网络与信息安全课内实验

对DDos攻击的理解

### 本次实验目的

〉 1. 熟悉 Linux 系统,Wireshark 软件基本操作。

〉 2. SYN 洪泛攻击的实现与观察。

### 实验平台

Server：ubuntu虚拟机，安装Apache24

Attacker：ubuntu虚拟机，与server处于同一网段（局域网）

### 实验步骤

###### 1.安装虚拟机平台

很多时候，由于工作的需要，都需要在不同的系统环境中进行调试开发，要么自己有多台电脑，安装不同的系统，要么给电脑装多系统。但这些都不是很现实，前者要资金，后者想进行系统切换也够费劲的了，所以最好的解决办法还是安装虚拟机。

常用的虚拟机软件有VMware、VirtualBox、OpenVZ等等。在windows上推荐使用VMware或者VirtualBox。其中，VMware功能很丰富，比较快捷，方便；VirtualBox属于轻量级的虚拟机平台，而且是开源的，完整安装包很小。本人使用的是VirtualBox，大家可以自由选取。

需要注意的是，VirtualBox的复制粘贴等操作需要安装增强功能，推荐安装，教程如下：<https://jingyan.baidu.com/article/9f63fb914ab61ec8400f0edd.html>。

###### 2.安装虚拟机

本次实验的环境为Ubuntu，有同学如果已经安装了其他linux版本操作系统，可以直接使用，无需再次安装。

安装Ubuntu的第一步是需要下载Ubuntu系统。下载的官方网站为<http://releases.ubuntu.com/>。但是国内网速奇慢，所以一般使用镜像源。大家可以从<https://blog.csdn.net/gmzpx/article/details/80137714>中推荐的源下载。

Ubuntu一般可以选择14.04，16.04和18.04，个中区别可自行百度，本次实验都可使用，但推荐ubuntu16.04。

Ubuntu安装教程可参考<https://blog.csdn.net/scene_2015/article/details/83025750>。成功之后就可以看到与下图类似的界面，然后就可以开始我们愉快的实验了。

|  |  |
| --- | --- |
|  |  |

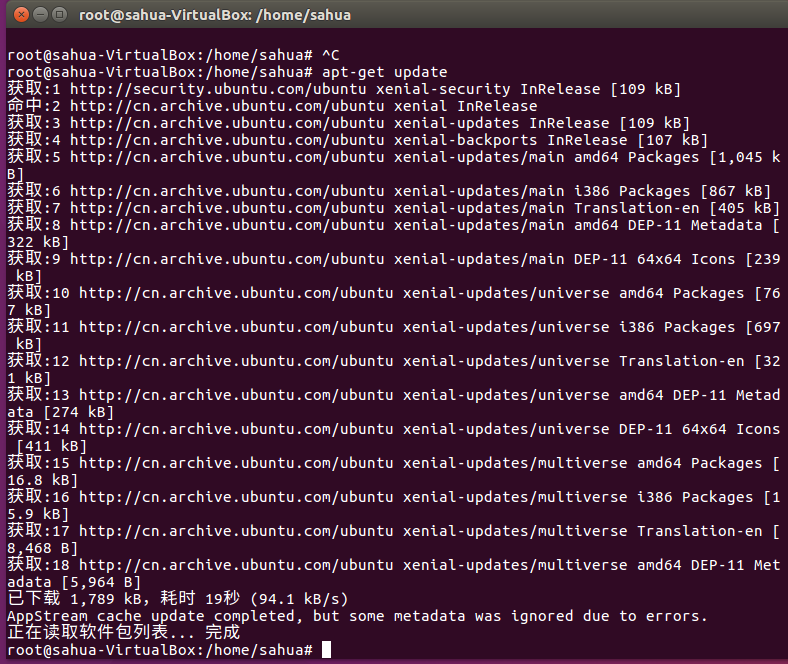
本次实验中，需要安装两个虚拟机，一个作为被攻击者，另一个作为攻击者，它们需要处于同一局域网。因此，需要将两个虚拟机都调整为交接模式或者NAT模式。通过ifconfig命令即可查看网络连接信息。

###### 3. 在server虚拟机上安装apache服务器

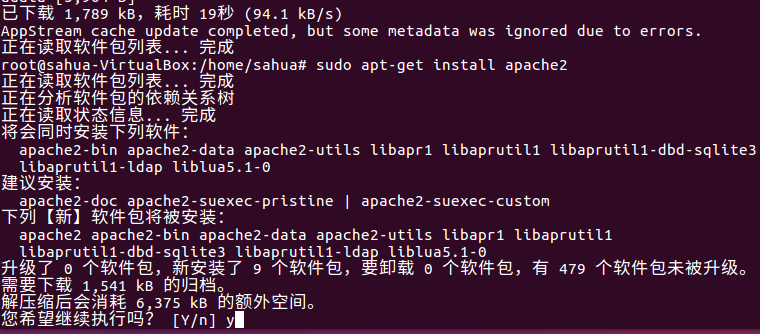
Apache是世界使用排名第一的Web服务器软件。我们按照apache的目的是搭建一个简单的网站，用来作为被攻击的目标。

首先，我们更新一下apt的软件库，方便之后下载

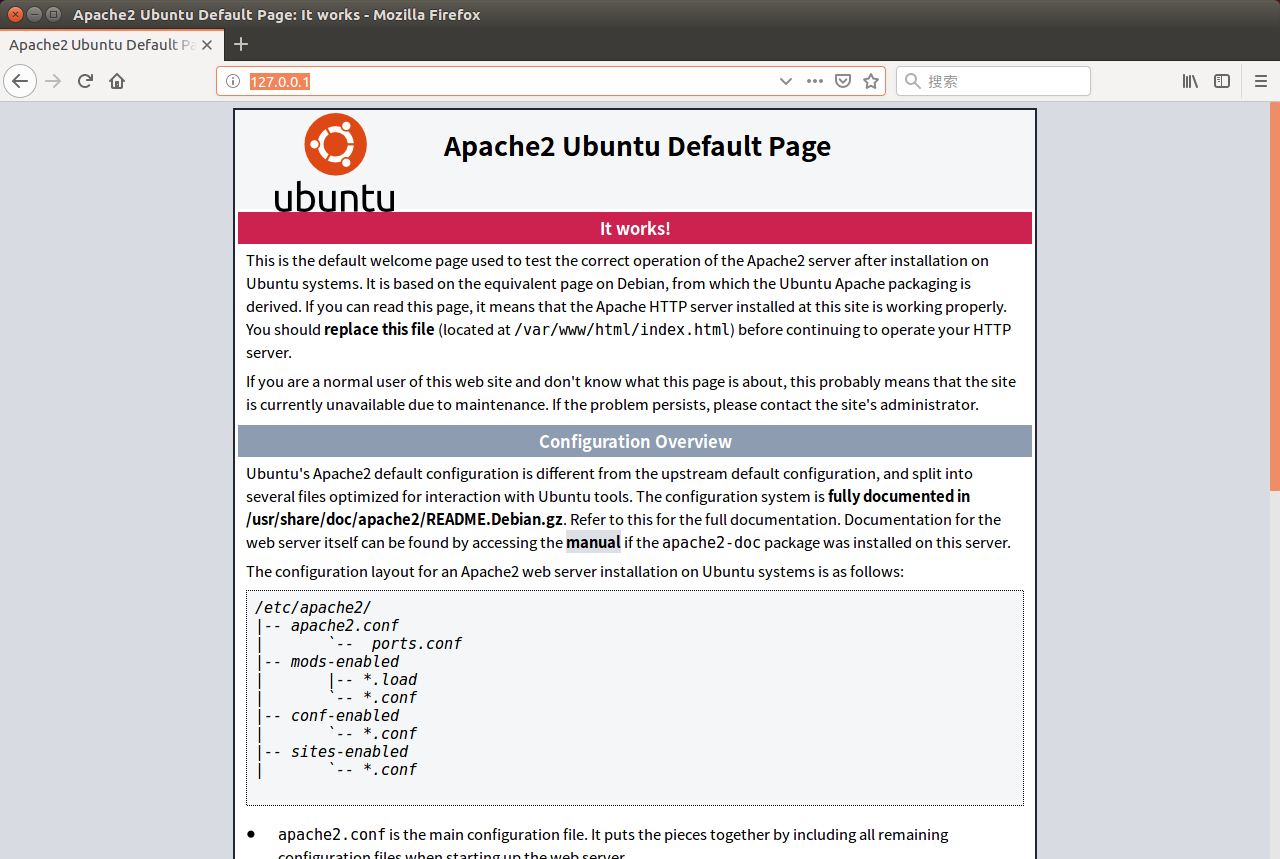
在终端输入命令：apt-get update



通过apt安装apache2：sudo apt-get install apache2

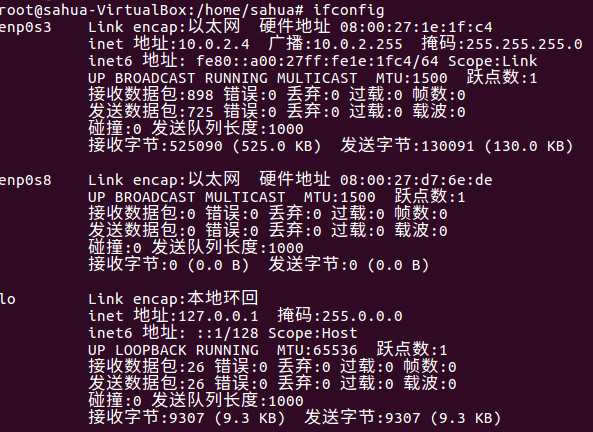


在浏览器中输入127.0.0.1访问，出现以下界面则安装成功：



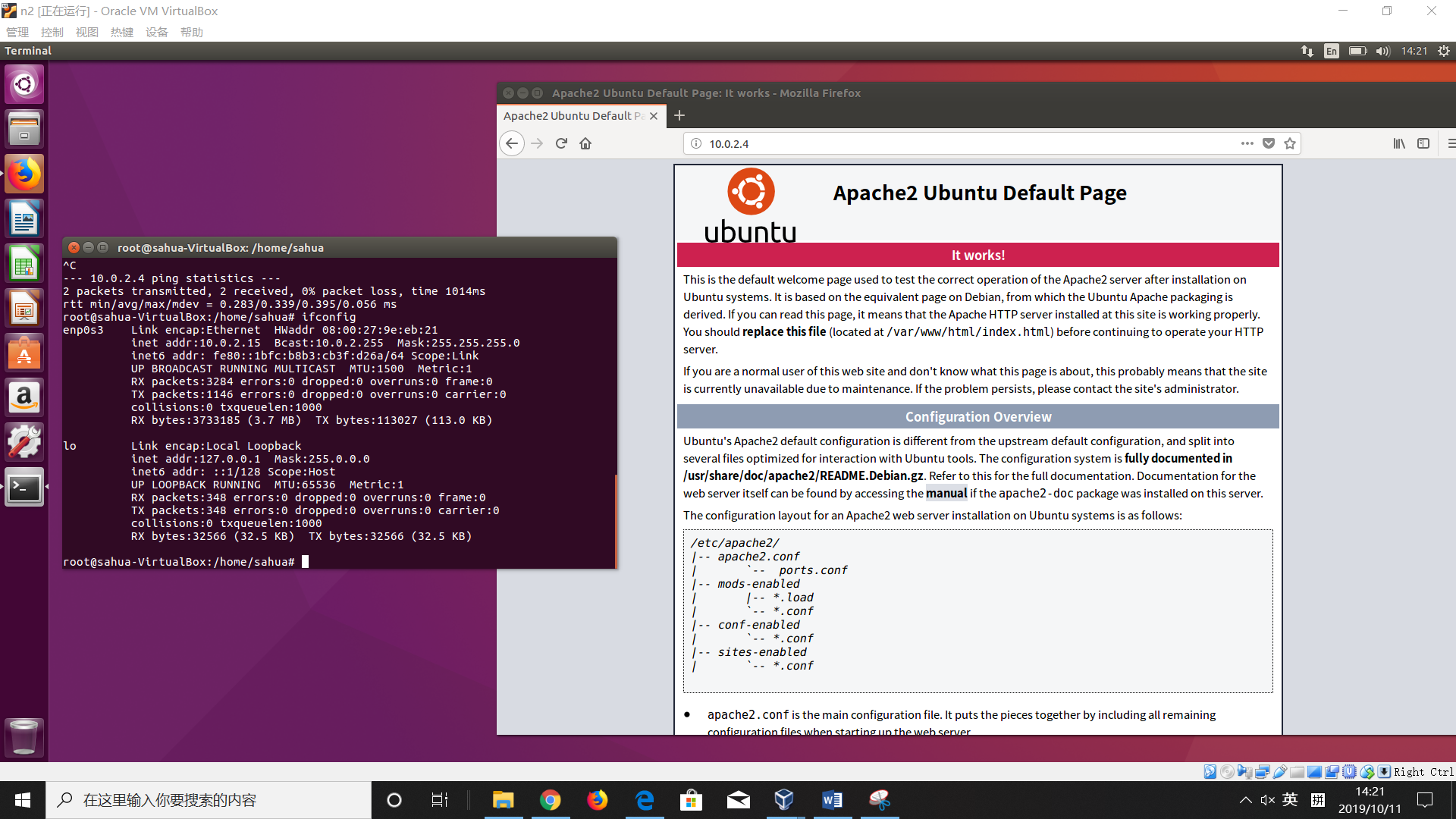
###### 4.SYN-Flood 攻击

通过ifconfig命令，我们获取apache2服务器的ip地址。



我的server ip地址为10.0.2.4

在攻击Ubuntu的浏览器上，输入10.0.2.4，如果也能访问，说明配置成功。



接下来，我们可以在攻击机上编写代码，进行攻击了。

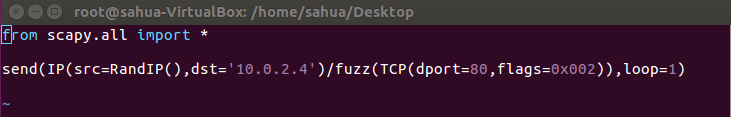
编写的代码使用python语言，使用的函数库为scapy，具体用法可以参照使用文档<https://scapy.readthedocs.io/en/latest/>。

编写前需要先下载函数库，分别运行：

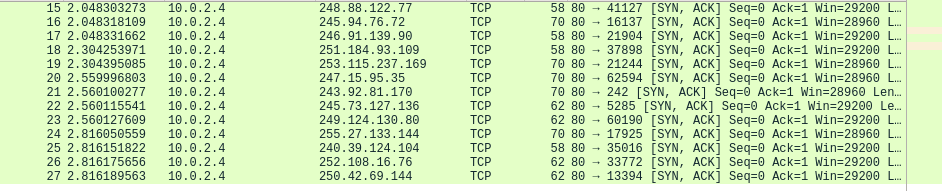
apt install python3-pip

pip3 install scapy

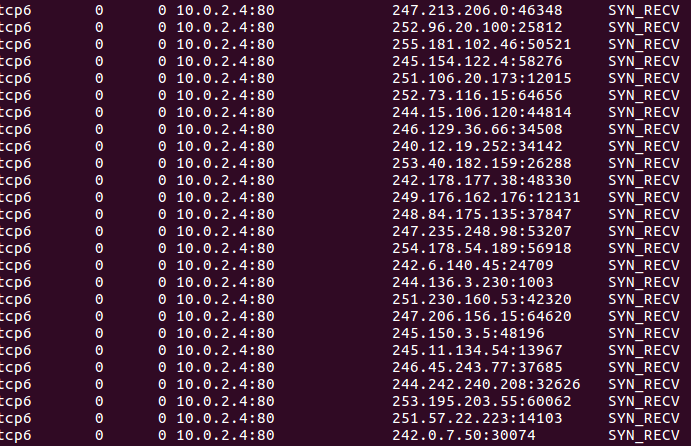
接下来书写程序：vim SYN\_flood.py



在server上用wireshark进行观察：



Server 运行 netstat –atn 可以看到，出现了很多的SYN请求。



### 实验报告要求

1.重复实验步骤，报告需包含实验目的、实验原理、实验步骤、实验小结等部分。

2.对SYN\_flood.py那一行命令的各个参数进行注释。

3.在wireshark上打开一个数据包，对其TCP协议上的每一个参数进行解释。

4.写遇到的问题和解决方法。