CobbLiu（留候）

专注高性能服务器开发、分布式存储

目前在一家云计算公司的分布式文件系统上研究和开发Bug.

略懂分布式，略懂文件系统，略懂C/C++

会写Golang/Erlang/Python/Perl/PHP/Shell

工具: Emacs24 + Poker II
新浪微博: @
邮箱：cobblau@gmail.com

昵称：CobbLiu
园龄：5年8个月
粉丝：144
关注：0
+加关注

< 2017年12月 >

日	一	二	三	四	五	六
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

搜索

找找看

谷歌搜索

常用链接

我的随笔

我的评论

我的参与

最新评论

利用LD_PRELOAD hook代码

loader在进行动态链接的时候，会将有相同符号名的符号覆盖成LD_PRELOAD指定的so文件中的符号。换句话说，可以用我们自己的so库中的函数替换原来库里有的函数，从而达到hook的目的。这和Windows下通过修改import table来hook API很类似。相比较之下，LD_PRELOAD更方便了，都不用自己写代码了，系统的loader会帮我们搞定。但是LD_PRELOAD有个限制：只能hook动态链接的库，对静态链接的库无效，因为静态链接的代码都写到可执行文件里了嘛，没有坑让你填。

先是受害者，我们的主程序main.c，通过strcmp比较字符串是否相等：

```c
#include <stdio.h>
#include <string.h>

int main(int argc, char *argv[])
{
    if( strcmp(argv[1], "test") )
    {
        printf("Incorrect password\n");
    }
    else
    {
        printf("Correct password\n");
    }
    return 0;
}
```

然后是用来hook的库hook.c：

```c
#include <stdio.h>
#include <string.h>
#include <dlfcn.h>

typedef int(*STRCMP)(const char*, const char*);

int strcmp(const char *s1, const char *s2)
{
    static void *handle = NULL;
    static STRCMP old_strcmp = NULL;

    if( !handle )
    {
        handle = dlopen("libc.so.6", RTLD_LAZY);
        old_strcmp = (STRCMP)dlsym(handle, "strcmp");
    }
    printf("hack function invoked. s1=<%s> s2=<%s>\n", s1, s2);
    return old_strcmp(s1, s2);
}
```

因为hook的目标是strcmp，所以typedef了一个STRCMP函数指针。由于hook的目的是要控制函数行为，所以需要从原库libc.so.6中拿到“正版”strcmp指针，保存成old_strcmp以备调用。

```
Makefile：

test: main.c hook.so
    gcc -o test main.c

hook.so: hook.c
    gcc -fPIC -shared -o hook.so hook.c -ldl
```

执行：

```
$ LD_PRELOAD=./hook.so ./test 123
hack function invoked. s1=<123> s2=<test>
Incorrect password

$ LD_PRELOAD=./hook.so ./test test
hack function invoked. s1=<test> s2=<test>
Correct password
```

使用PRE_LOAD劫持库函数的这种做法可以做很多事情，比如劫持随机函数random, random_r等，使得看起来是公平的摇号程序可以自如地由自己控制；比如实现一些高级功能，zlibc就是使用这个技术来做压缩，但是上层应用对其完全无感知；比如紧急fixbug，你可以preload一个函数库来使你的有bug的程序如期运行；比如访问应用程序的内存，做一些你想做的事 :)

参考：Reverse Engineering with LD_PRELOAD

转自：http://hbprotoss.github.io/posts/li-yong-ld_preloadjin-xing-hook.html

分类: Linux编程技术

CobbLiu
关注 - 0
粉丝 - 144
+加关注

« 上一篇：perf之record
» 下一篇：rename系统调用的实现浅析

posted @ 2016-08-01 13:18 CobbLiu 阅读(131) 评论(0) 编辑 收藏

我的标签

随笔分类

C(17)
C++(18)
DNS(14)
Emacs(15)
Erlang(3)
Go(10)
leveldb(5)
Linux编程技术(26)
Linux内核(9)
Linux文件系统(8)
Linux系统技术(50)
python&php&perl(5)
笔试&面试(14)
分布式存储(7)
分布式系统(7)
软实力(2)
数据结构和算法(18)
数据库(7)
网络编程(11)
源码分析(6)
杂(7)

积分与排名

积分 - 217059
排名 - 1005

阅读排行榜

1. python pickle模块(75434)

2. STL源码学习----lower_bound和upper_bound算法(45550)

3. DNS开源服务器BIND最小配置详解(33121)

4. Ubuntu12.04设置屏幕分辨率(29846)

5. mysqlbinlog 查看binlog时报错unknown variable 'default-character-set=utf8'(15989)

评论排行榜

1. STL源码学习----lower_bound和upper_bound算法(8)

2. python pickle模块(6)

3. BIND9源码分析奠基(6)

4. DNS消息格式(5)

5. 串的模式匹配算法---Horspool(5)

推荐排行榜

1. python pickle模块(11)

2. 内存问题排查工具 --- valgrind(5)

3. DNS开源服务器BIND最小配置详解(5)

4. STL源码学习----lower_bound和upper_bound算法(5)

5. STL源码学习----内存管理(4)

最新IT新闻:
· 我国第一颗暗物质粒子探测卫星悟空号“取经”记
· 外媒：腾讯实施特洛伊木马投资计划 欲伏击美科技巨头
· 微信支付即将登陆马来西亚 与支付宝抢滩东南亚市场
· 华为Mate 10 Pro拍摄的乌镇美图 华丽醉人
· 马云、马化腾、李彦宏、库克齐聚乌镇，都说了啥？
» 更多新闻...

最新知识库文章:
· 以操作系统的角度述说线程与进程
· 软件测试转型之路
· 门内门外看招聘
· 大道至简，职场上做人做事做管理
· 关于编程，你的练习是不是有效的？
» 更多知识库文章...