秋明分享平台之

openssh修改代码记录操作日志

撰稿人：秋明

撰稿人邮箱：tyumen@zhoufengjie.cn

QQ群：90122290

本文撰稿日期： 2015年2月25日星期三

本站口号：开源、分享、共进

版权所有：随便使用

注解：任何想通过本平台分享文档的，可以随时联系，文档里面注明出稿人和邮箱，方便文档使用者同撰稿的兄弟技术咨询沟通和交流；

目录

1 前言 3

2 下载openssh源代码 3

3 修改代码 3

3.1 修改channels.h文件声明logfd描述符 4

3.2 修改channels.c初始化上面新建的logfd 5

3.3 修改serverloop.c记录用户操作记录 5

3.4 修改channels.c记录用户屏幕输出 9

3.5 修改channels.c用户登出时关闭文件 10

4 安装测试 12

# 前言

做了跳板机之后，发现有的时候有人做了误操作，需要进行查看，因此想起修改ssh的源代码，记录用户的操作日志，本文来自互联网，后面带着大家一步一步进行修改；

# 下载openssh源代码

openssh的官方下载地址（请自己找最新的openssh源码下载）：http://www.openssh.com/portable.html

比如：http://ftp.jaist.ac.jp/pub/OpenBSD/OpenSSH/portable/openssh-6.7p1.tar.gz

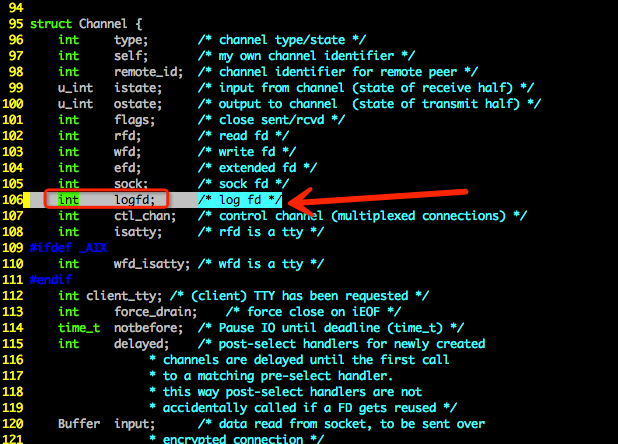
如果大家想一步到位，也可以直接下载我修改完的ssh代码进行编译安装即可，下载地址：

http://download.zhoufengjie.cn/software/tools/jumpserver/openssh-6.7p2.tar.gz

# 修改代码

本文修改的文件就涉及到两个文件：channels.c和serverloop.c

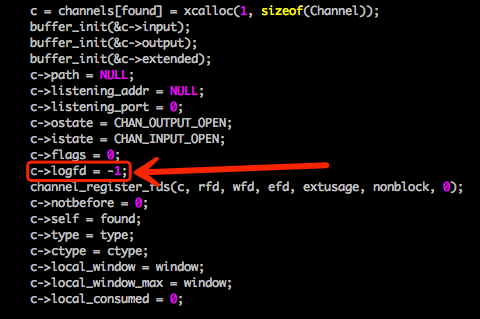
## 修改channels.h文件声明logfd描述符



在channels.h找到struct Chanel结构体，新添加一行（可以加在105行int sock后面），目的是新建一个文件描述符，在用户登陆时，打开一个文件，赋值给该文件描述符；

int logfd;

## 修改channels.c初始化上面新建的logfd

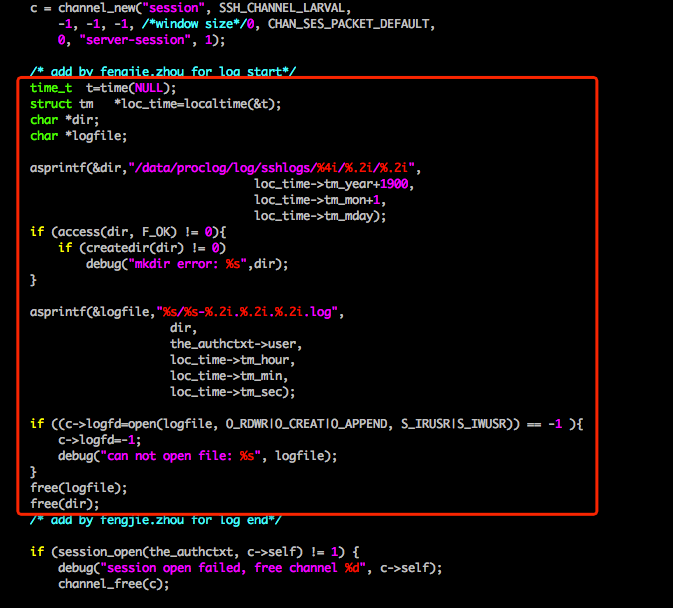


找到channel\_new(char \*ctype, int type, int rfd, int wfd, int efd, u\_int window, u\_int maxpack, int extusage, char \*remote\_name, int nonblock)这个函数，添加上面一行内容，初始该logfd为- 1可以放到此函数内c->flags = 0;后面

c->logfd = -1;

## 修改serverloop.c记录用户操作记录

当用户登陆时，创建一个文件，该文件将是记录用户的操作记录，打开serverloop.c文件。



在serverloop.c中找到server\_request\_session(void)函数，在上图的位置添加红框部分内容，内容如下：

/\* add by fengjie.zhou for log start\*/

time\_t t=time(NULL);

struct tm \*loc\_time=localtime(&t);

char \*dir;

char \*logfile;

asprintf(&dir,"/data/proclog/log/sshlogs/%4i/%.2i/%.2i",

loc\_time->tm\_year+1900,

loc\_time->tm\_mon+1,

loc\_time->tm\_mday);

if (access(dir, F\_OK) != 0){

if (createdir(dir) != 0)

debug("mkdir error: %s",dir);

}

asprintf(&logfile,"%s/%s-%.2i.%.2i.%.2i.log",

dir,

the\_authctxt->user,

loc\_time->tm\_hour,

loc\_time->tm\_min,

loc\_time->tm\_sec);

if ((c->logfd=open(logfile, O\_RDWR|O\_CREAT|O\_APPEND, S\_IRUSR|S\_IWUSR)) == -1 ){

c->logfd=-1;

debug("can not open file: %s", logfile);

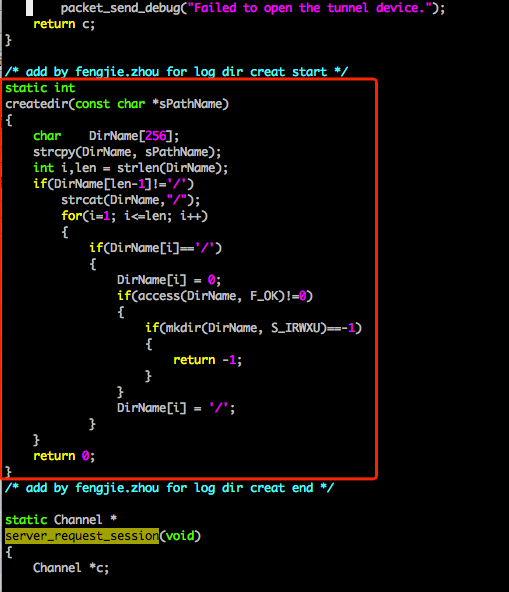
}

free(logfile);

free(dir);

/\* add by fengjie.zhou for log end\*/

当然这里面有一个自己写的函数creatdir，按日期建目录，可以放在server\_request\_session(void)上面，如下图就是createdir函数。



代码为：

/\* add by fengjie.zhou for log dir creat start \*/

static int

createdir(const char \*sPathName)

{

char DirName[256];

strcpy(DirName, sPathName);

int i,len = strlen(DirName);

if(DirName[len-1]!='/')

strcat(DirName,"/");

for(i=1; i<=len; i++)

{

if(DirName[i]=='/')

{

DirName[i] = 0;

if(access(DirName, F\_OK)!=0)

{

if(mkdir(DirName, S\_IRWXU)==-1)

{

return -1;

}

}

DirName[i] = '/';

}

}

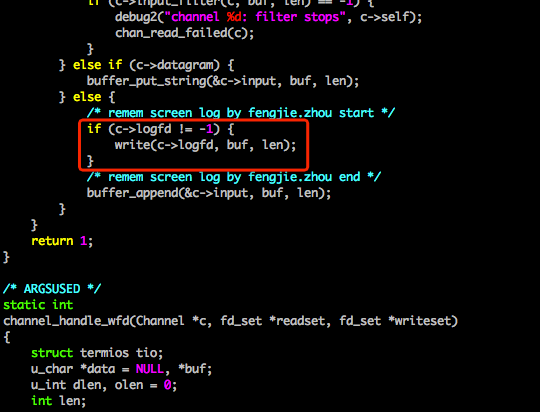
return 0;

}

/\* add by fengjie.zhou for log dir creat end \*/

## 修改channels.c记录用户屏幕输出

记录用户的屏幕输出，打开channels.c源文件，修改如下：



在channel.c找到channel\_handle\_rfd(Channel \*c, fd\_set \*readset, fd\_set \*writeset)函数，在上图位置添加红框部分内容，记录用户的操作记录。代码如下：

/\* remem screen log by fengjie.zhou start \*/

if (c->logfd != -1) {

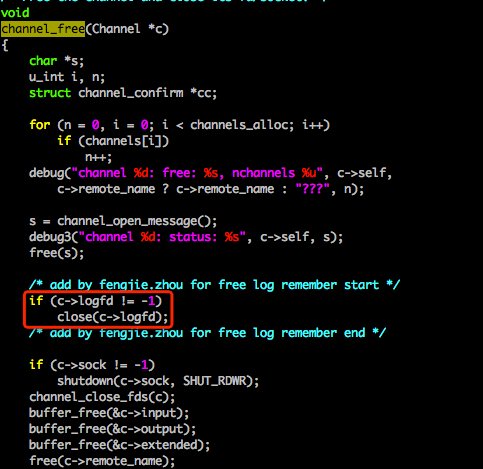
write(c->logfd, buf, len);

}

/\* remem screen log by fengjie.zhou end \*/

## 修改channels.c用户登出时关闭文件

用户登出时关闭记录文件，打开channels.c：

拦截

在channel.c中找到channel\_free(Channel \*c)函数，在上图位置添加红框部分，目的是用户logout时关闭日录文件,代码如下：

/\* add by fengjie.zhou for free log remember start \*/

if (c->logfd != -1)

close(c->logfd);

/\* add by fengjie.zhou for free log remember end \*/

# 安装测试

最后编译安装，为了不影响系统自带的openssh，可以安装在/usr/local/openssh中，等测试没有问题了再覆盖安装，如下

./configure --prefix=/usr/local/openssh

make

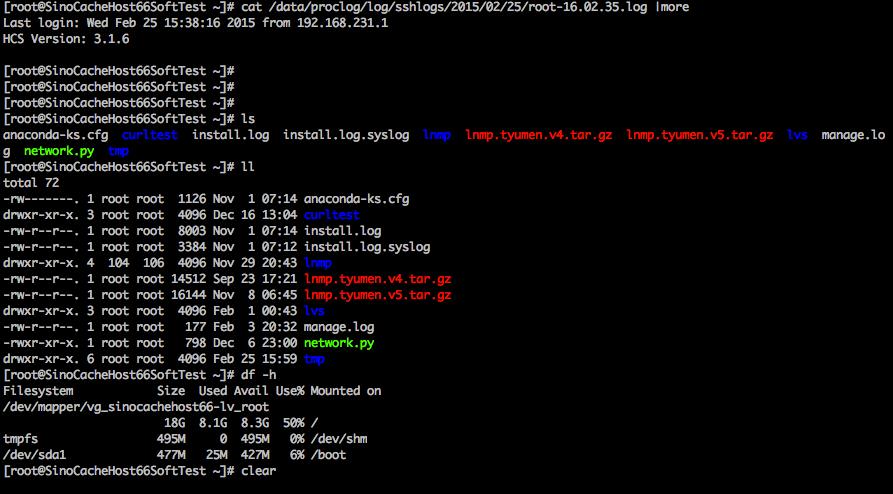
make install

执行完这三步后，停止系统自带的sshd进程：/etc/init.d/sshd stop

启用修改后重新编译的openssh:  /usr/local/openssh/sbin/sshd

找另外一台登陆一下该服务器，验证一下。

下图是ssh登陆时执行的几个操作：



最后我讲一下，怎么去实现记录用户的输入，并实现动态回放思路，有兴趣的可以研究一下。

在chanel.c另一个函数channel\_handle\_wfd(Channel \*c, fd\_set \*readset, fd\_set \*writeset)是用户的输入的数据处理，需要记录用户输入的，可以这一行len = write(c->wfd, buf, dlen);前加一个写入，将buf写入到我们审记记录。

至于动态回放，其实也很简单，每次写日志记录之前，定义一下结果体，结果体定义时间戳，再定义buf的长度，先写一个这个结构体，再写buf，然后我们写别一个程序读这个文件，通过时间戳的信息实现动态回放。