网络安全实验中 DDoS 攻击实验的实现

王希斌，廉龙颖，高 辉，郎春玲

（黑龙江科技大学 计算机与信息工程学院，哈尔滨 150022）

摘要 研究 DDoS 攻击技术，找出网络运行中隐藏的风险，是增强网络安全的一种重要手段。为了充分了解 DDoS 攻击原理和技术，提高学生的网络攻防实践能力，在基于 OpenStack 的网络安全实验平台中使用攻击软件 Trinoo 和 TFN2K，设计并实现了基于 UDP 方式的 DDoS 攻击模拟实验。

关 键 词 网络安全实验；DDos 攻击；实验平台

中图分类号 TP393 **文献标志码** A doi：10.3969/j.issn.1672－4550.2016.01.020

Implementation of DDoS Attack in Network Security Experiment

WANG Xibin，LIAN Longying，Gao Hui，Lang Chunling

（School of Computer and Information Engineering，Heilongjiang University of Science and Technology，Harbin 150022，China）

Abstract It is an important method to enhance network security through researching DDoS attack techniques to identify hidden risks in network service. In order to understand the principles and techniques of DDoS attack，and improve their practical ability of offense and defense，. DDoS attack simulation experiment based on UDP is designed and implemented using the famous attack software Trinoo and TFN2K based on the OpenStack network security experimental platform.

Key words network security experiment；DDos attack；experimental platform

网络安全的威胁主要来自计算机病毒、黑客入侵和拒绝服务攻击三个方面[1]，尤其是在拒绝服务攻击基础上发展起来的分布式拒绝服务（distributed denial of service，DDoS）攻击已成为网络安全的第一大威胁。DDoS 攻击不仅是一种攻击手段，也是网络安全公司用来模拟用户访问，测试网络设备、网络最大带宽和服务器最大负载能力的方法[2]。因此，有必要在高校的网络安全课程教学中建立一套完整的攻防实验环境，研究 DDoS 攻击原理和手段，为检测和防御 DDoS 攻击奠定基础。

黑龙江科技大学计算机学院的网络安全技术实验课程中开设了 DDoS 攻击实验，目的是让学生了解 DDoS 攻击的原理和技术。本文主要阐述了基于 OpenStack 的网络安全实验平台的 DDoS 攻击实验的实现。

1 实验目的和实验内容

DDoS 攻击实验目的：1）了解 DDoS 攻击过程；2）掌握 DDoS 攻击工具使用方法，实现 DDoS 攻击；3）通过分析实验数据，理解 DDoS 攻击原理。

DDoS 攻击实验内容：1）在实验平台中搭建 DDoS 攻击实验虚拟网络；2）使用 Trinoo 和 TFN2K 软件对攻击目标发动 UDP Flood 方式的 DDoS 攻击；3）使用网络数据分析软件 NetworkActive PIAFCTM 捕捉数据包，分析实验数据。

2 实验原理

2.1 DDoS 攻击概念

DDoS 攻击是指采用分布式的大规模的拒绝服务攻击。攻击者通过组建 DDoS 攻击网络，并向攻击网络中的攻击服务器和攻击器发出攻击指令，用超出被攻击目标处理能力的海量数据包来消耗目标系统的资源，最终导致网络服务瘫痪[3－5]。

2.2 DDoS 攻击体系

一个比较完善的 DDoS 攻击体系包括攻击者、攻击服务器、攻击器和攻击目标 4 个部分，如图 1 所示，是一种 n∶m 的映射关系。攻击者指黑客所使用的主机，它操纵整个攻击过程，向攻击服务器发送攻击命令；攻击服务器和攻击器都是攻击者侵入并控制的主机，其中安装特定的 DDoS 攻击程

收稿日期：2014－10－30

基金项目：黑龙江省教育科学“十二五”规划 2013 年度青年基金专项课题（GBD1213039）。

作者简介：王希斌（1981－），男，硕士，讲师，主要从事程序设计、网络安全方面的研究。

序[6]，攻击服务器发送攻击指令到攻击器上，而攻击器则接收和运行攻击服务器发来的命令[7]，攻击目标指被攻击的服务器或主机。

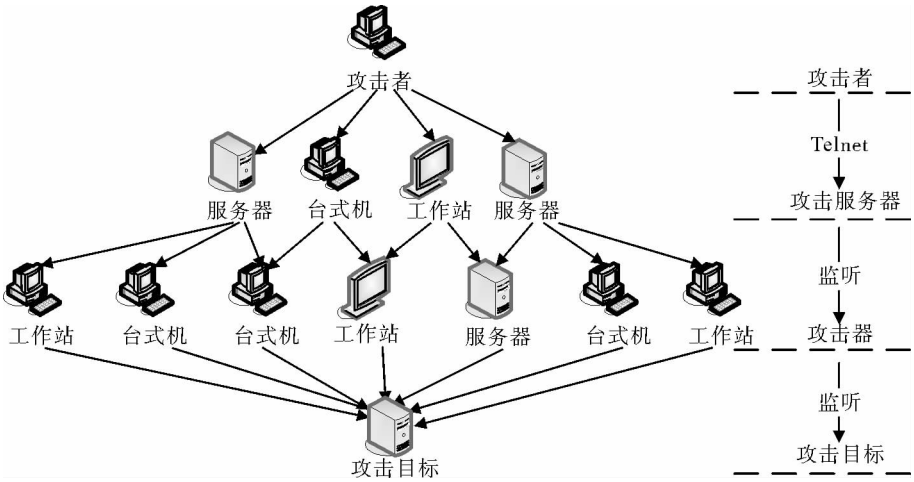

图 1　DDoS 攻击体系

2.3　基于 UDP 的 DDoS 攻击方式

按照 TCP/IP 协议的层次可将 DDoS 攻击分为基于 ARP 的攻击、基于 ICMP 的攻击、基于 IP 的攻击、基于 UDP 的攻击、基于 TCP 的攻击和基于应用层的攻击[8]。本实验选择基于 UDP 的 DDoS 方式进行攻击实验。

基于 UDP 的 DDoS 攻击中，攻击者通过发送大量伪造源 IP 地址的 UDP 数据包进行拒绝服务攻击。目前，互联网上提供 www 和 mail 等服务的设备一般默认开放一些 UDP 服务。由于 UDP 协议是一种面向无连接的服务，因此针对每一个开放的 UDP 服务端口，都可以进行相关的攻击，最终使网络可用带宽被耗尽，无法向用户提供正常的网络服务[9]。

3　实验环境

3.1　基于 OpenStack 的网络安全实验平台

黑龙江科技大学搭建了基于 OpenStack 的网络安全实验平台，如图 2 所示。该平台采用抽象分层模式，实验平台抽象为 3 层结构，分别是面向底层虚拟化的硬件资源管理层、面向 OpenStack 的网络虚拟化层以及面向用户的实验应用层。在 OpenStack 中使用 SDN 网络虚拟化技术，通过 Neutron 组件创建虚拟网络和路由器、负载均衡等各种网络节点，最终搭建出满足网络安全实验需求、真实、隔离、可扩展、可编程的实验环境。

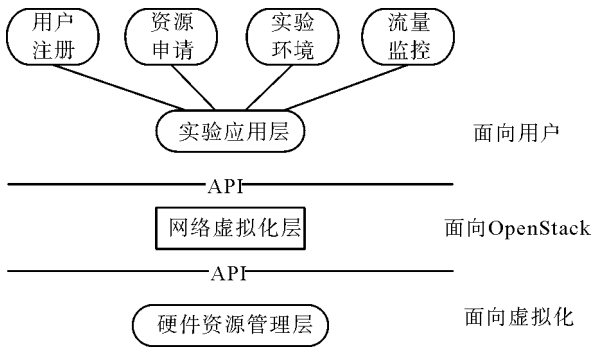

图 2　实验平台 3 层结构

3.2　实验拓扑

在基于 OpenStack 的网络安全实验平台中，根据 DDoS 攻击体系设计和创建虚拟网络，拓扑结构如图 3 所示，其中 PC0 作为攻击者，PC1 作为攻击服务器，PC2、PC3、PC4 和 server1 作为攻击器，server4(Web Server)作为攻击目标。

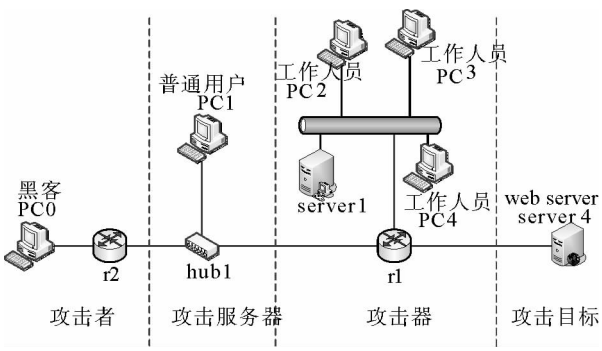

图 3　实验环境拓扑结构图

3.3　实验设备及工具

根据图 3 的实验环境拓扑图，在 OpenStack 平台中进行网络配置，主机和服务器的系统及服务软件安装配置，具体配置信息见表 1。

表 1 主机与服务器配置信息

机器名	IP 地址	操作系统	实验软件
PC0	192. 168. 1. 1	Windows2000	
PC1	192. 168. 2. 1	Windows2000	TFN2K、Trinoo
PC2	192. 168. 2. 2	ReadHat Linux 9	
PC3	192. 168. 2. 3	Solaris 11	
PC4	192. 168. 2. 4	Windows 7	
server1	192. 168. 2. 5	Windows Server 2003	
server4	192. 168. 3. 1	Red Hat 5. 0	Apache – 1. 3. 17

4 DDoS 攻击实现

在实验虚拟网络中，攻击者 PC0 通过 Telnet 控制攻击服务器 PC1，PC1 中运行 Trinoo 和 TFN2K 攻击工具，控制攻击器 PC2、PC3、PC4 和 server1，对攻击目标 server4 发起 UDP Flood 攻击，同时使用网络数据分析软件 NetworkActive PIAFCTM 捕捉数据包，分析 DDoS 攻击实验数据。

4. 1 DDoS 工具分析

现在常用的 DDoS 攻击工具有 Trinoo、TFN、TFN2K、Mstream 和 Stacheldraht 等[10-13]，本文分别采用 Trinoo 和 TFN2K 作为攻击工具实现 DDoS 攻击。Trinoo 和 TFN2K 都由攻击服务器程序和攻击器程序两部分组成。在实验网络中，PC1 作为攻击服务器，PC2、PC3、PC4 和 server1 作为攻击器。

Trinoo 是最早发布的 DDoS 工具，由攻击服务器程序 master 和攻击器程序 ns 组成。它的工作方式是攻击者通过 27665/TCP 端口建立 TCP 连接来实现远程控制程序与攻击服务器通信，攻击服务器向攻击器的 27444/UDP 端口传递攻击指令[14]。

TFN2K 是 TFN 的 2000 版本，由攻击服务器程序 tfn 和攻击器程序 td 组成。TFN2K 的攻击服务器程序向攻击器程序发送攻击目标的列表，攻击器程序根据攻击列表对攻击目标进行拒绝服务攻击[15]。一个攻击服务器上的客户进程可以控制多个攻击器，这些攻击器在攻击过程中相互协同，从而保证攻击的连续性。

4. 2 实现

1)使用 Trinoo 工具实现 DDoS 攻击。

Trinoo 中的 master 程序植入攻击服务器 PC1 中，ns 程序分别植入攻击器 PC2、PC3、PC4 和 server1 中。

在 ns. c 中写入攻击服务器 PC1 的 IP，并进行编译和安装：

char * master [ ] = { “192. 168. 2. 1”, NULL};

在 PC1 中启动 master，默认密码为 gOrave：

masterhost# ./master

成功启动后将显示连接成功提示：

trinoo v1. 07d2 + f4 + c [Mar 202014：14：19：42]

在 PC2、PC3、PC4 和 server1 中分别执行 ns，启动攻击器程序。

检测各攻击器程序是否成功启动：

trinoo > mping

mping：Sending a PING to every Bcasts

trinoo > PONG 1 Received from 192. 168. 2. 2

PONG 1 Received from 192. 168. 2. 3

PONG 1 Received from 192. 168. 2. 4

PONG 1 Received from 192. 168. 2. 5

收到成功响应提示后，设定攻击时间为 60 s：

trinoo > mtimer 60

mtimer：Setting timer on bcast to 60

发起 DDoS 攻击，攻击目标 server4 (IP：192. 168. 3. 1)：

trinoo > dos 192. 168. 3. 1

Dos：Packeting 192. 168. 3. 1…

2)使用 TFN2K 工具实现 DDoS 攻击。

将 TFN2K 工具包拷贝到 PC1 中，输入 make 命令进行编译安装，编译时输入自定义的密码 ddos。编译安装后，产生两个可执行文件：tfn 和 td。

在 PC2、PC3、PC4 和 server1 中分别运行 td 命令来启动 TFN2K 攻击器程序。

在 PC1 的 hosts. txt 文件中添加 PC2、PC3、PC4 和 server1 的 IP 并保存，IP 地址分别为 192. 168. 2. 2、192. 168. 2. 3、192. 168. 2. 4 和 192. 168. 2. 5。

在 PC1 中执行如下命令，控制 hosts 文件中的多台攻击器向攻击目标 server4(IP：192. 168. 3. 1)发起 UDP Flood 攻击：

tfn - f hosts. txt - c4 - i 192. 168. 3. 1

protocol：random

sourceIP：random

clientinput：singlehost

command：commenceudpflood

passwordverification：ddos

4.3　实验数据分析

1)数据流量分析。

经过测试，使用 Trinoo 工具进行 DDoS 攻击时，1 台攻击器发送数据包个数为 13 000 packets/s 左右；而使用 TFN2K 工具时，1 台攻击器发送数据包为 2 800 packets/s 左右。由此可见，在实验中，1 台 Trinoo 攻击器产生的 UDP 包占有的带宽大约是 1 台 TFN2K 攻击器产生的 UDP 包占有带宽的 5 倍。

2)DDoS 工具特性分析。

使用 Trinoo 工具产生的攻击数据包：

UDP　47　192.168.2.2　192.168.3.1　769　1 404

使用 TFN2K 工具产生的攻击数据包：

UDP　2129.108.94.10　192.168.3.1　65 534　48

查看两个工具产生的数据包，Trinoo 的 UDP 包的源地址 192.168.2.2 是攻击器 PC2 的 IP 地址，而 TFN2K 的源地址是伪造的。通过分析可知，使用 TFN2K 作为 DDoS 攻击工具隐蔽性更好，更不易被检测到。

根据 DDoS 攻击实验的结果，可在后期实验中提出实际网络系统结构的改进方案，并在实验平台中验证其可行性和性能。

5　结束语

为解决网络安全实验受到实验条件限制的问题，黑龙江科技大学开发了基于 OpenStack 的网络安全实验平台。在实验平台中创建满足实验需求的虚拟网络，并分别采用 Trinoo 和 TFN2K 工具实现了 DDoS 攻击实验。通过真实的攻击实践操作，使学生掌握了 DDoS 攻击原理，提高了攻防实践能力，教学效果良好。在此实验的基础上，可以进一步研究 DDoS 攻击检测方法，培养学生分析、解决网络安全问题的能力。

参 考 文 献

[1] 李长隆 . DDoS 攻击的原理及防范 DDoS 攻击的策略[J]. 电脑与电信，2007(8)：39 – 40.

[2] 陈波 . 分布式拒绝服务攻击研究[J]. 计算机工程，2002，28(6)：63 – 65，113.

[3] 王颖熙 . 基于 UDP 的 DDoS 攻击实验[J]. 中山大学研究生学刊(自然科学、医学版)，2004，25(4)：100 – 112.

[4] GASTI P，TSUDIK G，UZUN E，et al. DoS and DDoS in named data networking[J]. International Conference on Computer Communications and Networks，2013，44(3)：1 – 7.

[5] 张卫东，李晖，尹钰 . 网络安全实验教学方法的研究[J]. 实验室研究与探索，2007，26(12)：298 – 301.

[6] 黄妍妍 . 网络服务管理中的 DDoS 攻击预防策略[J]. 河北科技图苑，2003，16(5)：31 – 33.

[7] ZARGAR S T，JOSHI J，TIPPER D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks[J]. Communications Surveys & Tutorials，2013，15(4)：2046 – 2069.

[8] PENG T，LECKIE C，Ramamohanarao K. Survey of network – based defense mechanisms countering the DoS and DDoS problems[J]. ACM Computing Surveys，2007，39(1)：3.

[9] 顾群业，李广福 . 拒绝服务攻击方式分析及防御策略部署[J]. 网络安全技术与应用，2005(7)：43 – 45.

[10] 林梅琴，李志蜀，袁小铃，等 . 分布式拒绝服务攻击及防范研究[J]. 计算机应用研究，2006，23(8)：136 – 138，151.

[11] JEON D. Understanding DDoS attack，tools and free anti – tools with recommendation[EB/OL]. [2014 – 08 – 25]. http：//www.sans.org/infoseFAQ/threats/Understamding ddos.htm.

[12] ISOZAKI H，ATA S，OKA I，et al. Performance improvement on probabilistic packet marking by using history caching[C]//APSITT′OS Information and Telecommunication Technologies，2005.6th Asia – Pacific Symposium，Piscafauany，N.J：IEEE Press，2005：381 – 386.

[13] DOULIGERIS C，MITROKOTSA A. DDoS attacks and defense mechanisms：classification and state of the art[J]. Computer Networks，2004，44(5)：643 – 666.

[14] XIANG Y，ZHOU W L. Mark – aided distributed filtering by using neural network for ddos defense[C]//GLOBECOM05：Global Telecommunications Conference.[S.l.] IEEE Press，2005(3)：1701 – 1705.

[15] STORM P. Tribe flood network (TFN2K) DDoS tool(2000)[EB/OL]. [2014 – 09 – 10]. http：//packetstormsecurity.org/distributed/TFN2k_ Analysis – 1.3. txt.