所需要的所有文件（包）daq-2.06 \ libdnet-1.12 \ libpcap-1.8.1 \

pcre2-10.23 \ snort-2.9.9.0 \zlib-1.2.11 \

首先安装一些依赖的包

yum install gcc

yum install g++

yum install glibc-headers

yum install gcc-c++

yum install bison flex

tar zxvf zlib-1.2.11

cd zlib-1.2.11

./configure && make && make install

tar zxvf daq-2.06

cd daq-2.06

./configure && make && make install

tar zxvf libpcap-1.8.1

cd libpcap-1.8.1

./configure && make && make install

（yum -y install pcre-devel.x86\_64）

tar zxvf pcre2-10.23

cd pcre2-10.23

./configure && make && make install

tar zxvf libdnet-1.12

cd libdnet-1.12

./configure && make && make install

tar zxvf snort-2.9.9.0

cd snort-2.9.9.0

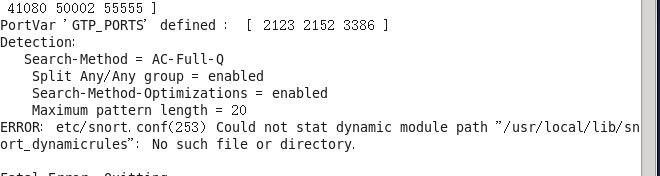
./configure && make && make install

遇到错误可参考 <http://blog.csdn.net/x_white/article/details/8657076>

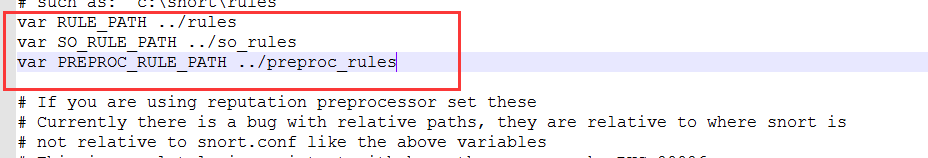
snort.conf的位置

启动snort: snort -c snort/snort-2.9.9.0/etc/snort.conf

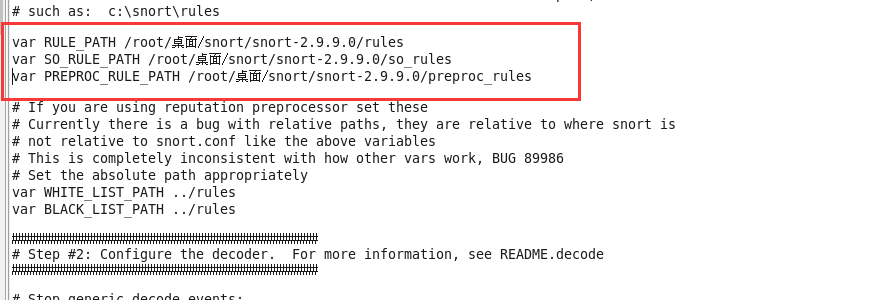
可能遇到的问题



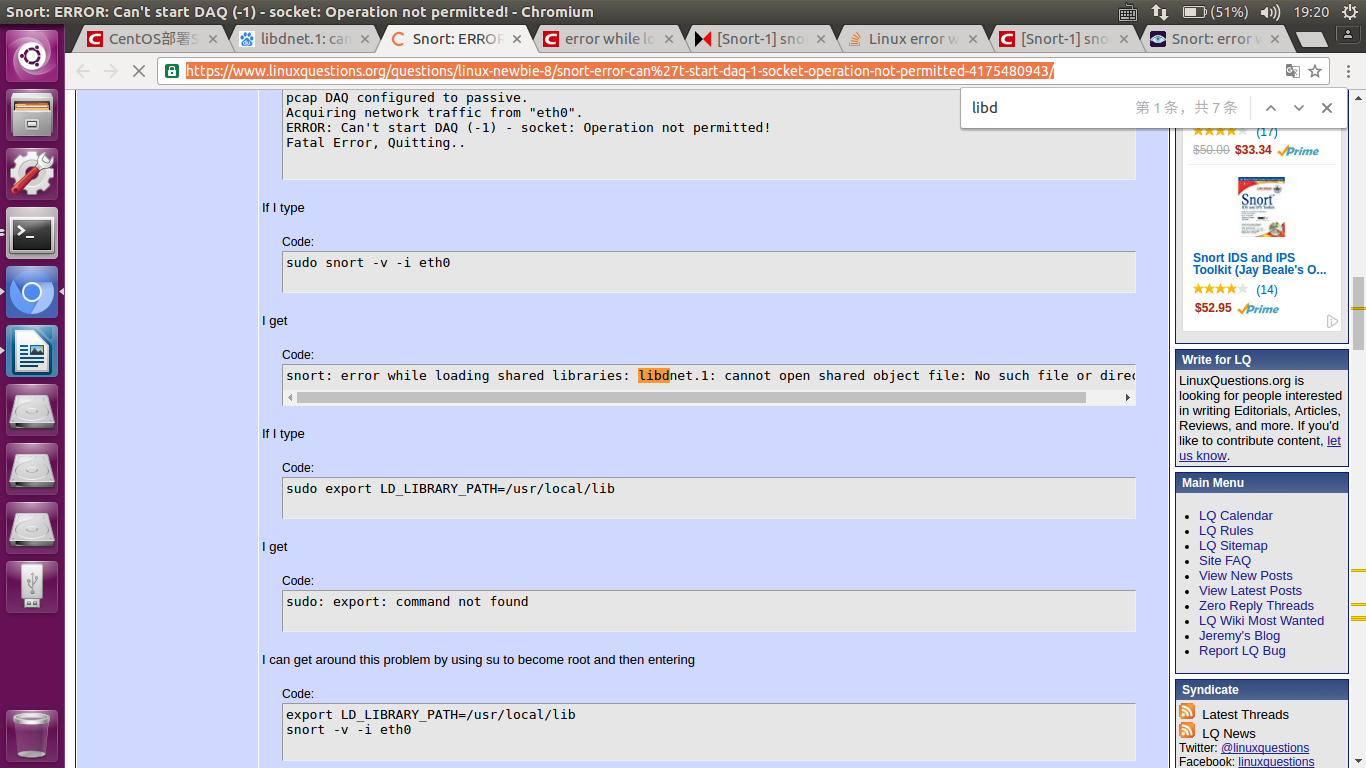
在对应的目录下新建snort\_dynamicrules 文件夹即可

要将rules、so\_rules、preproc\_rules文件夹及里面的文件copy到snort下并改snort.conf中的文件

改为绝对路径

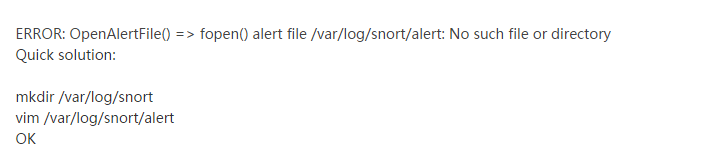


[https://www.linuxquestions.org/questions/linux-newbie-8/snort-error-can%27t-start-daq-1-socket-operation-not-permitted-4175480943/](https://www.linuxquestions.org/questions/linux-newbie-8/snort-error-can't-start-daq-1-socket-operation-not-permitted-4175480943/)

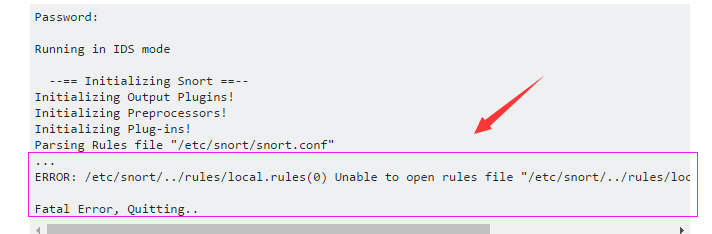


安装完后要自己下载规则库（rules）,一般来说下载的规则库中木有white\_list.rules和black\_list.rules，此时要自己要rules文件夹中创建这两个文件（可以为空），

在启动的过程中可能会遇到以下错误，此时建立相应的目录文件（var/log/snort/alert）即可,



有时碰到以下这个错误



那是因为你启动时所在的目录错了，最好在当前用户的根目录下



但是要有攻击alert中才会有记录，可以在icmp.rules中加入规则

alert icmp any any -> any any (msg:"icmp 666666666666"; sid:8888888;)#拦截所有icmp