1. 实验项目名称：

实验5-2-base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：

1)        熟悉base的安装和配置

1. 实验器材（设备、虚拟机名称）：

CentOS6.5：192.168.1.2

1. 实验步骤：

1. **修改LAMP环境**

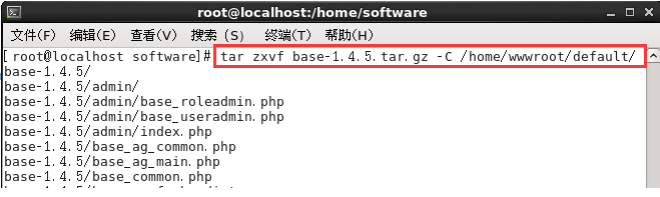
1    打开终端，进入目录“/home/software/”，查看当前目录下的文件。输入“tar zxvf adodb519.tar.gz –C /home/wwwroot/default”。



1.2    解压完成后，将文件夹重命名为adodb。执行命令“mv /home/wwwroot/default/adodb5 /home/wwwroot/default/adodb”。



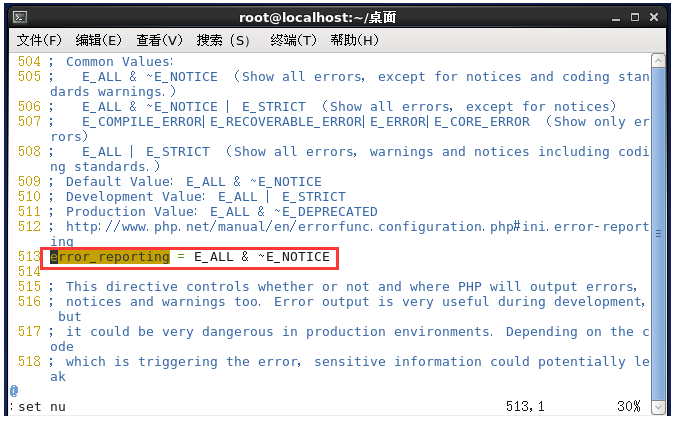
1.3    解压“/home/software”目录下的base-1.4.5.tar.gz，解压到文件夹“/home/wwwroot/default/”下。



1.4    将解压后的文件夹重命名为base。



1.5    修改php.ini的配置信息，php.ini文件在“/etc”目录下。

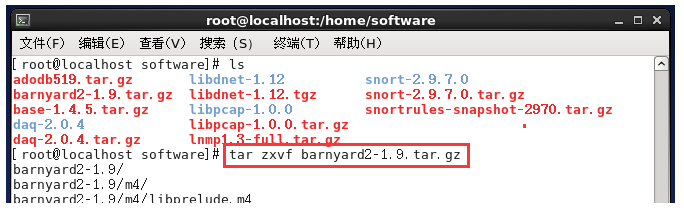


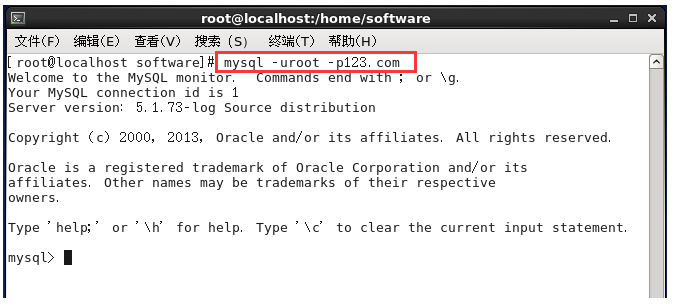
1.6    设置default目录的权限，“chown –R apache:apache /home/wwwroot/default”。

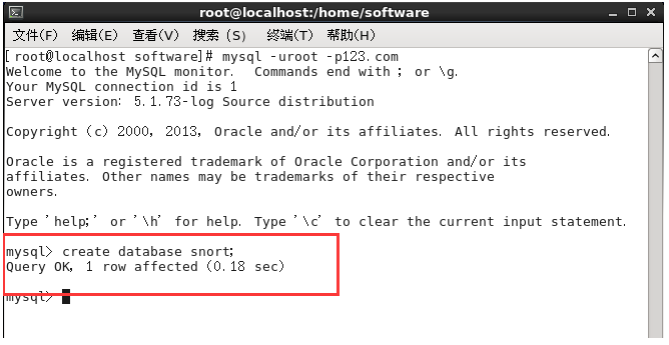


1.7    修改default文件夹的权限。

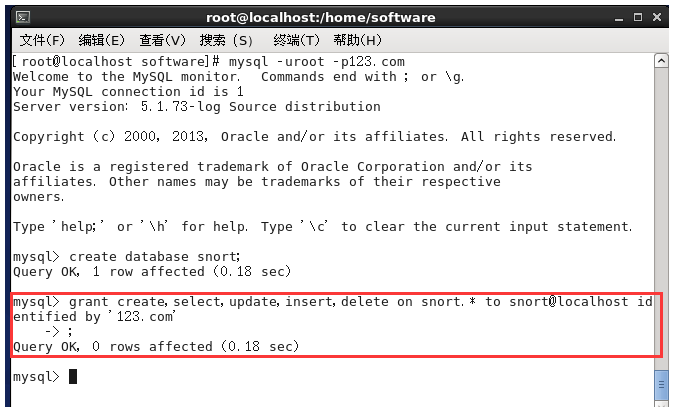


1.8    解压“/home/software”目录下的barnyard2-1.9.tar.gz（压缩包中有需要用到的文件）。

1.9    启动mysql，命令为“mysql –uroot –p123.com”，用户名为“root”，密码为“123.com”。

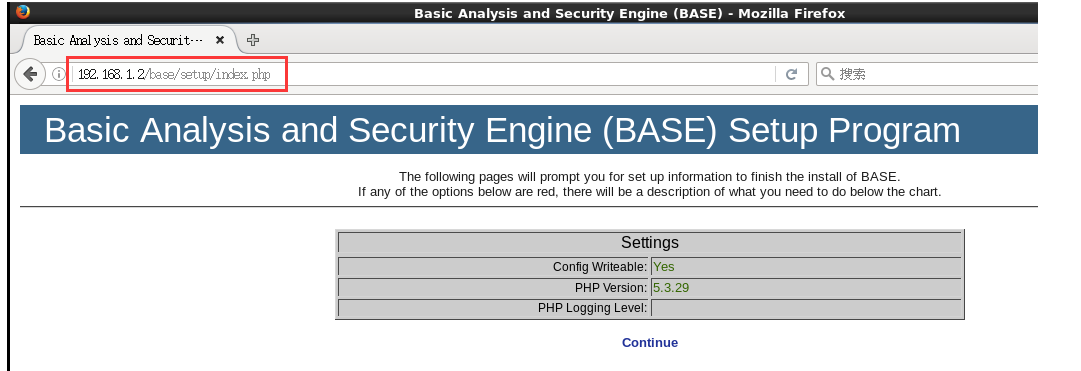
1.10  创建名为“snort”的数据库。

1.11  给数据库用户赋予snort数据库的权限。

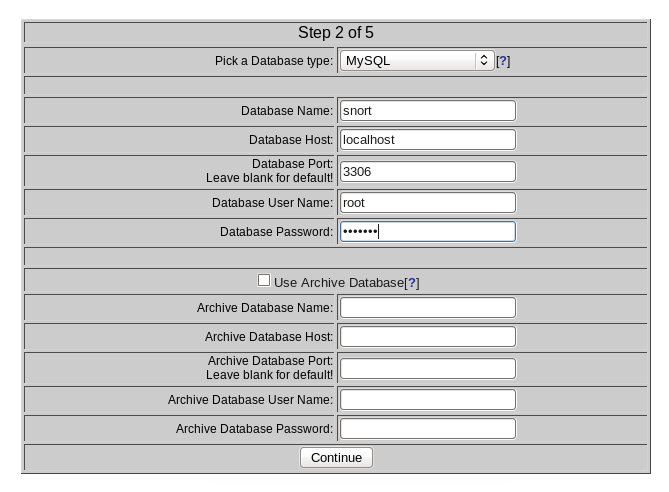


1.12  退出数据库，返回终端状态输入命令“mysql –usnort –p123.com –D snort < /home/software/barnyard2-1.9/schemas/create\_mysql”将barnyard2-1.9文件中的数据导入。

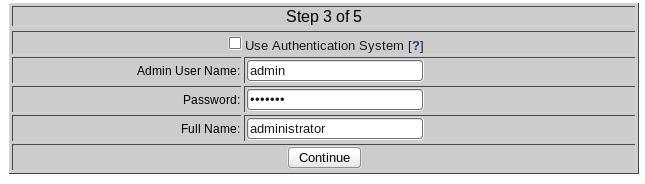


1.13  使用浏览器访问http://192.168.1.2/base/setup/index.php得到如图反馈信息，说明base环境安装成功。并单击continue按钮。若单击continue按钮后报错，应把/home/wwwroot/defaule/base/base\_conf.php文件删除。

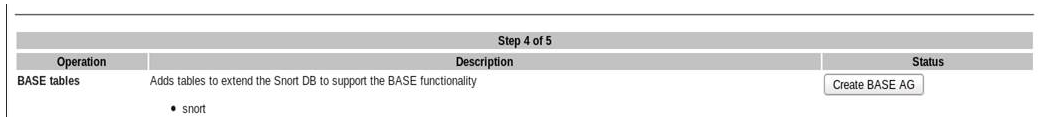
1.14  在第一个选项中选择简体中文“simplified\_chinese”，第二输入框中输入adodb的路径 “/home/wwwroot/default/adodb”。并单击continue按钮。

1.15  依次输入数据库名称“snort”，数据库地址“localhost”，数据库端口“3306”，数据库用户名“root”，数据库密码“123.com”。图中下半部分不在这里使用，单击continue按钮。

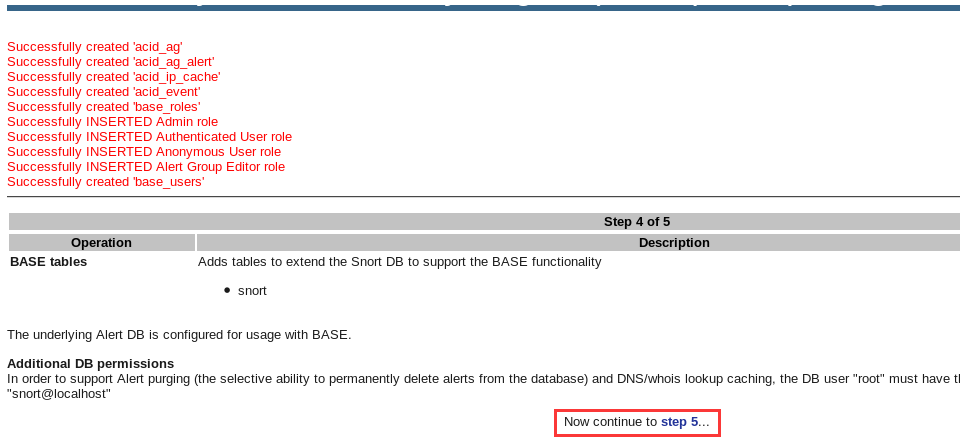
1.16  输入管理员名称“admin”，密码设置为“123.com”，全名为“administrator”。单击continue按钮。

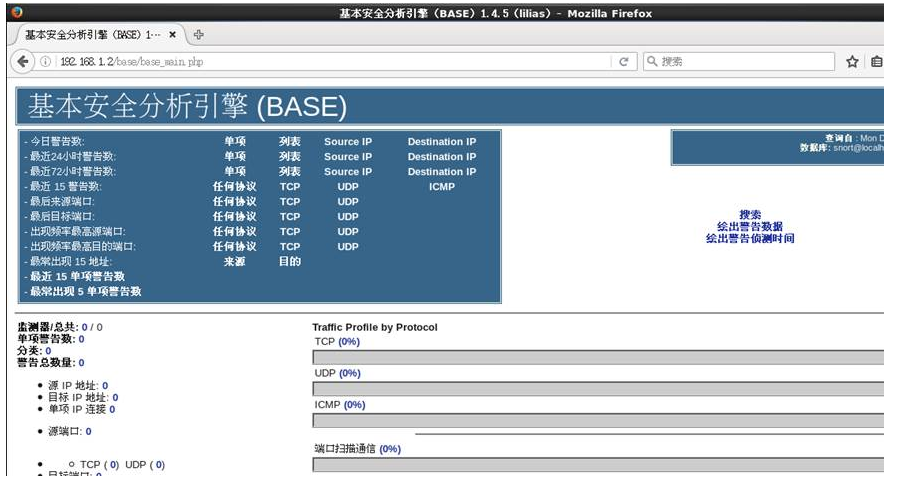


1.17  单击“create base AG”按钮。



1.18  系统会自动创建，创建信息为图中红色文字，单击step 5按钮。



1.19  跳转至base安全分析的主页。

1. 实验结果及分析：
2. 总结及心得体会：