1. 实验项目名称：

实验5-1-snort与其基础环境的安装配置

1. 实验原理：

1)        Snort能够对网络上的数据包进行抓包分析，但区别于其它嗅探器的是，它能根据所定义的规则进行响应及处理。Snort 通过对获取的数据包，进行各规则的分析后，根据规则链，可采取Activation（报警并启动另外一个动态规则链）、Dynamic（由其它的规则包调用）、Alert（报警），Pass（忽略），Log（不报警但记录网络流量）五种响应的机制。Snort有数据包嗅探，数据包分析，数据包检测，响应处理等多种功能，每个模块实现不同的功能，各模块都是用插件的方式和Snort相结合，功能扩展方便。例如，预处理插件的功能就是在规则匹配误用检测之前运行，完成TIP碎片重组，http解码，telnet解码等功能，处理插件完成检查协议各字段，关闭连接，攻击响应等功能，输出插件将得理后的各种情况以日志或警告的方式输出。

1. 实验目的：

熟悉基础环境的搭建和snort的安装配置

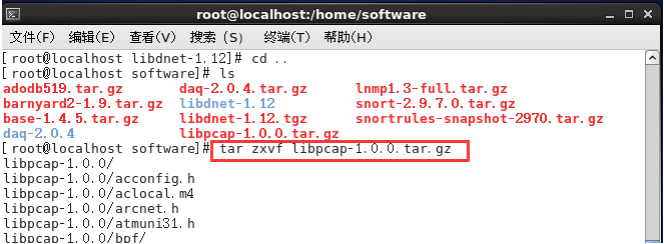
1. 实验器材（设备、虚拟机名称）：

CentOS6.5：192.168.1.2

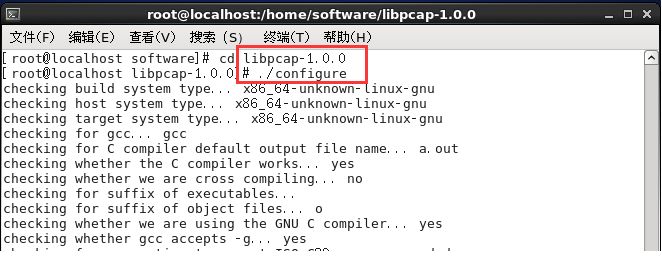
1. 实验步骤：

1. **安装snort+barnyard2**

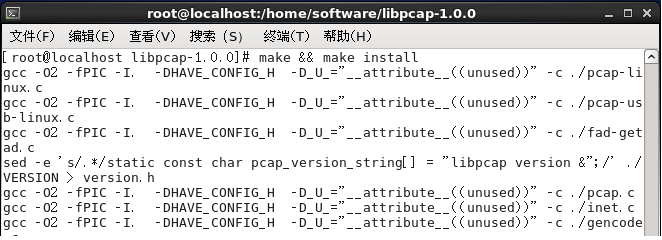
1.1 进入/home/software目录，解压libpcap-1.0.0.tar.gz。



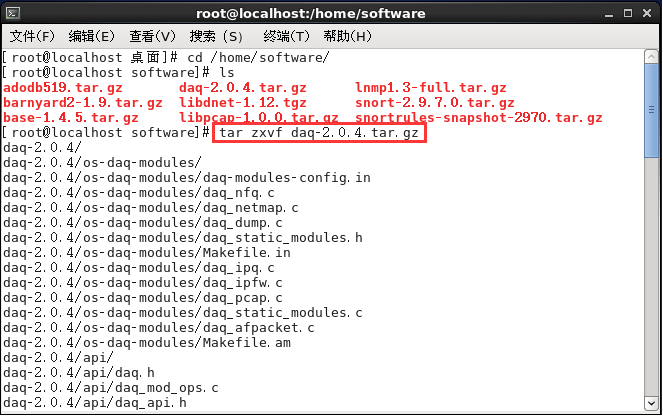
1.2 进入目录libpcap-1.0.0的目录执行“./configure”命令进行配置。



1.3 执行命令“make && make install”，进行libpcap的编译安装。



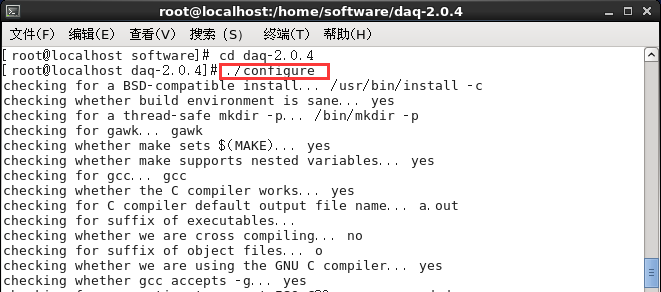
1.4   进入目录“/home/software”，ls查看文件，执行命令“tar zxvf daq-2.0.4.tar.gz”，解压daq-2.0.4.tar.gz文件。



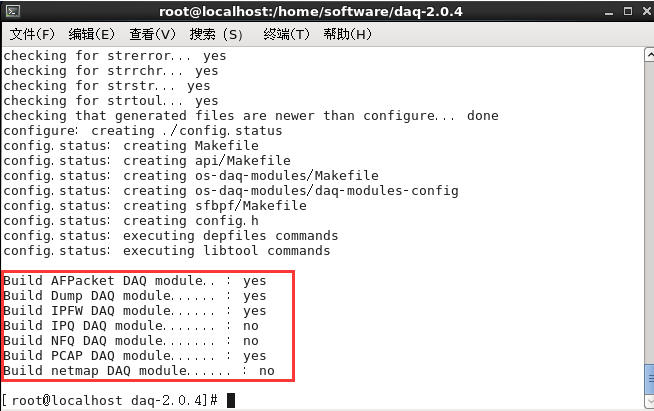
1.5 使用cd命令切换到daq-2.0.4的目录下。



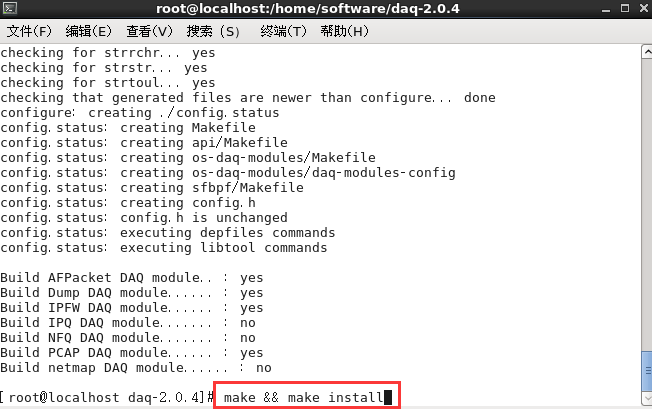
1.6 执行命令“./configure”对daq-2.0.4进行配置。



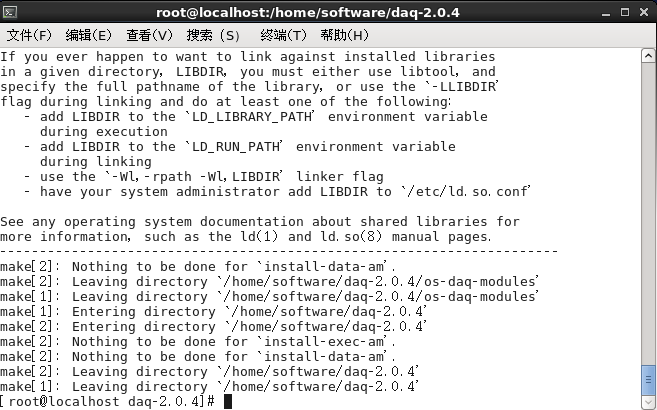
1.7 得到如下反馈信息说明，可以进行正确安装。



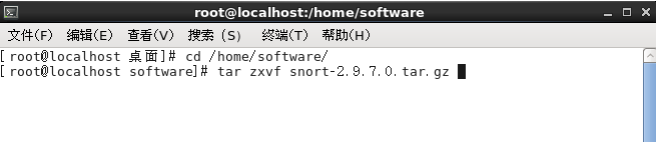
1.8    执行命令“make && make install”进行安装。



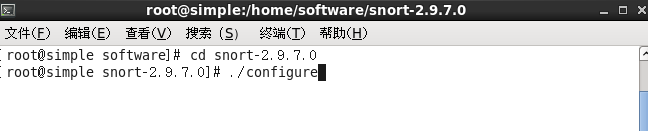
1.9    得到如下信息说明安装成功。



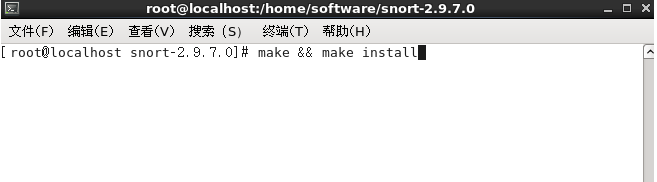
1.10  返回上级目录，解压snort-2.9.7.0。



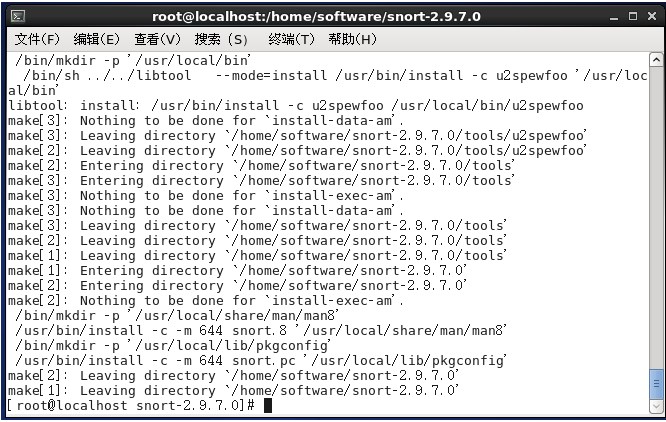
1.11 并使用命令“cd snort-2.9.7.0”进入snort的目录， 执行命令“./configure”对snort-2.9.7.0进行配置。



1.12 进入snort-2.9.7.0目录。执行命令“make && make install”。



1.13  安装完成。

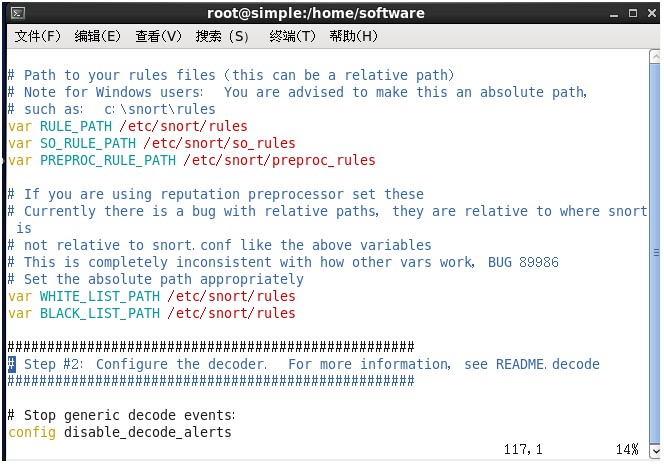


**2、配置snort和barnyard2**

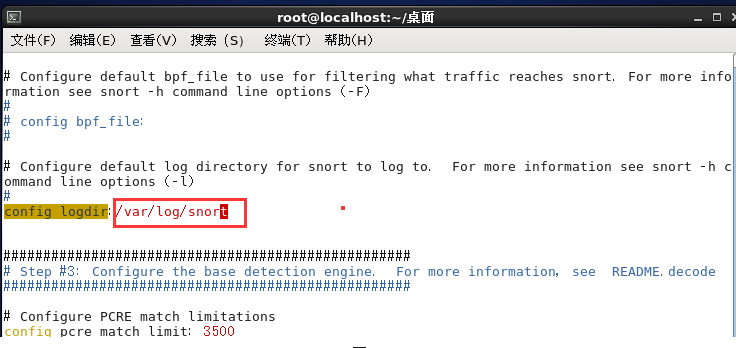
2.1    依次执行以下命令。



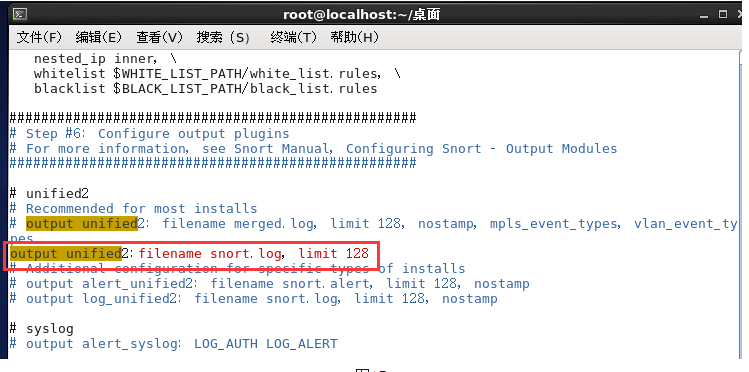
2.2    编辑snort的配置文件，执行命令“vim /etc/snort/snort.conf”。修改路径变量



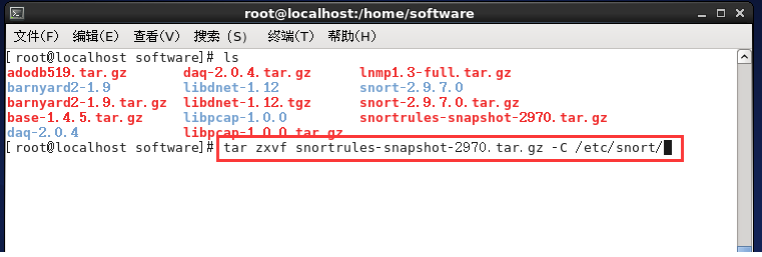
2.3    设置log目录，执行命令“vim /etc/snort/snort.conf”。



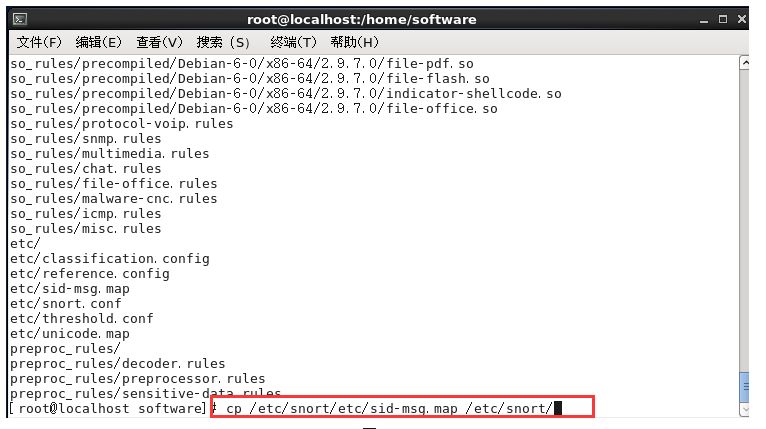
2.4    配置输出插件。



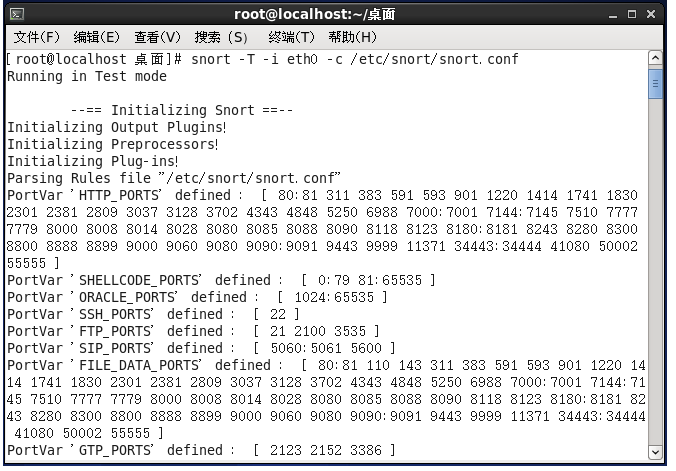
2.5    解压/home/software下的rules文件。



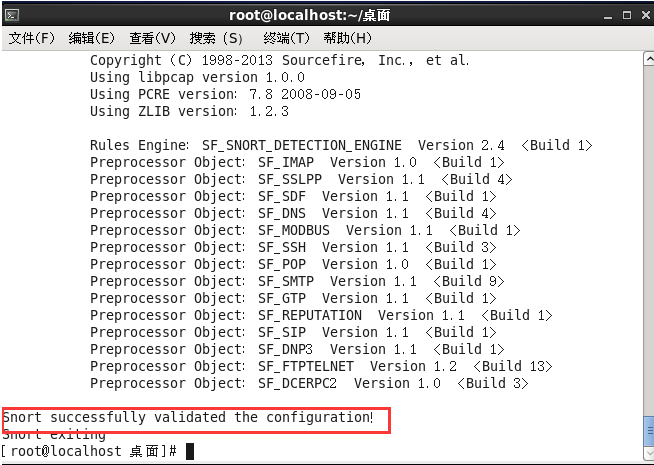
2.6    解压后，将文件sid-msg.map复制到/etc/snort目录下。



2.7    输入命令“snort -T -i eth0 -c /etc/snort/snort.conf”，进行测试。“-T参数为测试的意思，-i指定接口，-c 指定配置文件”。(如果提示失败缺少libsfbpf.so.0依赖，那么先执行命令“ldconfig”，然后再次执行snort的测试命令)。



2.8    得到返回“successful”字样说明，安装及配置成功。



1. 实验结果及分析：
2. 总结及心得体会：