第 17 卷第 4 期和增刊　　广西科学院学报　　Vol. 17, No. 4 & Supplement
2001 年 11 月　　Journal of Guangxi Academy of Sciences　　November 2001

分布式拒绝服务型攻击原理及防范措施
Attacking Pattern and Protection Measures of Distributed Denial of Service

黄振俭
Huang Zhenjian

（广西民族学院　南宁　530006）
(Guangxi University for Nationalities, Nanning, 530006)

摘要　分布式拒绝服务型攻击（Distributed Denial of Service 简称 DDoS）是目前黑客常用的网络攻击手段，本文阐述了 DDoS 的原理与过程，并试图寻找其攻击的规律，由此提出相应的防范措施。

关键词　拒绝服务　分布式拒绝服务　攻击控制台　攻击管理机　攻击执行机
中图法分类号　TP393.08

Abstract　Distributed Denial of Service (DDoS) is one of the most common means of attacking network used by hackers nowaday. The theory and process of DDoS are analyzed to find out rules of attacking. Some suggests for protection are given.

Key words　denial of service, distributed denial of service, client, handler, agent

分布式拒绝服务型攻击 Distributed Denial of Service（简称 DDoS），是建立在拒绝服务 DoS (Denial of Service) 理论基础上的一种新型的网络攻击手段，DoS 理论由来已久，其主要特征是通过虚假 IP 在很短的时间内向目标主机发送大量的数据包，造成目标主机信息堵塞，从而不能对别的正常请求提供服务。可以举个简单例子：有人不断地向一家实行电话订餐的快餐店拨打电话，使得其他客户无法拨通快餐店的电话，在其他客户看来，这家快餐店就是“拒绝服务”。

最初 DoS 并不是一种网络攻击手段，而是以网络测试工具的身份出现，因为它可以产生大量的分布数据包，可用于模拟多用户并发访问网站，由此测试网络的最大带宽、网络设备的运行能力、服务器的最大负载能力等。

DDoS 在 1999 年时还停留在理论的探讨上，2000 年 1 月下旬，来自全美国的网络安全专家们在加利福尼亚举行的第 6 次 RSA 安全会议上讨论了这种攻击并试图制定对付措施，2000 年 2 月，黑客们使用 DDoS 连续攻击了 Yahoo，ebay，Amazon 等许多知名网站，致使一些站点中断服务长达数小时甚至几天，国内的新浪等站点也遭到类似的攻击。这次攻击浪潮使 DDoS 名声大振，从此为社会所关注。在 2001 年 5 月的中美黑客大战中，DDoS 也被广泛使用，至此，DDoS 已成为影响网络安全的一个不容忽视的问题。

2001-06-29 收稿。

电子商务的飞速发展，也使得 DDoS 的危害变得格外现实，一个很实际的例子是，一个拍卖网站以极低价格起拍一件昂贵的物品，攻击者在低价位应价后，即实施 DDoS 攻击，使网站无法再回应其他正常请求，从而低价获取拍卖物品。

本文拟从 DDoS 的原理与过程中寻找其攻击规律，由此提出相应的防范措施。

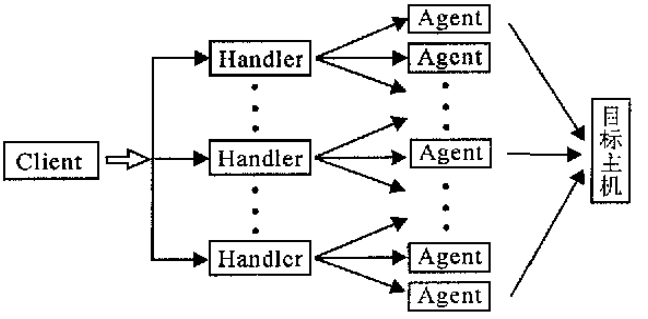

图 1　DDoS 结构示意图

1　原理

DDoS 采用的是一种多层客户机/服务器体系结构，如图 1 所示：

攻击管理机（Handler）是一些已被入侵的主机，攻击者利用各种安全漏洞获得登录的权限，并把攻击管理程序植入主机中运行，在接收到控制台的命令后，攻击管理程序就会向其所管辖的多台攻击执行机 Agent 下达攻击指令。Handler 扮演的角色类似于军队里的军官。

攻击执行机（Agent）是攻击的直接执行者，就象在战场上冲锋陷阵的士兵。Agent 也是一些被入侵的主机，攻击者在里面植入攻击程序，攻击程序一般会内置一个或多个 Handler 的地址，直接受控于 Handler，在接收到 Handler 的指令后，Agent 就会连续向目标主机发送大量的拒绝服务数据包，从而耗尽目标主机网络的带宽与资源。

攻击控制台（Client）是攻击者向 Handler 下达攻击指令的机器，Client 可以是网络上任何一台主机，甚至可以是一台移动的便携机，攻击控制台就如同运筹帷幄之中，决策千里之外的将军。

DDoS 的这种多层客户机/服务器的体系结构使得攻击者更为隐蔽，攻击效果更为突然和有效，在这其中，攻击管理机 Handler 起到了很重要的作用。它有如下的特点：(1) 隔绝网络联系，增大回溯查找攻击者的难度，有效地保护了攻击者；(2) 使控制台 client 的操作更为简单、快捷，攻击者可以使用网络上的任何一台机器，位置非常灵活，而且发布命令的时间很短，所以非常隐蔽，难以定位，在命令下达到为数不多的 Handler 后，控制台就可以断开网络连接，从而逃避追踪。这些 Handler 随后自行将攻击指令下达各个攻击执行机，不再需要控制台的干预；(3) 简化了攻击执行机 Agent 的攻击程序，Agent 只需执行一些简单的程序，不断地向目标主机发送大量的连接请求而不作任何回答即可。这就使得攻击更为密集紧凑；(4) 增大攻击的突然性与协同性，如果由 Client 直接向 Agent 下达攻击指令，由于 Agent 数目过多，很容易造成 Client 的网络阻塞，使指令到达 Agent 的时间有所延迟，从而影响攻击的突然性与协同性；使用 Handler 则可避免此种情形，因为各个 Handler 一般处于不同的网络，可以有效地分流控制指令流。另外，直接下达攻击指令还有一个弊端，就是 Client 的网络流量会突然增大，这种流量剧增现象很容易被监控系统察觉，从而搜寻到攻击者的位置与意图。

2　过程

由上述 DDoS 原理可以大致了解到其攻击的大概步骤：(1) 通过扫描大量主机以寻找可入侵的主机目标；(2) 通过常规方法入侵主机，安装特殊的后门程序；(3) 利用已入侵主机，通过网络监听等手段进一步扩充入侵主机群；(4) 在入侵的主机中安装攻击管理程序和攻击程

序；（5）等时机成熟，攻击者由 Client 端发出攻击指令，指令到达 Handler 后即断开连接；（6）Handler 向 Agent 发布攻击命令，Agent 收到攻击命令，即向目标主机发送拒绝服务数据包。

由此可知，有许多无关主机可以支配是整个攻击的前提条件，这些主机数目越多，与目标主机之间的联系越紧密，网络带宽越宽，攻击效果就越好。

3 防范措施

3.1 确保外围主机和服务器的安全

针对 DDoS 攻击的第 1，2，3 步骤，我们首先要确保外围主机和服务器的安全，一旦单位内部的主机或临近网络的主机被入侵，那么其他的主机被入侵的可能性会变得很大。而且，如果网络内部的主机被用来对本机进行 DDoS 攻击，效果会更明显。所以必须要保证外围主机和服务器的安全，尤其是那些拥有高性能主机和高带宽的网络。只要黑客无法获得大量无关主机，就无法发动有效攻击。

为了确保主机和网络的安全，我们可以采取以下方法：

（1）及时了解有关主机操作系统的安全漏洞和相应的补救措施。现在互联网上有许多旧的和新的漏洞攻击程序。系统管理员应经常登录有关漏洞数据库的安全网站，如 securityfocus.com 或 packetstorm.securify.com，以确保服务器不受这些漏洞影响。记住，入侵者总是利用已存在的漏洞进入系统并安装攻击程序的。

（2）充分了解系统和服务器软件是如何工作的，经常检查系统配置和安全策略。及时安装补丁程序和升级系统软件。另外还要时刻留意安全站点公布的与操作系统及软件有关的最新安全漏洞和问题。以免给黑客可乘之机。

（3）对所有可能成为目标的主机都进行优化。禁止所有不必要的服务。另外多 IP 主机也会增加攻击者的难度。建议在多台主机中使用多 IP 地址技术，而这些主机的首页只会自动转向真正的 web 服务器。

（4）检查文件完整性：当确定系统未曾被入侵时，应该尽快备份所有二进制程序和其它重要的系统文件，并且周期性地与这些文件比较以确保不被非法修改。另外，强烈推荐将这些文件保存到另一台主机或可移动介质中。

（5）管理员应当订阅安全信息报告，实时地关注所有安全问题的发展。

3.2 使用反黑客软件

针对 DDoS 攻击的第 4 个步骤，我们可以根据实际情况使用有针对性的反黑客软件，目前已经有一些工具软件可以检测特定系统是否安装了 DDoS 的攻击管理程序和攻击程序，例如 FBI 的 find—ddos 工具（可在 http：//www.fbi.gov 上找到），这些程序可以扫描系统，找出已安装的攻击程序，防止机器被黑客利用。

3.3 其他防范措施

针对 DDoS 攻击的第 5，6 个步骤，我们可以采取以下措施：

（1）使用包过滤的技术。主要是过滤对外开放的端口，防止假冒地址的攻击，使得外部机器无法假冒内部机器的地址来对内部机器发动攻击。

可以使用 Cisco IOS 来检查路由器的详细设置，当然，它也不仅限于 Cisco 的设备，登陆到将要配置的路由器上，在配置访问控制列表（ACL）之前先初始化一遍。如

c3600 (config) #access-list 100 permit ip 207. 22. 212. 0 0. 0. 0. 255 any

c3600 (config) #access-list 100 deny ip any any

然后我们假设在路由器的 S0 口上进行 ACL 的设置，我们进入 S0 口，并进入配置状态：

c3600 (config) #int ser 0

c3600 (config—if) #ip access-group 100 out

通过显示 access-list 来确认下面的访问权限已经生效。

c3600#sho access-lists 100

Extended IP access list 100

permit ip 207. 22. 212. 0 0. 0. 0. 255 any (5 matches)

deny ip any any (25202 matches)

对于应该使用向内的包过滤还是使用向外的包过滤一直存在着争论。RFC（要求评论文档）2267 建议在全球范围的互联网上使用向内过滤的机制，但是这样会带来很多的麻烦，在中等级别的路由器上使用访问控制列表不会带来太大的麻烦，但是已经满载的骨干路由器上会受到明显的威胁。

(2) 识别非法数据包。一般来说，用于攻击的数据包都会有些特征，比如超长或畸形的 ICMP 或 UDP 包等，如果数据包本身比较正常，但其中的数据比较特异，如存在伪装和加密，那么就有可能是 Handler 向 Agent 发布的攻击命令。对于这些非法和伪装的数据包，可以使用防火墙对其进行严格过滤。

(3) 优化路由和网络结构。如果你管理的不仅仅是一台主机，而是网络，就需要调整路由表以使拒绝服务攻击的影响减到最小。应设置 TCP 侦听功能，禁止网络不需要使用的 UDP 和 ICMP 包通过，尤其是不应该允许出现 ICMP "不可到达" 消息。详细设置请参阅相关路由器技术文档。

(4) 通过监视端口使用情况的方法来监测入侵。常见的 DDoS 工具一般都有自己特定的通讯方式，以下是几种常见分布式拒绝服务攻击工具的特征：

(a) Trinoo：Client、Handler 和 Agent 主机相互间通讯时使用如下端口：

1524 tcp

27665 tcp

27444 udp

31335 udp

注：以上所列出的只是该工具的缺省端口，仅作参考。

(b) TFN：Client、Handler 和 Agent 主机相互间通讯时使用 ICMP ECHO 和 ICMP ECHO REPLY 数据包。

(c) Stacheldraht ：Client、Handler 和 Agent 主机相互间通讯时使用如下端口和数据包：

16660 tcp

65000 tcp

ICMP ECHO

ICMP ECHO REPLY

注：以上所列出的只是该工具的缺省端口，仅作参考。

(d) TFN2K：Client、Handler 和 Agent 主机相互间通讯时并没有使用任何指定端口（在

运行时指定或由程序随机选择），但结合了 UDP、ICMP 和 TCP 数据包进行通讯。

如果本地机的上述端口处于监听状态，那么系统很可能已经受到了侵袭，即使黑客已经对端口的位置进行了修改，但如果外部主机主动向网络内部的高标号端口发起连接请求，那么系统也有可能遭到入侵。通过对防火墙进行合理设置可以对这个过程进行监测和过滤。

(5) 要求与 ISP 协助和合作。DDoS 攻击很容易耗尽带宽，单凭网络管理员是无法对付这些攻击的。与你的 ISP 协商，确保他们同意帮助你实施正确的路由访问控制策略以保护带宽和内部网络。比如当发生攻击时，你的 ISP 可以对主干路由器进行限流措施来降低攻击所造成的影响。

(6) 追根溯源寻找到正在进行攻击的机器和攻击者，将攻击者绳之以法。可以采用多种方法来寻找攻击者所处的位置：(a) 最常用的方法是在数据流中搜寻特征字符串，在 Handler 向 Agent 发布的攻击命令中，一般会有特定的命令字符串，搜寻到这些字符串，就可以确定 Handler 和 Client 的位置；(b) 用统计的方法寻找攻击来源。在攻击之前，目标网络的域名服务器 (DNS) 通常会收到远远超出正常数量的正向和反向的地址查询，这些查询往往意味着攻击的来临；(c) 通过数据流量来判断。在攻击时，攻击数据的来源地址会发出超过正常极限的数据包，这样，对通讯数据量进行统计也可以得到有关攻击系统的位置和数量的信息。

追踪攻击者不是一件很容易的事情，一旦其停止了攻击行为，很难将其发现。唯一可行的方法就是在其进行攻击的时候，根据路由器的信息和攻击数据包的特征，采用一级一级回溯的方法来查找其攻击源头。这就需要各级部门的协同配合才能很好地完成。

4 结语

由于 TCP/IP 协议的设计原则是在实现上力求简单高效，为了避免增大代码量和降低运行效率，TCP/IP 协议族中的许多协议的安全措施很不完善，比如在 TCP/IP 堆栈中存在许多漏洞，如允许碎片包、大数据包、IP 路由选择、半公开 TCP 连接、数据包 flood 等等，这些都会降低系统性能，甚至使系统崩溃。拒绝服务攻击就充分利用了这些漏洞，达到攻击的目的，因此 TCP/IP 协议的进一步完善将有助于避免类似攻击。

DDoS 是一种较为先进的攻击方式，但任何攻击方式都有其规律性和弱点，我们只要掌握其攻击的规律，抓住其弱点，就能对其加以监测和控制。

参考文献

1 Douglas E. Comer, David L Stevens. Internet working with TCP/IP. Second Edition. Prentice-Hall Inc, 1994.

2 Brent Chapman D, Elizabeth D Zwicky. 构筑因特网防火墙. 北京：电子工业出版社，1998. 1.

3 Andrew S Tanenbaum. 计算机网络. 第 3 版. 北京：清华大学出版社，1998. 7.

4 Mcclure, Scambray, Kurtz. Network Security Secrets and Solutions. McGraw-Hill Companies, 1999.

（责任编辑：黎贞崇）