

evo

自强不息，厚德载物 ii 自动驾驶，让生活更美好 ^_^

目录视图

👍

摘要视图

RSS

订阅

个人资料



aidear_evo

🖋 博客专家

关注

原创
264粉丝
95喜欢
329评论
53

等级：📖 博客 6

访问量：41万+

积分：6986

排名：4081

HELLO WORLD

-> 【Github】 <-

博客专栏



Bash百宝箱

文章：55篇

阅读：80308



设计与架构

文章：28篇

阅读：22317



Linux之美

文章：27篇

阅读：38033



C/C++沉思录

文章：35篇

阅读：53453



图形图像

文章：73篇

阅读：152438



Python来了

文章：25篇

阅读：36562



CS-计算机科学备忘录

文章：22篇

阅读：24308

【C】libc中的hook机制

标签：libc malloc hook

2015年11月20日 20:29:58

👁 1743人阅读

💬 评论(0)

⭐ 收藏

🚩 举报

分类：C/C++ (32) ▾

📄 版权声明：本文为博主原创文章，未经博主允许不得转载。https://blog.csdn.net/iEearth/article/details/49951567

libc中的hook机制，主要用于内存分配，它就像无处不在的钩子一样，一旦设置好了 hook，我们就可以在内存分配的地方随心所欲地做我们想做的事情。

在malloc.h中，声明了一些hook，原型如下：

```
1 /* Hooks for debugging and user-defined versions. */
2 extern void (*__free_hook) (void *__ptr, const void *);
3 extern void (*__malloc_hook)(size_t __size, const void *);
4 extern void (*__realloc_hook)(void *__ptr, size_t __size, const void *);
5 extern void (*__memalign_hook)(size_t __alignment, size_t __size, const void *);
6 extern void (*__after_morecore_hook) (void);
```

从上面的注释中可以看出，我们可以自定义这些hook，用于debug。这些hook都是函数指针，以__malloc_hook为例，当指定__malloc_hook为自定义的钩子后，调用malloc时，就会进入我们指定的自定义钩子，下面以一个例子说明。

```
1 // test.cpp
2 #include <stdio.h>
3 #include <stdlib.h>
4 #include <malloc.h>
5
6 static void* (*old_malloc_hook)(size_t, const void*); // 函数指针，用于保存原始的malloc钩子
7
8 static void* my_malloc(size_t size, const void *caller) // 自定义malloc钩子
9 {
10     static int malloc_time = 0; // 记录malloc钩子调用了几次
11     __malloc_hook = old_malloc_hook; // 还原malloc钩子，否则下面真正的malloc调用会造成递归死循环
12     void *ptr = malloc(size); // 真正的内存分配
13     __malloc_hook = my_malloc; // 重置malloc钩子为自定义值
14     printf("%s, addr: %p, size: %lu, time:%d\n", __func__, ptr, size, ++malloc_time);
15     return ptr;
16 }
17
18 void __attribute__((constructor)) malloc_init() // __attribute__((constructor)) 是gcc的
19 // 意思是在进入main主方法之前会首先调用这个函数，我们用它来初始化malloc钩子
20 {
21     old_malloc_hook = __malloc_hook; // 保存原始的malloc钩子
22     __malloc_hook = my_malloc; // 设置malloc钩子为自定义值
23 }
24
25 int main()
26 {
27     char *c = (char*)malloc(sizeof(char)); // malloc
28     free(c);
29
30     int *i = new int; // new
31     delete i;
32
33     FILE *f = fopen("./file", "r"); //fopen
34     if (NULL != f) {
35         fclose(f);
36     }
37 }
```

文章分类

- CS (3)
- Arch (25)
- C/C++ (33)
- Java (6)
- Python (25)
- JS (12)
- Tools (20)
- Linux (64)
- Android (16)
- Graphics (20)
- Qt (46)

联系我们

请扫描二维码联系客服

webmaster@csdn.net

400-660-0108

QQ客服 客服论坛

关于 · 招聘 · 广告服务 · 百度

©1999-2018 CSDN版权所有

京ICP证09002463号

经营性网站备案信息

网络110报警服务

中国互联网举报中心

北京互联网违法和不良信息举报中心

```
38     return 0;
39 }
```

运行结果如下：

```
1 $g++ -o test test.cpp
2 ./test
3 my_malloc, addr: 0x209c010, size: 1, time:1
4 my_malloc, addr: 0x209c010, size: 4, time:2
5 my_malloc, addr: 0x209c030, size: 568, time:3
```

1

从上面的结果可以看出，不仅malloc调用会进入我们自定义的malloc钩子，而且new en（还有许多其它的函数）也会进入malloc钩子。需要注意的一点是，这些内存分配的钩子需要不断的还原其位置，也真是因为如此，hook机制不适用于多线程。

- 上一篇
- 【C】使用backtrace获取堆栈信息
- 下一篇
- 【Linux】LD_PRELOAD用法



世界上最好的语言，PHP凭什么这么“说”

课程包含PHP零基础入门、PHP基础编程、数据库、项目实战、linux、框架开发到高级+企业项目实战，深入浅出地剖析和分解了PHP企业级开发项目在实际工作中的应用。

18502 [查看更多>>](#)

一种hook libc库函数的简易方案

wonderdaydream 2017年07月04日 18:21 366

有时候我们分析/逆向ELF文件时，可能想直接运行ELF看看效果，同时又想捕获ELF文件用了哪些字符串、回连地址&端口、操作了哪些文件等等特征信息。这时我们可以巧妙的借用LD_PRELOAD，来实现一种...

Linux系统调用Hook姿势总结

tianyeming 2016年03月24日 19:31 5769

<http://www.cnblogs.com/LittleHann/p/3854977.html> 主题 Linux 相关学习资料 <http://xiaonieblog.co...>

ELF文件及android hook原理

u012455213 2016年12月24日 21:23 1907

可执行和可链接格式(Executable and Linkable Format，缩写为ELF)，常被称为ELF格式，在计算机科学中，是一种用于执行档、目的档、共享库和核心转储的标准文件格式。...

在应用程序中替换Linux中Glibc的malloc的四种方法

littlefang 2010年12月03日 12:35 15793

打算优化系统的内存分配，接管glibc提供的内存管理，但是整个工程的代码量很大，使用malloc、realloc、calloc和free的地方到处都是，如果自己写好的接口需要重命名所有的调用，先不说工...

拦截malloc、free等库函数（malloc钩子）

LBO4031 2016年05月29日 22:59 2837

__malloc_hook是一组glibc提供的malloc调试变量中的一个，这组变量包括： void *(*__malloc_hook)(size_t size, const void *caller...

关于Android上对so进行函数的hook的完整原理解析，最新测试通过

<http://pan.baidu.com/s/1boiw3iJ> 共享出来源码吧，里面有远程注入（inject）和下面方法2的源码以及使用libsubstrate的方式，修改go...



scjie168

2016年09月07日 18:05

📖 1800



malloc 调用跟踪浅谈



robertsong2004

2016年09月10日 19:16

📖 847

之前转载了一篇文章，关于memory leak的检出。 <http://blog.csdn.net/robertsong2004/article/details/52496184> 这里面使用的方...



通过HOOK系统的API接口实现对API功能的修改



ouchengguo

2014年04月01日 13:03

📖 1462

一、实现功能头文件：AnalysisIniFile.h #ifndef __ANALYSISINIFILE_H__ #define __ANALYSISINIFILE_H__ #include ...

MSFunction原理



gavin0123

2014年09月22日 17:20

📖 1228

整个Hook原理的分析，完成Hook功能，要做的事情大致有两件： 1.修改目标函数前N字节，跳转到自定义函数入口； 2.备份目标函数前N个字节，跳转回目标函数。...

逆向角度分析 CydiaSubstrate Hook 原理



u013702935

2014年02月28日 16:25

📖 2981

简介 CydiaSubstrate，iOS7越狱之前名为 MobileSubstrate（下文简称为MS或MS框架），作者为大名鼎鼎的Jay Freeman(saurik)。MS框架为越狱iDe...

malloc 源码



zhongjiekangping

2011年09月07日 15:16

📖 3347

两个函数取自UNIX 版本6 malloc.c文件，一个为malloc函数，一个为mfree函数 2515:/*map数组是一个空闲资源列表，其中每个存储区由其长度和相对地址定义*/ ...

如何hook dlopen和dlsym底层函数



zhuanshenai

2016年06月24日 14:32

📖 3877

如何hook dlopen和dlsym底层函数android 逆向分析过程有时候需要hook dlopen和dlsym函数，打印调用的库或者函数名。利用cydia substrate的动态库，或者...

linux 下的hook



taina2008

2008年04月02日 17:49

📖 4010

◆ 如何修改动态库符号表 作者：wangdb (mailto:wangdb@nsfocus.com) 主页：<http://www.nsfocus.com/> 日期：2000-10-14 一、E...

Linux下Hook一个共享库函数



linuxheik

2016年04月18日 19:28

📖 1566

有时程序员需要完成这类任务：假如你有一个二进制版的系统，例如现在流行的android，你需要为这个系统开发一个软件。这个软件牵涉到系统行为，因此需要对系统做修改。然而你并没有这个系统的所有源码...

内存分配钩子__malloc_hook, __realloc_hook, __free_hook的使用

mem.h #ifndef __MEM_H__ #define __MEM_H__ #include #include static void *(*old_malloc_hook)(siz...



hoi0714

2012年08月26日 17:11

📖 1623

open和fopen的区别



hairetz

2009年05月05日 00:01

📖 31194

open和fopen的区别：1.缓冲文件系统缓冲文件系统的特点是：在内存开辟一个“缓冲区”，为程序中的每一个文件使用，当执行读文件的操作时，从磁盘文件将数据先读入内存“缓冲区”，装满后再从内存“缓冲...

采取个hook技巧对writefile函数进行阻碍（2）



wxl1986622

2012年05月21日 10:44

📖 1602

内容充分的生命就是长久的生命，我们要以此为而不是以时间来衡量生命。<http://www.cnblogs.com/zhxfi/archive/2011/11/03/2233846.html> 这个是笔者之...



1



fopen与open的区别（好文）



oscarjulia

2017年05月23日 11:21

📖 442

参考文章：<http://www.cnblogs.com/hnrainll/archive/2011/09/16/2178706.html> <http://www.cnblogs.com/joeblac...>

malloc hook初探



think_ycx

2017年09月14日 16:50

📖 244

<http://www.jianshu.com/p/0d7aa3166eec> 在程序中设置钩子，用来在malloc，realloc，free的时候，对其进行检查，可以看到对应的函数调用后...

【C】libc中的hook机制



iEearth

2015年11月20日 20:29

📖 1743

libc中的hook机制，主要用于内存分配，它就像无处不在的钩子一样，一旦设置好了hook，我们就可以在内存分配的地方随心所欲地做我们想做的事情。在malloc.h中，声明了一些hook，原型如...