网络入侵检测系统（Snort）实验 实验平台的搭建和测试

原创

duoaduo 于 2012-02-23 16:37:46 发布 5943 收藏 6
分类专栏： 技术类 文章标签： 网络 平台 apache php archive mysql

本文链接：https://blog.csdn.net/duoaduo618/article/details/7287700

（晕，怎么不能粘贴图片啊，先发文档，图片慢慢加吧····）当初做实验的时候，参看了网上很多文章，但是因为每个机子的环境不一样所以要根据自己的机子进行调试才能出来想要的结果。恩。就是这样·（这个是自己论文里的一部分，所以会出现类似4.1这样的编号 ）

4.1实验平台的搭建

1）实验软件：

（1）Microsoft virtual pc虚拟机

（2）windows server 2003镜像文件

（3）网络数据包截取驱动程序

WinPcap_4_1_2.zip

http://winpcap.polito.it/

（4）Windows 版本的Snort 安装包

Snort_2_9_0_5_Installer.exe

http://www.snort.org/

（5）Windows 版本的Apache Web 服务器

apache_2.2.4-win32-x86-no_ssl.zip

http://www.apache.org/

（6）Windows版本的PHP脚本环境支持

php-5.2.5-Win32.zip

http://www.php.net/

（7）Windows 版本的Mysql 数据库服务器

mysql-5.0.22-win32.zip

http://www.mysql.com/

（8）ACID（Analysis Console for Intrusion Databases）基于PHP的入侵检测数据库分析控制台

acid-0.9.6b23.tar.gz

http://www.cert.org/kb/acid

（9）Adodb（Active Data Objects Data Base）PHP库

adodb504.tgz

http://php.weblogs.com/adodb

（10）PHP图形库

jpgraph-2.3.tar.gz

http://www.aditus.nu/jpgraph

（11）snort 规则包

rules20090505.tar.gz

http://www.snort.org

2）安装步骤如下

（1）虚拟机和操作系统的安装

运行虚拟机安装程序，默认安装即可，打开控制台，新建一个虚拟机，按照提示具体填写，选择镜像文件，启动，安装好镜像系统后，效果如下：

图4-1 虚拟机

（2）组件的安装

在c:下建立duoduo的文件夹，再在其下建立duo的文件夹放入所有的安装程序，在后续的安装时，把可以选择安装路径的组件安装在duoduo的文件夹下

①安装WinPcap

运行WinPcap_4_1_2.zip，默认安装。

②安装mysql

运行mysql-5.0.22-win32.zip，选择自定义安装选择安装路径C:\duoaduo\mysql下，安装时注意：端口设置为3306（以后要用到），密码本实验设置成123，

图4-2 配置端口

图4-3 配置密码

添加环境变量：

图4-4 配置环境变量

③安装apache

运行apache_2.2.4-win32-x86-no_ssl.zip

安装到c:\duoaduo\apache

④下面安装php

解压php-5.2.5-Win32到c:\duoaduo\php

添加gd图形库支持

复制c:\duoaduo\php\php5ts.dll和c: \duoaduo\php\libmysql.dll文件到%systemroot%\system32

查询本机的%systemroot%

图4-5 查询机的%systemroot%

复制c: \duoaduo\php\php.ini-dist到%systemroot%并重命名为php.ini，
修改php.ini，分别去掉“extension=php_gd2.dll”和“extension=php_mysql.dll”前的分号，

图4-6 配置php.lni(1)

并指定extension_dir="c:\duoaduo\php\ext"，

图4-7配置php.lni(2)

同时复制c:\duoaduo\php\ext下的php_gd2.dll与php_mysql.dll到%systemroot%\system32

在C:\duoaduo\apache\conf\httpd.conf中添加LoadModule php5_module c:/duoaduo/php/php5apache2_2.dll和AddType application/x-httpd-php .php，AddType application/x-httpd-php-source .phps

图4-8 配置httpd.conf

重启Apache服务。

在C:\duoaduo\apache\htdocs目录下新建webinf.php（文件内容为：<?phpinfo();?>）并使用http://127.0.0.1/webinf.php访问测试是否能够显示当前Apache服务器的信息，如果显示如图4-9所示，则表明Apache和php工作基本正常。

图4-9 正确运行Apache和php

如果显示如图4-10所示，则表明Apache和php工作不正常。

图4-10 错误信息

原因是 addtype 的那两句话有错误，检查修改就可以了。

⑤安装Snort

运行Snort_2_9_0_5_Installer.exe

安装在C:\duoaduo\Snort下即可，

运行C:\duoaduo\Snort\bin\snort.exe

或者在DOS中找到该位置，

如果安装 snort成功会出现一个可爱的小猪

图4-11 Snort运行正常

并按照以下修改C:\duoaduo\Snort\etc\snort.conf文件：

var RULE_PATH c:\duoaduo\snort\rules

include classification.config

include reference.config

修改为绝对路径：

include c:\duoaduo\snort\etc\classification.config

include c:\duoaduo\snort\etc\reference.config

在该文件的最后加入下面语句：

output database: alert, mysql, host=localhost user=root password=123 dbname=snort encoding=hex detail=full

创建 snort 数据库的表

复制 c:\duoaduo\snort\schames 文件夹下的create_mysql 文件到C:\duoaduo\mysql\bin文件夹下

打开 mysql 的的客户端执行如下命令

Create database snort;

Create database snort_archive;

Use snort;

Source create_mysql;

Use snort_archive;

Source create_mysql;

Grant all on *.* to “root”@”localhost”

加入 php 对 mysql 的支持：

修改 c:\windows\php.ini 文件去掉 extension=php_mysql.dll 前的分号。

复制c:\duoaduo\php\ext 文件夹下的 php_mysql.dll 文件到 c:\windows 文件夹。

复制c:\duoaduo\php\libmysql.dll文件到c:\windows\system32下

⑥安装 adodb

解压缩 adodb 到 c:\ids\php5\adodb 文件夹下。

⑦安装 jgraph

解压缩 jpgraph 到 c:\duoaduo\php\jpgraph 文件夹下

⑧安装 acid

解压缩 acid 到 c\duoaduo\apache\htdocs\acid 文件夹下

修改 acid_conf.php 文件

为以下内容

```
$DBlib_path="c:\duoaduo\php\adodb";
$DBtype="mysql";
$alert_dbname ="snort";
$alert_host = "localhost";
$alert_port ="3306";
$alert_user="root";
$alert_password="123";
$archive_dbname="snort_archive";
$archive_host="localhost";
$archive_port="3306";
$archive_user="root";
$archive_password="123";
$ChartLib_path="c:\duoaduo\php\jpgraph\src";
```

⑨重启apache、mysql服务

⑩在浏览器中初始化acid数据库

http://localhost/acid/acid_db_setup.php

以上配置正确会有下面的显示：

图4-12 正确配置acid

安装成功，测试一下：

启动Apache和mysql服务

运行ACID：打开浏览器，地址为http://127.0.0.1/acid。如果有下图所示，则表示ACID安装成功。

图4-13正确安装acid

运行c:\duoaduo\snort\bin>snort -c "c:\duoaduo\snort\etc\snort.conf" -l "c:\duoaduo\snort\log" -vdeX

-X 参数用于在数据链接层记录raw packet 数据

-d 参数记录应用层的数据

-e 参数显示 / 记录第二层报文头数据

-c 参数用以指定snort 的配置文件的路径

-v 参数用于在屏幕上显示被抓到的包

图4-14 正确记录日志

4.2实验测试

1）Snort的使用：

（1）嗅探器:所谓的嗅探器模式就是Snort从网络上读出数据包然后显示在你的控制台上。

①如果你只要把TCP/IP包头信息打印在屏幕上，只需要输入下面的命令：

./snort–V

图4-15 运行./snort–V

②如果要把所有的包记录到硬盘上，你需要指定一个日志目录，snort就会自动记录数据包：./snort -dev -l ./log

图4-16 运行./snort -dev -l ./log

这时会在相应文件夹下，记录数据：

图4-17 文件记录信息

（2）网络入侵检测系统:Snort最重要的用途还是作为网络入侵检测系统(NIDS)，使用下面命令行可以启动这种模式：

./snort -dev -l ./log -h ***.***.***.***/** -c snort.conf

图4-18运行网络入侵检测命令

（3）网络入侵检测模式下的输出选项

在NIDS模式下，有很多的方式来配置Snort的输出。在默认情况下,Snort以ASCII格式记录日志，使用full报警机制。如果使用full报警机制，snort会在包头之后打印报警消息。使用-s选项可以使Snort把报警消息发送到syslog，默认的设备是LOG_AUTHPRIV和LOG_ALERT。可以修改snort.conf文件修改其配置。Snort还可以使用SMB报警机制，通过SAMBA把报警消息发送到Windows主机。为了使用这个报警机制，在运行./configure脚本时，必须使用--enable-smbalerts选项。

下面是一些输出配置的例子：使用默认的日志方式(以解码的ASCII格式)并且把报警发./snort -c snort.conf -l ./log -s -H给syslog：

具体本实验环境运行:\snort -c c:\duoaduo\snort\etc\snort.conf -l c:\duoaduo\snort\log -s -H

图4-19运行网络入侵检测模式下的输出选项（1）

图4-20 运行网络入侵检测模式下的输出选项（2）

2）Snort与控制台，数据库的使用检测：

（1）设置监测包含的规则。

找到snort.conf文件中描述规则的部分，如下图所示：

图4-21 配置snort.conf

前面加＃表示该规则没有启用，将local.rules之前的＃号去掉，其余规则保持不变

（2）运行C:\duoaduo\Snort\bin中的snort.exe, 不关闭窗口，浏览网页

（3）打开acid检测控制台主界面

图4-22 显示数据

点击右侧图示中TCP后的数字“1%”，将显示所有检测到的TCP协议日志详细情况

图4-23 详细信息（1）

TCP协议日志网页中的选项依次为：流量类型、时间戳、源地址、目标地址以及协议

选择控制条中的“home”返回控制台主界面，在主界面的下部有流量分析及归类选项，

图4-24 流量分析及归类选项

图4-25 近24小时的数据流

可以看到，表中详细记录了各类型流量的种类、在总日志中所占的比例、出现该类流量的起始和终止时间等详细分析。

点击第一条信息的起始时间2008-02-13 01:49:01会显示起详细的信息。

图4-26 详细信息(1)

图4-27 详细信息(2)

控制台中所以以蓝色显示的都可以点击以查看详细数据。在此就不一一演示了。