA...
IDA在mojave macOS崩溃解决方案 07-12
下载libqcocoa.dylib 将其copy到 /Applications/IDA Pro 7.0/ida.app/Contents/PlugIns/platforms/路径下或者替...
ida pro 下载地址 04-17
ida pro破解绿色版下载, 下载解压到目录安装即可使用。安装密码在install_pass.txt文件中
IDA实例_lego_noob的博客 11-5
再来看看这个类的另类脱法。直接运行该程序，DUMP下来,再使用IMPORTREC的IAT AutoSearch功能修复输入...
修复不连续的导入表_wangtiankuo的博客 11-24
转储保存之后,用IDA查看,基址是40000,函数调用都变成了Memory[地址],在IDA中修改基址为0x910000,函...
IDA Pro 7.6版IDA Pro 7.6版 09-04
IDA Pro 7.6 IDA Pro 7.6版
IDA实例教程 热门推荐 crkres9527 2万+
IDA实例教程 作者：笨笨雄 邮箱：nemo314@gmail.com 1 软件环境 静态分析有很多好处，例如加壳的...
REVERSE(IDA修改花指令/栈平衡/z3)学习笔记_小龙在线-C... 11-1
IDA修复栈平衡 反编译时报错,sp栈有错误，查看栈帧,首先打开栈帧: main_0工编里有栈帧不平衡: 在084右键修...
IDA pro使用笔记_AlienEowynWan的博客 11-4
用IDA加载文件,IDA会创建一个数据库,其组件分别保存在4个文件中,.id0, .id1,.nam,.til,分别对应是一个二叉树形...
Python-FixIDAPython修复IDA加载IDAPython时出现的错误 08-10
FixIDAPython - 修复IDA加载IDAPython时出现的错误
学习 IDA 使用 大将军王虎剩的专栏 3243
1.安装 IDA Pro 百科： 交互式反汇编器专业版（Interactive Disassembler Professional），人们常称其为IDA Pr...
arm ida 伪代码 安卓 符号表_一款本马释放器的简单分析及IDA的强... 11-26
该步入正题了,上面查看变长属性,文件大小不是很大,字符串和导入表信息也不多,因此我们决定从入口点开始进...
iOS 符号表恢复 & 逆向支付宝_weixin_34415923的博客 10-31
分析这部分需要用到 IDA 这个反汇编软件，这里结合两个实际的小例子来说明: 1._NSConcreteStackBlock 假设...
工具 IDA Pro Luzhuo 的博客 1154
工具 IDA Pro 本文由 Luzhuo 编写,转发请保留该信息. 原文: https://blog.csdn.net/Rozo/article/details/79816842...
开源一个IDA小插件： 修复VMP dump导入函数 yan_star的博客 778
简述： 通常我们在静态分析vmp加壳后的程序或者驱动时，都会选择将其脱开然后看dump文件。但是vmp会将...
2020第十一届极客大挑战——Geek Challenge(部分解)_Ly... 12-22
2.用ida打开dll只看二进制选项,结合提示知道这是一个损坏的PE文件 3.用winhex简单修复 即随便找一个可执行P...
IDA简单Switch-Case结构的汇编代码分析 faithzz的专栏 3434
使用IDA进行静态逆向分析，很重要的一点是是对高级语言程序结构的解析，比如Switch-Case结构，IDA的F5功...
ida 7.0插件IDA Class Informer PlugIn 最新版 10-23
ida 7.0插件IDA Class Informer PlugIn 最新版官方原版,放在ida的PlugIns,添加plugins.cfg相关项就可以使用
IDA Pro 支持 macOS 10.15 04-19
IDA Pro 7.0 支持 macOS 10.15，支持 F5 反编译。解压后打开文件夹，如果打不开 ida64.app，执行 sudo xattr ...
IDA-SIG_idapro_源码 最新发布 09-30
Collectoin of IDA Pro sig file
IDAPython中文教程手册 10-18
IDAPython中文教程手册，翻译自英文文档，密码：123。
ida7.0插件合集 12-22
ida7.0插件合集2020年12月最新收集,包括IDA_ClassInformer_PlugIn,HexRaysCodeXplorer,auto_re,UltraAnalyz...
Mac IDA 7.6.zip 06-24
IDA 7.6版本，支持Mac 11.2.3系统
Remove VirtualPortGroup Specify vSwitch weixin_33798152的博客 88
Script ---------- #Remove all...
IDA pro脱壳实战过反调试标签 daide2012的博客 6027
IDA pro脱壳实战过反调试标签（空格分隔）： Apk逆向1. 前言之前总结了IDA pro脱壳的基本步骤，包括调试步...
© 2021 CSDN 皮肤主题: 大白 设计师:CSDN官方博客 返回首页
关于我们 招聘纳士 广告服务 开发助手 400-660-0108 kefu@csdn.net 在线客服 工作时间 8:30-22:00
公安备案号11010502030143 京ICP备19004658号 京网文（2020）1039-165号 经营性网站备案信息
北京互联网违法和不良信息举报中心 网络110报警服务 中国互联网举报中心 家长监护 Chrome商店下载
huzai9527 关注 0 0 0 专栏目录
举报