1. 实验项目名称：

嗅探器模式

1. 实验原理：

1) 嗅探器模式仅仅是从网络上读取数据包并作为连续不断的流显示在终端上。

1. 实验目的：

1)  学习snort的工作模式

1. 实验器材（设备、虚拟机名称）：

服务器centos 192.168.1.2 PC 192.168.1.3

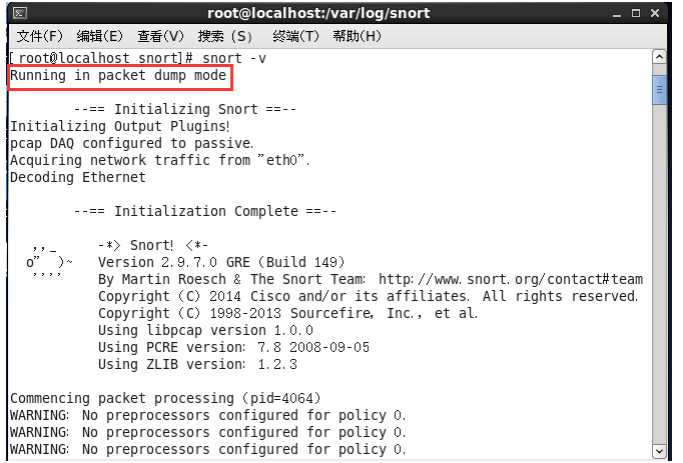
1. 实验步骤：

1. **嗅探模式**

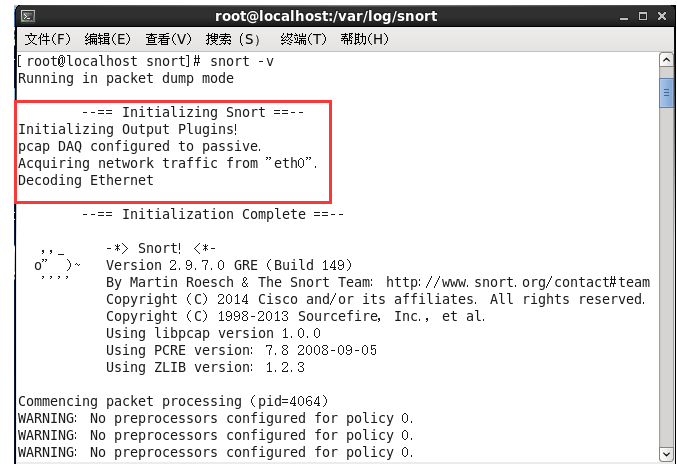
1.1    打开192.168.1.2主机上的终端。输入命令“snort -v”，进行snort的启动。



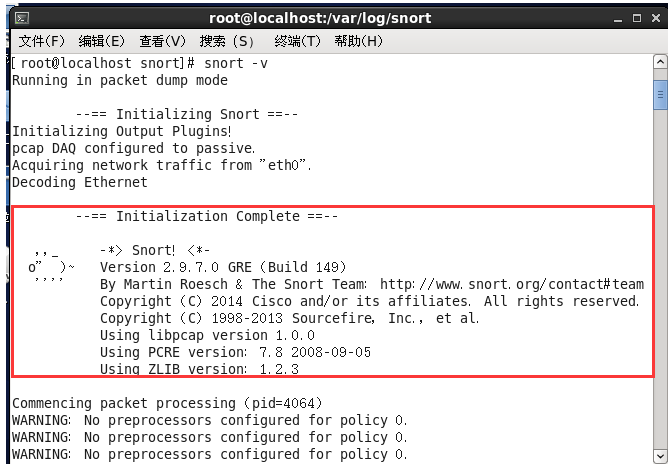
1.2    启动snort会得到回显。红框部分为当前运行的模式。



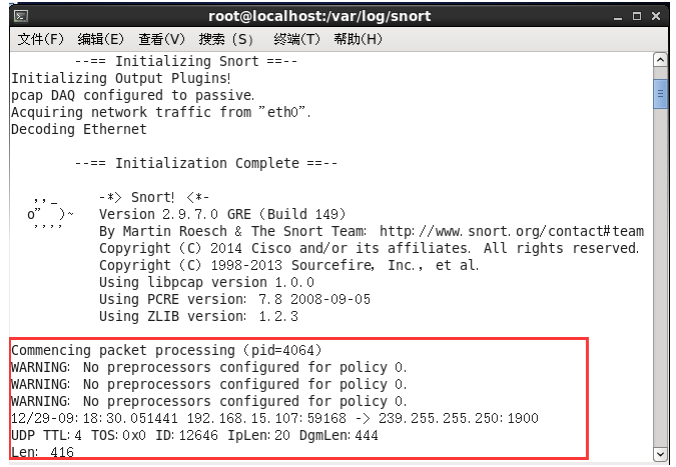
1.3    初始化输出插件部分。



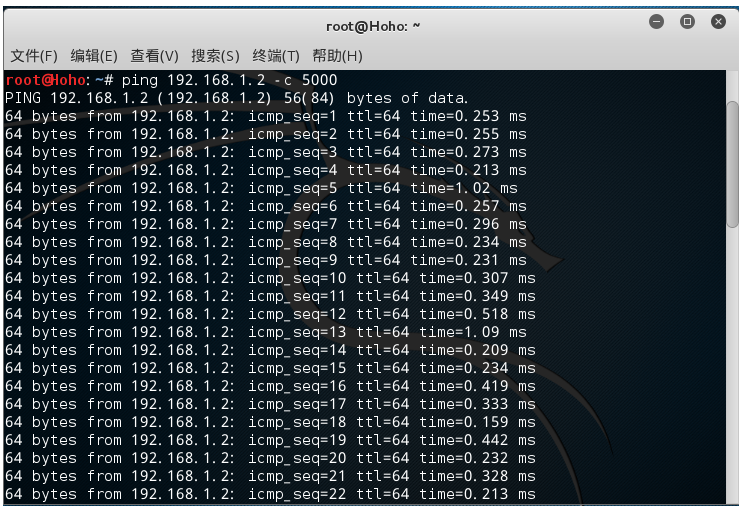
1.4    snort版本及版权信息。



1.5    数据包控制台的部分。

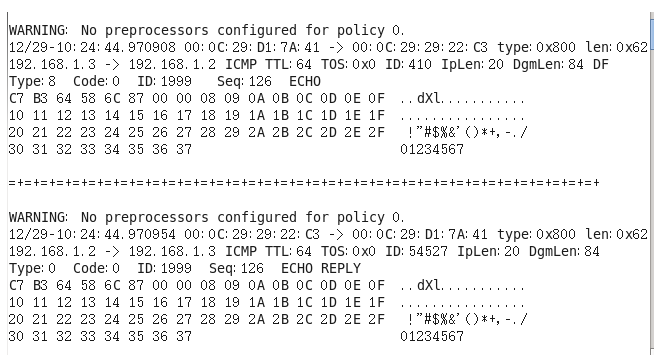


**二、实例分析**

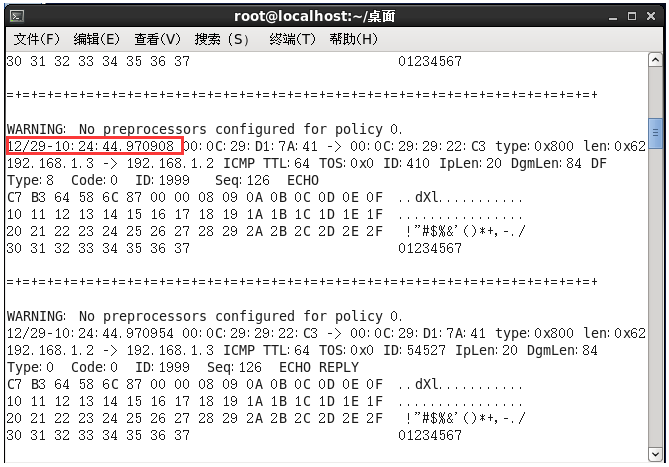
2.1    登录客户机192.168.1.3，打开终端输入命令“ping 192.168.1.2 –c 5000”(若客户机为windows操作系统，在cmd下执行命令"ping 192.168.1.2 -t"即可)。

2.2    切换到192.168.1.2的主机，打开终端输入命令“snort -i eth0 -vde”命令。



2.3    截取完整数据包进行分析。

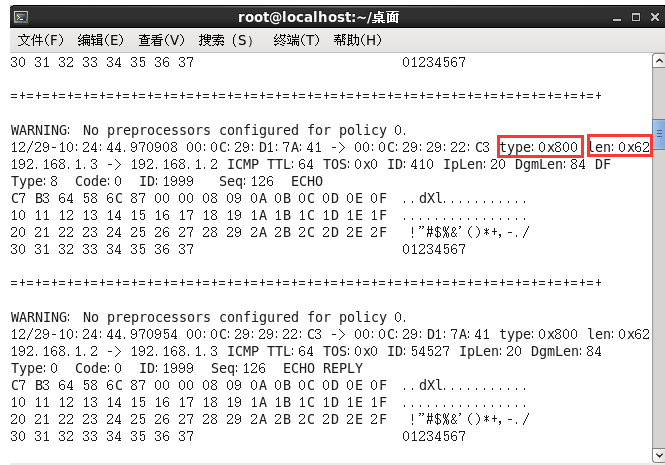
2.4    数据包中包含的信息有包捕获的时间。



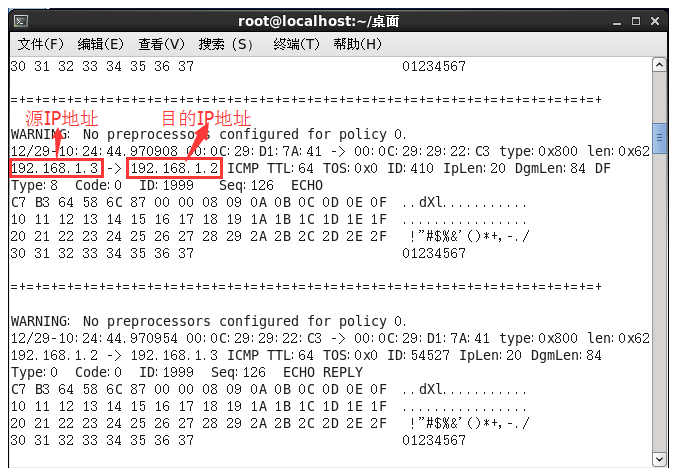
2.5    源MAC地址及目的MAC地址。



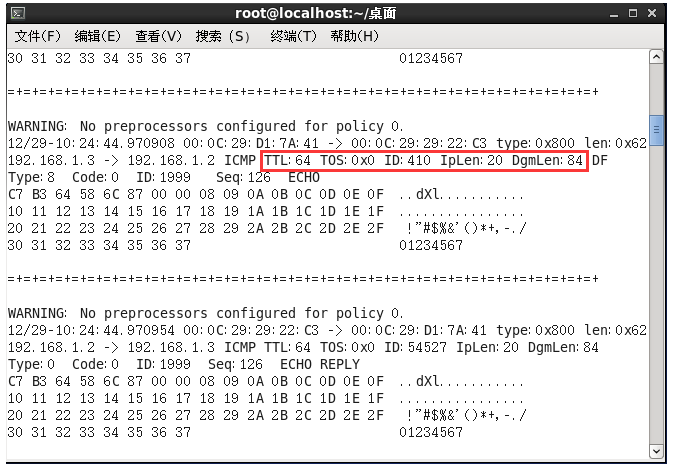
2.6    数据帧所负载的上层协议类型为IP（0x800），总长度为（0x62）。



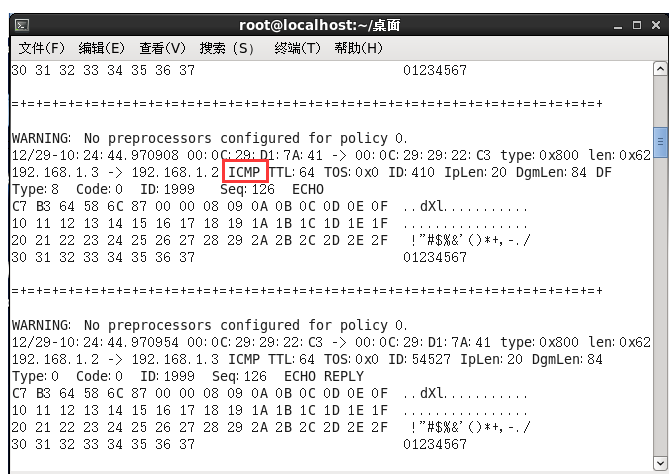
2.7    源IP地址为192.168.1.3，目的地址为192.168.1.2。



2.8    IP头中的TTL值是64，TOS值为0。IP长度为20，IP载荷是84字节。



2.9    包的传输协议为ICMP。



1. 实验结果及分析：
2. 总结及心得体会：