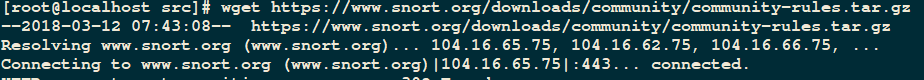
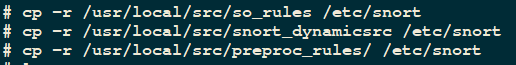
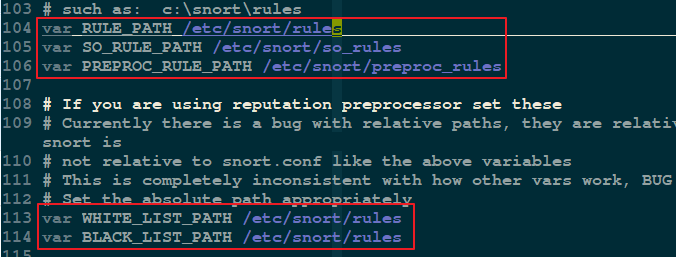
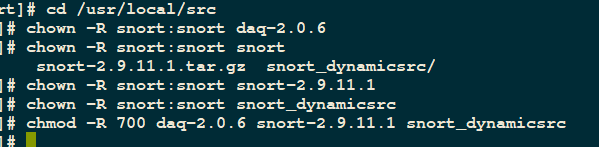
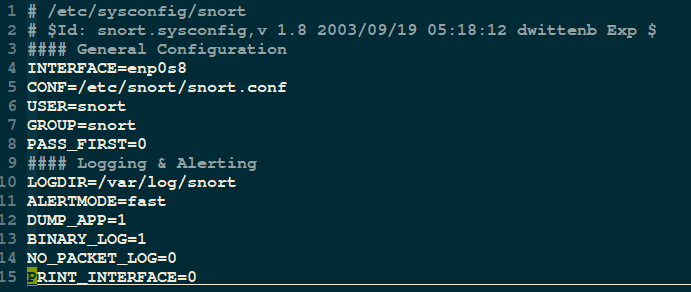
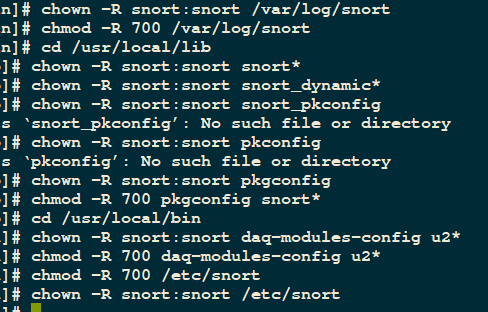
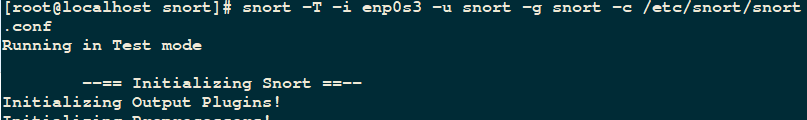
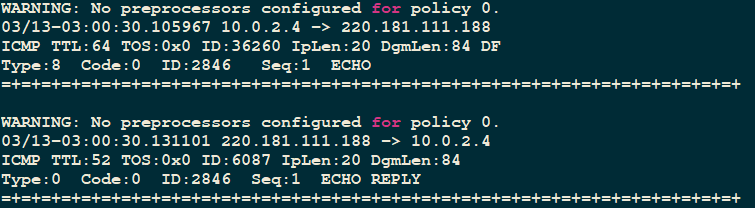
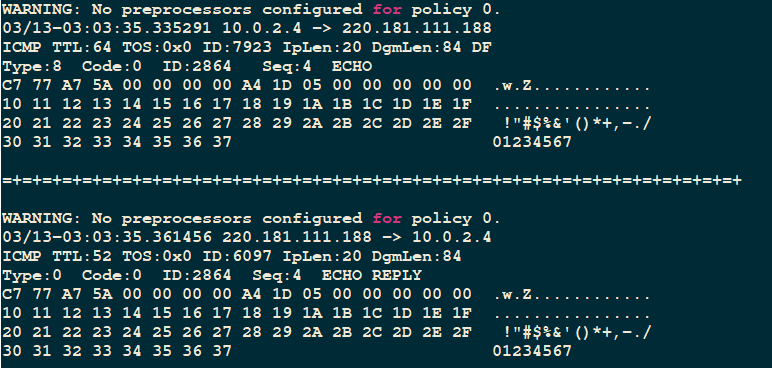
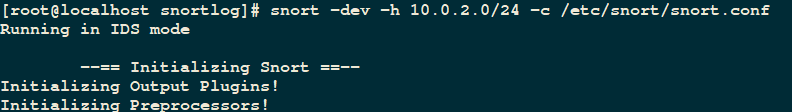
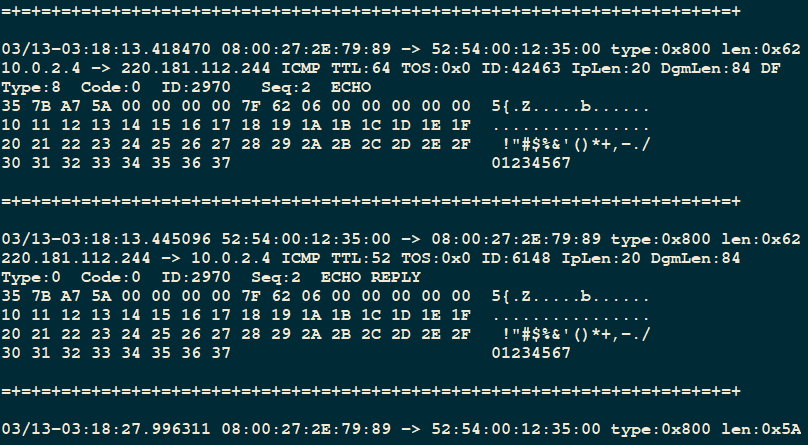
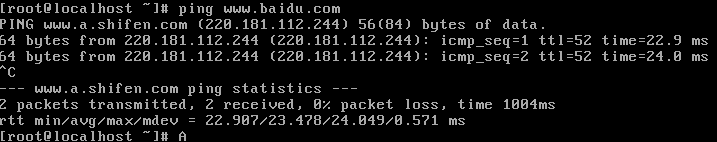
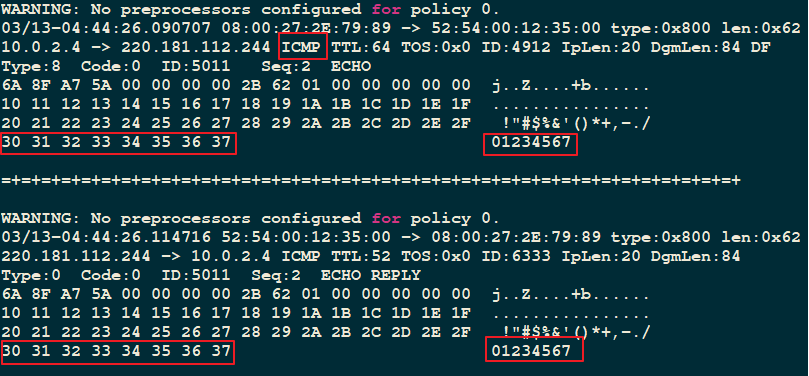
**Snort使用实例**

官网：<https://www.snort.org/>详细设置可参考官方文档

1. **按照官方说明安装snort**
   1. **安装依赖（提前安装centos epel源）  
      gcc flex bison zlib zlib-devel libpcap libpcap-devel pcre pcre-devel zlib zlib-devel libdnet libdnet-devel tcpdump**  
      
   2. **获取源码包**  
        
      地址可从官网获得
   3. **使用tar解压源码包并进入源码目录使用make编译安装**
      1. 进入daq目录，执行（ldconfig重新加载动态库）  
         ./configure  
         make  
         make install  
         cd /usr/local/lib  
         **ldconfig -v /usr/local/lib**
      2. 进入snort目录，执行  
         ./configure –enable-sourcefire  
         make  
         make install  
         cd /usr/local/lib  
         ldconfig -v /usr/local/lib
      3. 在官网下载过滤规则（使用wget下载的规则文件为一个html文档，使用google下载工具下载后，使用samba服务传送至centos服务器）  
         
      4. 拷贝配置文件  
         cd /etc/  
         mkdir snort  
         cd snort  
         cp /usr/local/src/snort\*\*/etc/\* .  
         tar -xvf /usr/local/src/{your rules file path}   
         将rules文件夹整个拷贝至/etc/snort,其余需要拷贝的配置文件在下图列出  
           
         
      5. 添加snort用户和用户组  
           
           
         
      6. 编辑配置文件修改变量内容  
         
      7. 权限设置  
         
      8. 设置文件链接  
         
      9. 编辑文件/etc/sysconfig/snort  
           
         更改权限  
         
      10. 权限设置  
            
          权限设置可以全部放在一起进行，目的是将所有与snort相关的文件所有者设为snort:snort，并将权限更改为700
      11. 测试配置文件设置  
            
          得到如下输出即为配置文件可用  
          
2. **Snort的工作模式**
   1. **嗅探器：将数据包显示在标准输出，使用snort -v,如果要解码应用层，添加-d选项**  
      ping数据包如上图，echo和echo reply，解码应用层如下  
      
   2. **数据包记录：将数据包记录到硬盘上，使用snort -dev -l logdir -h network**之后可通过snort -r logfile读出数据包记录，该记录为二进制文件，无法直接查看
   3. **入侵检测系统：根据已有规则文件检测数据包**snort -dev -l logdir -h network -c configfile  
      logdir default /etc/log/snort,报警记录会被记录在日志中  
        
      
   4. 报警机制（full、fast、socket、syslog、smb、none）  
      通过-A选项设置报警机制，-A fast报警信息包括时间戳、报警信息、源目的IP地址端口，-A full是默认模式，-A unsock发送到unix套接字，-A none关闭。常用选项可用过help查看，man snort可以获取更多帮助
3. **配置snort规则**
   1. **在官网下载规则文件，解压后拷贝至配置文件夹相应（安装过程涵盖）**
4. **编写snort规则**每条规则都包括规则头和规则选项。规则头包括动作、协议、IP地址、子网掩码、端口号，规则选项包括报警信息和异常包的特征码，使用特征码来决定是否采取指定动作。
   1. **规则动作**alert生成警报，并log此数据包  
      log记录此数据包  
      pass丢弃  
      activate报警并激活另一条dynamic规则  
      dynamic保持空闲直到被另一条规则激活
   2. **协议：平时用的通信协议：IP、TCP、UDP、icmp**
   3. **IP地址：netaddr/CIDR**192.168.1.0/24,可使用！操作符取非，可用[]指定IP地址列表，比如  
      [192.168.1.0/24,192.168.2.0],  
      用any表示任何主机
   4. **端口号**any表示任意端口，使用单个数字表示静态单个端口，使用num：num2表示端口范围，使用：num2表示从1-num2的所有端口
   5. **方向操作符：->,<>**
   6. **Activate、dynamic规则对**activate tcp !HOME\_NET any -> $HOME\_NET 143 (flagsA;content:”|089da|”;activates:1;<msg:”message to log”)  
      dynamic tcp !$HOME\_NET any -> $HOME\_NET (activated\_by:1;count:100;)  
      当第一条规则检测时，触发第二条规则，记录count个数据包
   7. **重要指令：include、var顾名思义**
   8. **规则选项：**
      1. Msg：“”；提示字符串
      2. Logto：“”；将触发该规则的包记录进某个文件中
      3. 更多选项参见snort manual
5. **测试：简便，编写记录icmp ping数据包**
   1. **编写简单规则如下**
   2. **运行snort**
   3. **在本地ping百度服务**
   4. **控制终端看到**
   5. **查看日志文件**