**网络信息安全**

**实验报告**

学号： 2220193816

姓名： 赤凯

班级： 网络2班

报告日期：2022年6月25

实验三： 网络攻防实验

**【实验目的】**

**1、掌握基于snort的入侵检测系统的搭建步骤；**

**2、掌握常见的网络攻击方式，并学会使用snort检测攻击；**

**【实验内容】**

**1、使用snort搭建入侵检测系统；**

**2、设计攻击，并使用入侵检测系统检测攻击；**

**【实验环境】**

**Ubuntu 18.04 LTS**

**【实验步骤】**

1. **安装库环境**

sudo apt-get update -y

sudo apt-get dist-upgrade -y

sudo apt-get install -y zlib1g-dev liblzma-dev openssl libssl-dev

sudo apt-get install -y build-essential bison flex

sudo apt-get install -y libpcap-dev libpcre3-dev libdumbnet-dev libnghttp2-dev

sudo apt-get install -y mysql-server libmysqlclient-dev mysql-client autoconf libtool

sudo apt-get install -y libcrypt-ssleay-perl liblwp-useragent-determined-perl libwww-perl

sudo add-apt-repository ppa:ondrej/php

sudo apt-get update -y

sudo apt-get install -y apache2 libapache2-mod-php5.6 php5.6 php5.6-common php5.6-gd php5.6-cli php5.6-xml php5.6-mysql

sudo apt-get install -y php-pear libphp-adodb

1. **下载软件包**

wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz

wget https://www.snort.org/downloads/snort/snort-2.9.16.tar.gz

wget https://github.com/firnsy/barnyard2/archive/v2-1.13.tar.gz -O barnyard2-2-1.13.tar.gz

wget https://github.com/shirkdog/pulledpork/archive/v0.7.3.tar.gz -O pulledpork-v0.7.3.tar.gz

wget https://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-520-for-php5/adodb-5.20.8.tar.gz

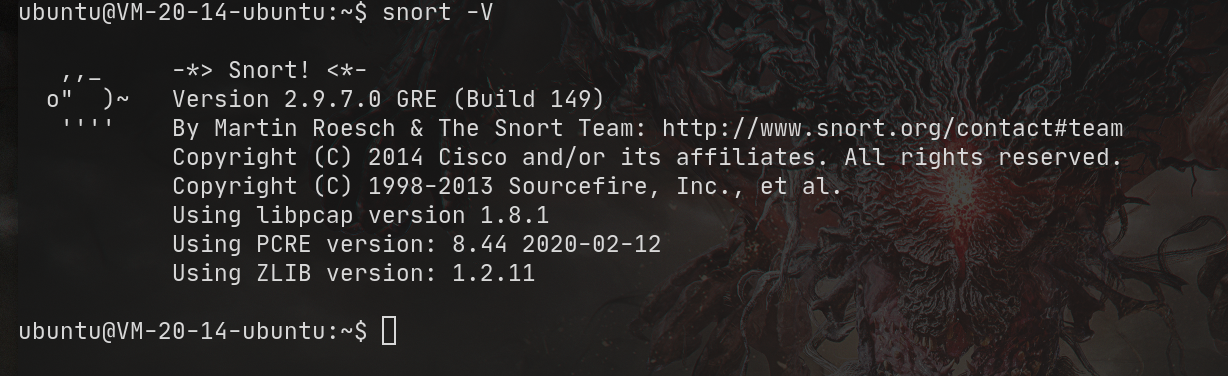
wget http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz

1. **安装snort**

**在ubuntu 18.04 中，可以直接使用命令安装:**

sudo apt install snort

**安装成功后输入命令可以看到如下界面:**

**配置用户环境**

# Create the snort user and group:

sudo groupadd snort

sudo useradd snort -r -s /sbin/nologin -c SNORT\_IDS -g snort

# Create the Snort directories:

sudo mkdir /etc/snort

sudo mkdir /etc/snort/rules

sudo mkdir /etc/snort/rules/iplists

sudo mkdir /etc/snort/preproc\_rules

sudo mkdir /usr/local/lib/snort\_dynamicrules

sudo mkdir /etc/snort/so\_rules

# Create some files that stores rules and ip lists

sudo touch /etc/snort/rules/iplists/black\_list.rules

sudo touch /etc/snort/rules/iplists/white\_list.rules

sudo touch /etc/snort/rules/local.rules

sudo touch /etc/snort/sid-msg.map

# Create our logging directories:

sudo mkdir /var/log/snort

sudo mkdir /var/log/snort/archived\_logs

# Adjust permissions:

sudo chmod -R 5775 /etc/snort

sudo chmod -R 5775 /var/log/snort

sudo chmod -R 5775 /var/log/snort/archived\_logs

sudo chmod -R 5775 /etc/snort/so\_rules

sudo chmod -R 5775 /usr/local/lib/snort\_dynamicrules

# Change Ownership on folders:

sudo chown -R snort:snort /etc/snort

sudo chown -R snort:snort /var/log/snort

sudo chown -R snort:snort /usr/local/lib/snort\_dynamicrules

**修改snort.conf 配置**

sudo vi /etc/snort/snort.conf

#第45行，ipvar HOME\_NET修改为本机的内部网络

ipvar HOME\_NET 192.168.146.130/24

#第104行，设置以下配置文件路径

var RULE\_PATH /etc/snort/rules

var SO\_RULE\_PATH /etc/snort/so\_rules

var PREPROC\_RULE\_PATH /etc/snort/preproc\_rules

var WHITE\_LIST\_PATH /etc/snort/rules/iplists

var BLACK\_LIST\_PATH /etc/snort/rules/iplists

#第521行添加

# output unified2: filename merged.log, l imit 128, nostamp, mpls event types, vlan event types }

output unified2: filename snort.u2, limit 128

#第546行取消注释，启用local.rules文件

include $RULE\_PATH/local.rules

**添加一条测试规则**

sudo vi /etc/snort/rules/local.rules

alert icmp any any -> $HOME\_NET any (msg:"ICMP Test detected!!!"; classtype:icmp-event; sid:10000001; rev:001; GID:1; )

sudo vi /etc/snort/sid-msg.map

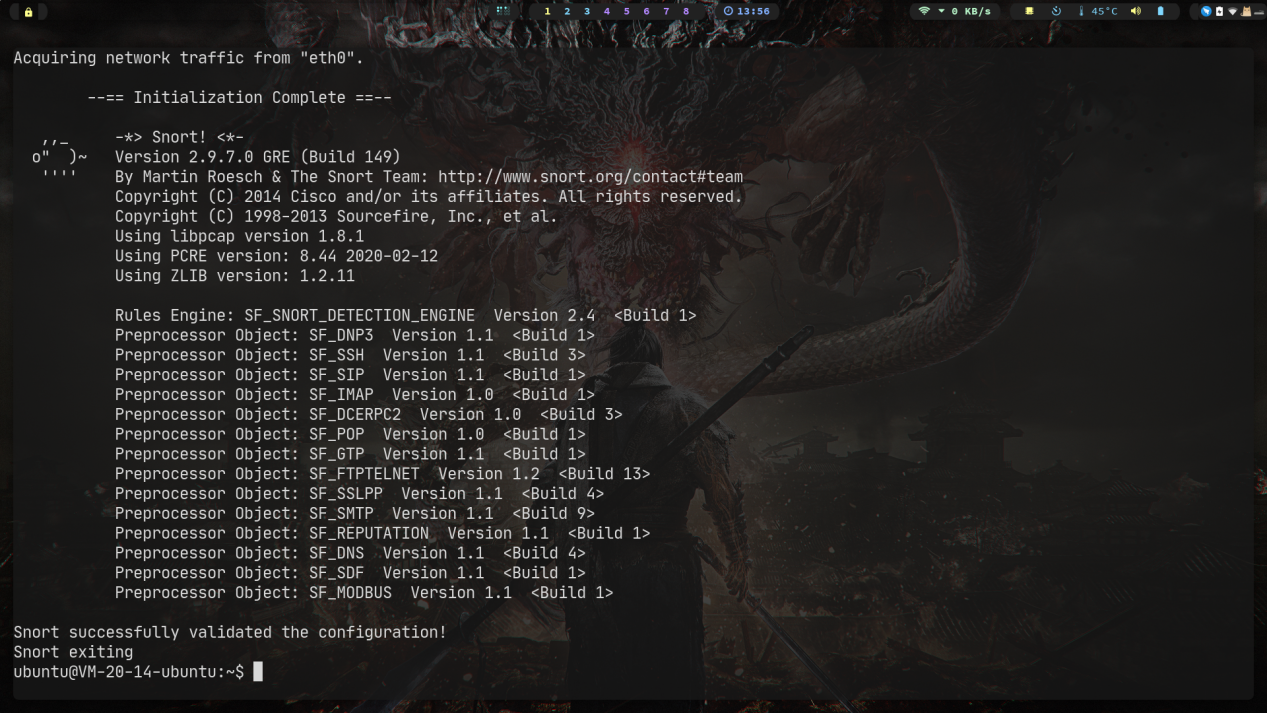
#v2

1 || 10000001 || 001 || icmp-event || 0 || ICMP Test detected || url,tools.ietf.org/html/rfc792

**测试配置文件**

sudo snort -T -c /etc/snort/snort.conf -i ens33

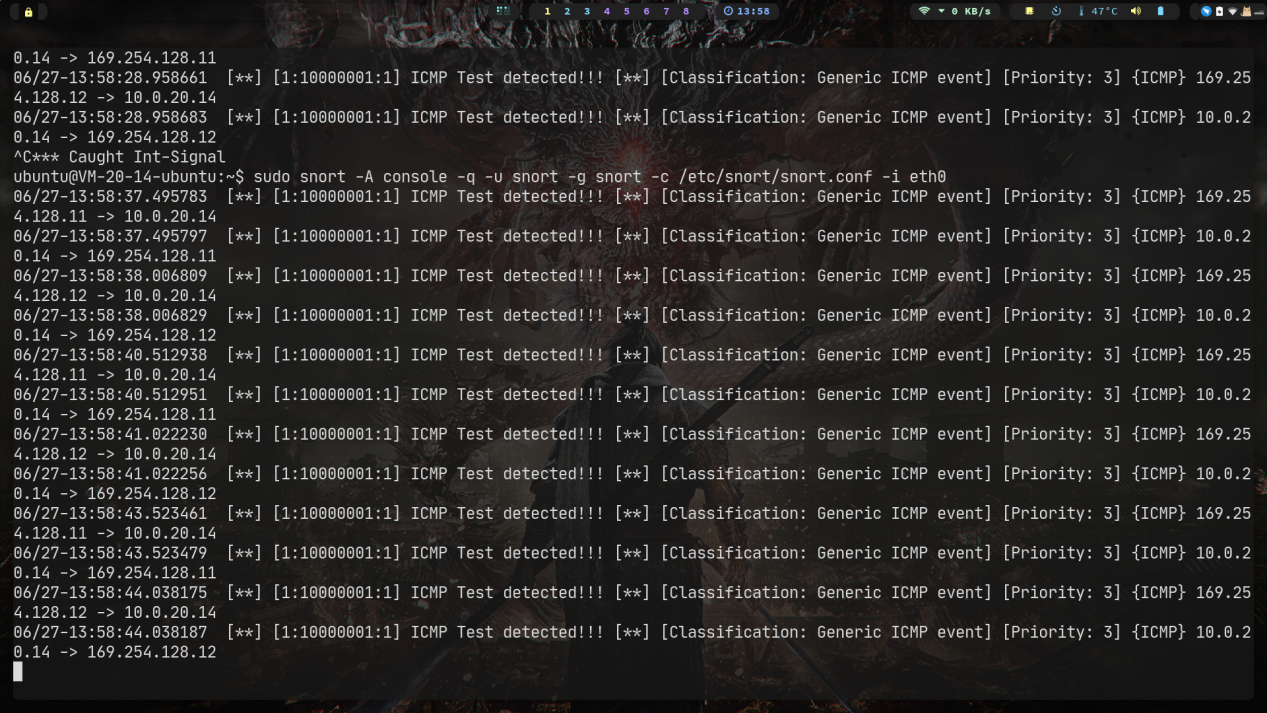
可以看到如图:



这时启动snort:

sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0

可以看到正在检测:



**4 安装Barnyard2**

tar zxvf barnyard2-2-1.13.tar.gz

cd barnyard2-2-1.13

autoreconf -fvi -I ./

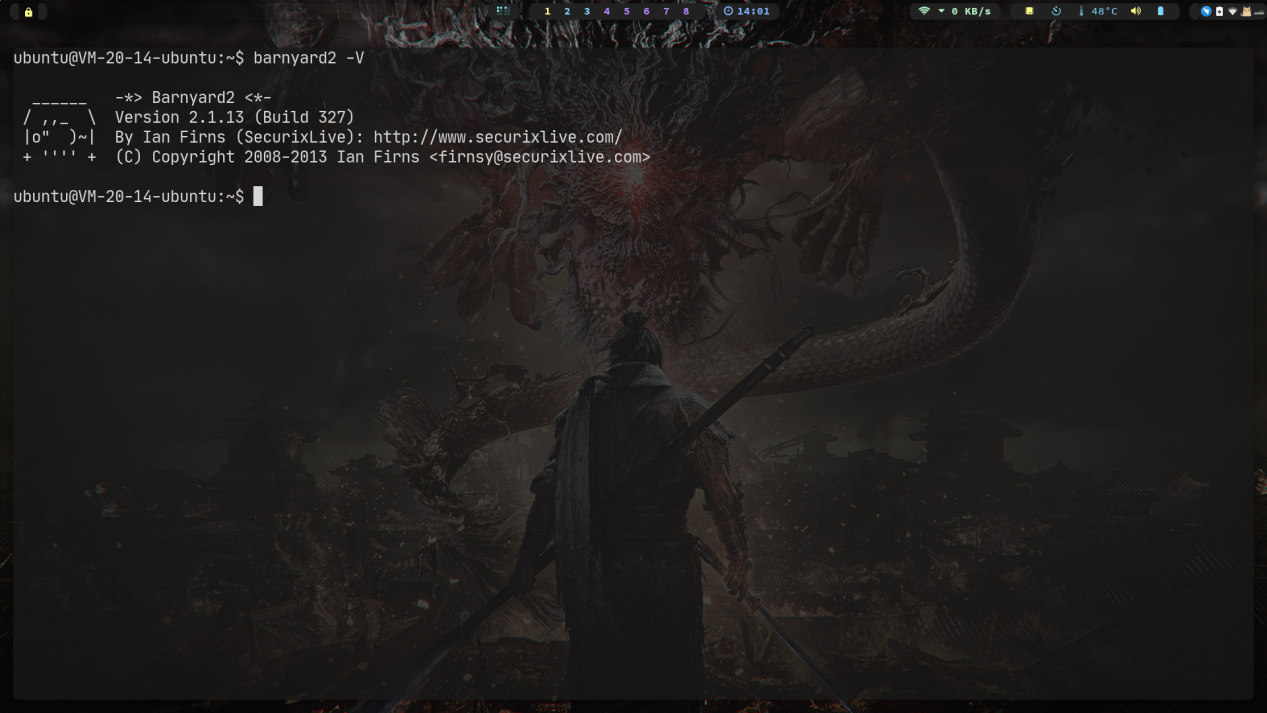
# Choose ONE of these two commands to run

./configure --with-mysql --with-mysql-libraries=/usr/lib/x86\_64-linux-gnu

./configure --with-mysql --with-mysql-libraries=/usr/lib/i386-linux-gnu

sudo make && sudo make install

**输入命令可以看到:**

****

**设置配置文件**

sudo cp ~/barnyard2-2-1.13/etc/barnyard2.conf /etc/snort/

# the /var/log/barnyard2 folder is never used or referenced

# but barnyard2 will error without it existing

sudo mkdir /var/log/barnyard2

sudo chown snort.snort /var/log/barnyard2

sudo touch /var/log/snort/barnyard2.waldo

sudo chown snort.snort /var/log/snort/barnyard2.waldo

**配置数据库**

ubuntu@ubuntu:~$ mysql -u root -p

mysql> create database snort;

mysql> use snort;

mysql> source ~/barnyard2-2-1.13/schemas/create\_mysql;

mysql> CREATE USER 'snort'@'localhost' IDENTIFIED BY '123456';

mysql> grant create, insert, select, delete, update on snort.\* to 'snort'@'localhost';

mysql> exit;

sudo vi /etc/snort/barnyard2.conf

#在末尾添加数据库配置

output database: log, mysql, user=snort password=123456 dbname=snort host=localhost sensor name=sensor01

修改barnyard2.conf权限防止被修改

sudo chmod o-r /etc/snort/barnyard2.conf

**进行测试**

# 开启snort，并向eth0发送ping数据包

sudo snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth0

# 开启barnyard2，将日志信息存入数据库

# 1.连续处理模式，设置barnyard2.waldo为书签

sudo barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -w /var/log/snort/barnyard2.waldo -g snort -u snort

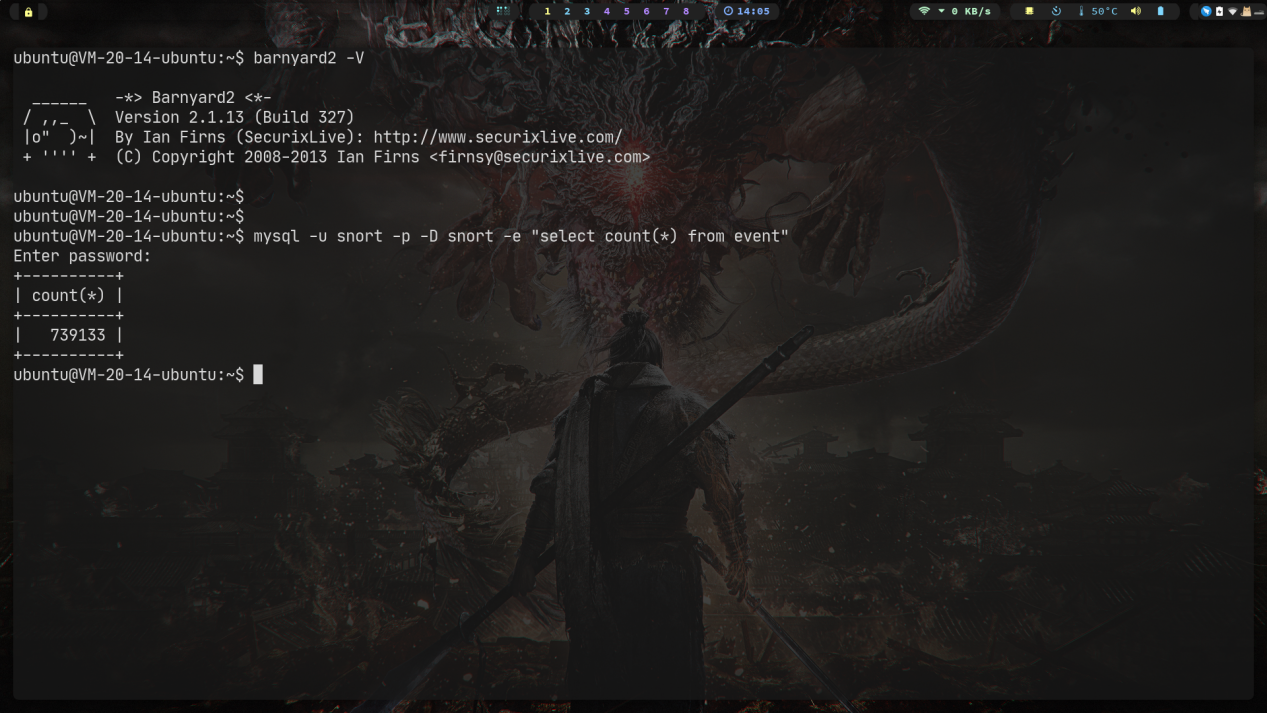
# 2.文件处理模式，处理单个日志文件

sudo barnyard2 -c /etc/snort/barnyard2.conf -o /var/log/snort/snort.log.xxx

# 查看数据库条目数量，看是否增加

mysql -u snort -p -D snort -e "select count(\*) from event"

**可以看到如下:**

****

**5 安装Base**

tar xzvf base-1.4.5.tar.gz

sudo mv base-1.4.5 /var/www/html/base/

cd /var/www/html/base

sudo cp base\_conf.php.dist base\_conf.php

sudo vi /var/www/html/base/base\_conf.php

$BASE\_Language = 'simplified\_chinese'; # line 27

$BASE\_urlpath = '/base'; # line 50

$DBlib\_path = '/usr/share/php/adodb/'; #line 80

$alert\_dbname = 'snort'; # line 102

$alert\_host = 'localhost';

$alert\_port = '';

$alert\_user = 'snort';

$alert\_password = '123456'; # line 106

// $graph\_font\_name = "Verdana";

// $graph\_font\_name = "DejaVuSans";

// $graph\_font\_name = "Image\_Graph\_Font";

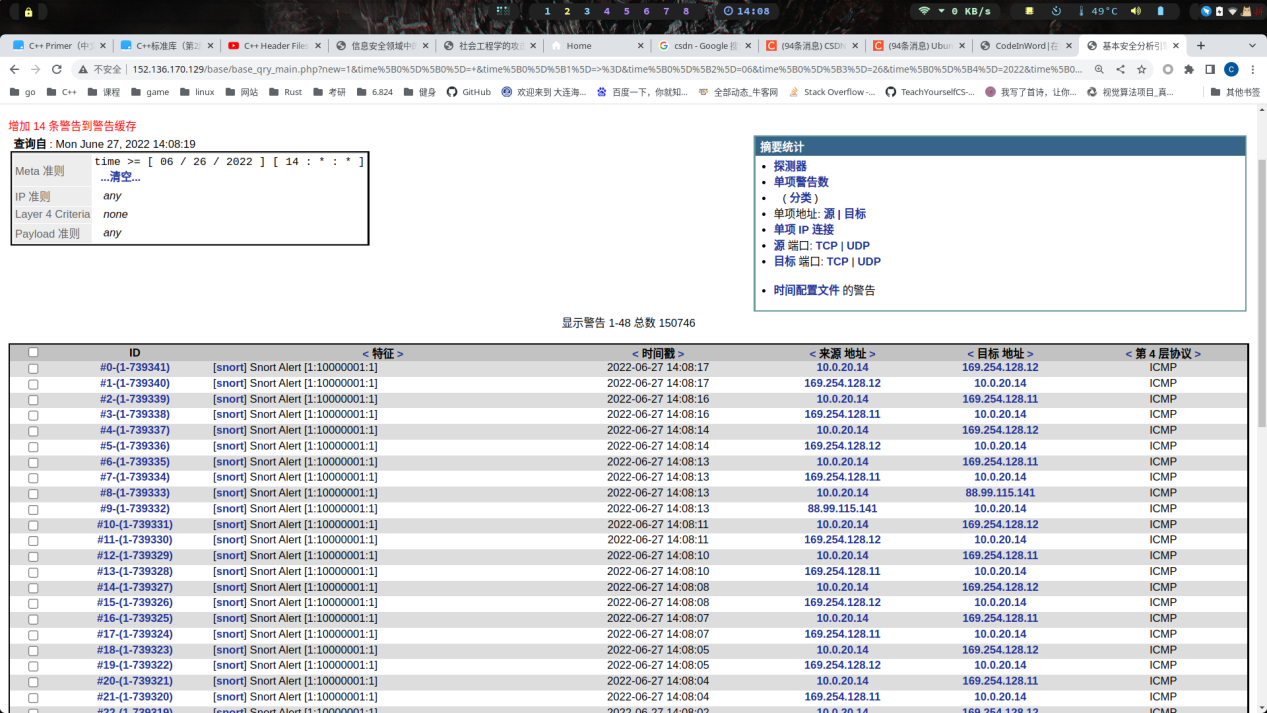
$graph\_font\_name = "";

sudo chown -R www-data:www-data /var/www/html/base

sudo chmod o-r /var/www/html/base/base\_conf.php

sudo service apache2 restart

通过浏览器访问http://x.x.x./base进行访问

****

**【结果分析】**

**构建完成的IDS系统可以通过snort 和 barnyard2 配合检测入侵，再通过base将结果展示出来。**

**【个人总结&心得体会】**

**通过此次实验，我学会了使用snort 及其他工具构建IDS环境。因为Snort的版本比较老，各种环境的搭建需要使用旧版本和查阅历史文档。通过网上查阅资料和提问，我成功搭建了环境，也学到了不少关于snort的知识。**