资源耗尽型 DoS 攻击分析及相关的实用防范技术

Analysis of the Resource – use – out DoS Attack and the Practical Defense Technology

孙海燕　（中国科学院研究生院　北京 100039）
鲁士文　（中国科学院计算技术研究所　北京 100080）

摘要：本文介绍了几种针对计算资源环境的拒绝服务攻击的方式及基本原理，重点分析了从服务器、网络设备和安全设备等方面防御 SYN Flooding 攻击的措施和应采取的整体防御策略，并结合实际工作经验给出处理 SYN 攻击的方法。

关键词：拒绝服务 SYN　攻击　策略　防范措施

1　前言

从上个世纪九十年代到近几年，拒绝服务攻击[1]（DoS：Denial of Service）给很多因特网服务提供商带来了巨大的麻烦和经济损失，如 2003 年 8 月发生的著名的微软公司 windowsupdate. com 更新网站的拒绝服务攻击事件，在这次网络攻击事件中，受全球冲击波病毒发作的影响造成该网站陷入瘫痪。本文将分析 DoS 的攻击原理，在此基础上结合几种流行的拒绝服务攻击方式，探讨其防范措施，并结合实际工作中的处理经验，提出 SYN Flooding 的故障处理方法。

2　拒绝服务攻击

DoS 是指攻击者有意阻碍合法用户使用某一服务的行为，攻击发生时消耗网络带宽或系统的其它有用资源，导致网络或系统不胜负荷，以陷于瘫痪。

攻击者可能采取以下三种方式中的一种或多种使服务系统崩溃：

（1）带宽耗尽——用大量数据阻塞用户与服务器之间的通信链路；

（2）资源耗竭——用大量请求消耗服务器系统资源；

（3）程序缺陷——利用受害主机所提供服务中处理数据上的缺陷，反复发送畸形数据，引发服务程序错误，大量占用系统资源

拒绝服务攻击技术采取了破坏网络服务的方式，其根本目的是使受害主机或网络不能及时接受和处理外部请求，或无法及时回应请求，使正常的用户服务请求无法得到响应，造成“拒绝服务”。

下面介绍几种常见的与计算环境主体相关的拒绝服务攻击。

2.1　SYN Flooding

SYN Flooding[2]是最广泛流行的拒绝服务攻击方式之一，它利用了 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，从而使得被攻击方资源耗尽（CPU 满负荷或内存不足）；其攻击方式及流程参见图 1。

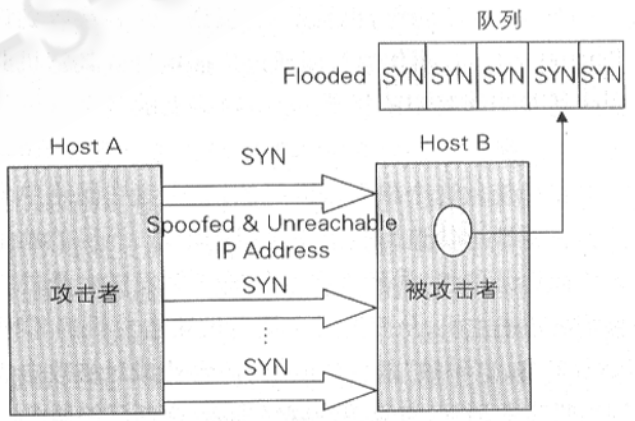

图 1　TCP SYN Flooding 攻击

正常的 TCP 连接需要进行三次握手过程，通常情况下，系统 B 在向系统 A 发送完 SYN/ACK 分组后，会停处在一个 SYN_RECV 状态，等待系统 A 返回一个 ACK

分组，此时系统 B 已经为准备建立此次连接分配了相应的资源，如果系统 A 是个攻击者，使用了假冒的发送地址，那么系统 B 将始终处于等待的“半连接”状态，直到连接建立定时器因超时而将该连接从系统的连接队列中清除为止；由于定时器设置的长短及连接队列被填满等原因，发动攻击的系统 A 在很短的时间内只要持续高速发送源地址经过伪装的连接请求到系统 B，就可以成功地对目标系统 B 实施拒绝服务攻击，系统 B 此时已经不能响应其它正常的服务连接请求。

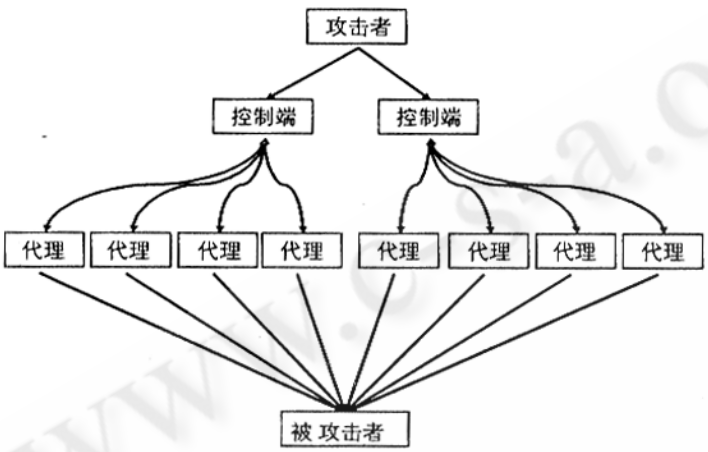

图 2　分布式拒绝服务攻击原理

2.2 Smurf (ICMP Sttack)

当网络中的某台计算机使用广播地址发送一个 ICMP echo 请求包时(例如 ping)，一些系统会回应一个 ICMP echo 回应包，也就是说，发送一个包会收到许多的响应包。广播信息可以通过广播地址或其它机制发送到整个网络中的机器，如向网络上的多个系统发送定向广播(directed broadcast)的 ping 请求。Smurf 攻击就是使用这个原理来进行的，攻击者在网络中发送出将源地址伪造为被攻击主机的地址、而目的地址为广播地址的包，导致许多系统响应并发送大量的信息给被攻击主机，从而造成大量到被攻击主机的 ICMP echo 回应，这种被“放大”了的回应会造成对被攻击者网络带宽的消耗，直至造成网络拥堵，中断网络服务。

2.3 Fraggle

Fraggle 基本概念及方法与 Smurf 类似，但它采用的是 UDP echo 信息。

2.4 分布式拒绝服务攻击

分布式拒绝服务[3](DDoS：distribution Denial of service)攻击作为一种新型的网络攻击手段，在近几年对网络安全已经构成极大的威胁。

分布式拒绝服务攻击从本质上说与 DoS 攻击使用的技术方法类似，但由于其在形式上具有分布式的特点，因此更具有危害性。DDoS 一般使用攻击工具进行，常用的工具有：Trinoo、TFNT、FN2K 等。攻击分为 3 层，分别是攻击者、主控端和代理端。攻击者是主控台，操纵整个攻击过程，它向主控端发送攻击命令；主控端是攻击者非法侵入并控制的一些主机，这些主机又分别控制大量的代理主机，主控端通过特定的程序接受攻击者发来的特殊指令，并把这些命令发送到代理主机上；代理端是攻击的执行者，它运行攻击器程序，接受和运行主控端发来的命令。

3 整体安全策略和防御措施

应对拒绝服务攻击需要做好基础的防御措施，从计算机系统和网络设备等方面运用技术手段来检测和预防攻击的发生，但更重要的是要制定和实施完善的安全防御策略，提高计算机和网络系统的整体安全性，将安全风险降到最低。

3.1 防御措施

SYN Flooding、Smurf 及 Fraggle 都是资源耗尽型网络攻击，我们可以从不同的角度来制定防御措施，总的来说可以从服务器和网络设备两个方面进行。在这里我们主要讨论应对 SYN Flooding 的措施。

(1) 改进服务器的 TCP 协议栈。如 SYN Cookie，运用该方法时，服务器并不对每个连接请求分配缓冲区，只有在确信连接建立后，才会分配缓冲区，可以缓解和消除攻击。

(2) Synkill。该方法是在服务器上通过监听方式检测 SYN Flooding 攻击，发现异常连接可以通过发出 RST 包来解除攻击。

(3) SYN Proxy。在防火墙上设置 SYN Proxy，利用防火墙来代替服务器进行 TCP 的三次握手，所有的半连接都被防火墙截取，对于正常的连接请求，则由防火墙充当请求者和服务器之间的连接管道。

(4) Ingress Filtering。在路由器设置“网络入口过滤”，检查过往包的源 IP 地址，以防止地址伪装。

由于不需要改变服务器的协议栈，采用基于防火墙/路由器的方法——即：SYN Proxy 和 Ingress Filte-

ring——更具有通用意义。由于在一般的网络中都会配置性能较好的路由器，因此这两种方式中，利用路由器来实现的 Ingress Filtering 方法又更具有普遍应用的意义。下面我们将对 Ingress Filtering 方法进行详细说明。

Ingress Filtering "入口过滤"是在路由器上设置 TCP 拦截或监视来实现的，相应的工作模式称为拦截模式和监视模式。拦截模式的工作原理与 Proxy 有点类似，是由路由器替代被请求服务器与请求者建立连接，这种方式比较耗费系统资源，也会增加建立初始会话的时延；监视模式允许请求者的 SYN 直接到达服务器，但是如果会话在系统设定的门限时间内还没有建立起来，则由路由器主动给服务器发送 RST 清除该连接。

此外，对源地址欺骗的淹没型攻击，仅靠"入口过滤"等特征匹配的方法来检测是不够的，因为存在同一攻击手法的不断演变，存在匹配速度的处理瓶颈，因此这种设置往往只能起到增加攻击者实施攻击的难度的作用，并不能抵制和化解攻击，在网络速度不断攀升的今天，也难以满足实际应用的需要。

3.2 安全防御策略

通过改进系统协议栈、加载监听程序及启用路由器/防火墙等网络设备的 DoS 防御功能，可以在一定程度上缓解、阻碍攻击，但很难完全阻止攻击。由于 DoS 攻击具有隐蔽性的特点，寻求行之有效的解决方法是不容易的，因此要加强安全防范意识，从计算机系统和网络设备、安全设备等多个方面一起入手，提高整体安全性。根据我们多年的工作经验，建议可采取以下安全防御策略：

(1) 及时安装系统补丁程序，禁止不用的服务，管理好计算机自身系统安全，不给攻击者可乘之机。同时，还要安装、启用个人防火墙/系统防火墙和防病毒软件，增强计算机系统的整体安全性。

(2) 建立有效的网络运行监管体系，经常检查系统配置信息、运行情况和安全日志，记录网络正常运行时的流量情况，为网络发生攻击时的预警和处理积累第一手资料。

(3) 在兼顾网络性能的基础上，尽量利用网络设备提供的安全设置进行防护，如在路由器上设置访问控制列表，禁止常见的漏洞扫描端口，启用流量管理 CAR 等。

(4) 网络安全设备是不可或缺的抵御攻击工具，经过合理配置的高性能防火墙和 IDS、IPS 设备能在很大程度上抵御攻击，保护网络的安全。

4 SYN 同步攻击处理过程

即使做了很多安全保护措施，但是要保证计算机和网络系统没有一点安全遗漏是很难的。下面分析一旦不幸遭遇了 SYN 攻击后，应如何处理才能减低攻击带来的损害，并最终阻止攻击。

网络攻击有来自网络内部的，也有来自网络外部的。有调查表明，80% 的网络攻击都来自网络内部(即使有的内部主机被来自外部的黑客植入了木马之类的程序而成为攻击者，但从直观后果看来攻击也是从内部发起的)，因此我们假定攻击从内部发起。

(1) 确定攻击影响范围。对于具有 Internet 接入的网络，存在内部网络和外部网络的区分，因此尽管攻击源存在于网络内部，但攻击的对象可能是外部 Internet 的某个服务器，也可能是内部网络上的某个服务器；两者带来的攻击影响范围也是不尽相同的，前者可能会耗尽 Internet 接入带宽，导致本地 Internet 服务中断，后者可能会影响内部网络的运行，出现业务网络中断的严重后果。确定受攻击影响的网络范围是非常重要的，这样可以引导我们向正确的方向查找攻击源。

(2) 查看安全设备、网络设备运行情况，追查攻击源。根据确定的范围，如果是影响到 Internet 连接的攻击发生，首先要查看防火墙和接入路由器的运行情况，包括 CPU、内存、端口等，并与平时记录的数据进行对比，以确定有无通信异常情况发生(异常情况包括在没有新增通信业务的情况下，系统的 CPU、内存的使用率或某些端口的流量突然比平常增加很多且持续不下)。对于防火墙设备，如果有大量突发的来自同一源地址或去往同一目的地址的线程出现，那么这种情况是非常可疑的，应列为重点检查对象。

如果攻击只影响到内网，则要有针对性地查看主要路由器和交换机的运行情况，通过 CPU、内存、端口的变化情况来逐级向下排查。很多攻击所用的数据包使用了伪 IP，直接查找是不可能的，但每个数据包中都有上一级路由器的物理地址，通过逐级查找路由器直

到最后的接入交换机，将攻击源细化到最后一层接入网络。

如何迅速发现网络中出现的通信异常，并及时确定相应的准确技术参数（如：异常通信的具体流向和流量信息，占用的网络端口，持续的时间等）是管理员能否在短时间内对网络安全攻击作出正确响应，减少对业务影响的一个关键因素。同时，网络管理员对网络设备日常运行情况的监视和准确把握也是非常重要的。

（3）利用网络流量监测技术和工具，帮助确定攻击源。Cisco 交换机/路由器设备提供了一种用于网络流量的检测技术——Netflow 。Netflow 可以对流经网络设备的 IP 数据流进行监测，形成不同类型业务的正常通信基线。这些数据可以输出到一个管理服务器上，由安全管理系统进行进一步的特征分析。在处理 SYN 攻击时运用 Netflow 技术也能起到很好的追踪作用。

如在一个启用了 Netflow 的交换机上检查目标端口为 4444（红色代码病毒）的网络流量情况，根据结果可以进一步进行攻击源的追踪。下面的命令输出结果描述了该交换机上目的端口为 4444 的 ip 流量情况，以及产生该流量的源地址和目的地址，这些信息可以帮助我们查找哪些主机可能已经感染了红色代码病毒。

```
sw > (enable) show mls statistics entry ip dst - port 4444
estination IP      Source IP      Prot   DstPrt
- - - - - - - - - - - - - - - - - - - - - - - - - - - -
10.10. * . *       10.20. * . *   TCP    4444
SrcPrt   Stat - Pkts   Stat - Bytes
- - - - - - - - - - - - - - - - - - - - - - - - - - - -
3076     8090          39902080
```

另外还可以在接入最终用户的交换机上运用 Sniffer 工具对网络流量进行实时监视，通过对监视结果的分析找出异常的网络连接，将源地址与连网用户信息比对找出重点怀疑对象，并将之立即从网络上剥离。网络嗅探器 Sniffer 在网络故障排查中是很有利用价值的工具，在排查的许多环节都可以用上。

（4）查找异常进程/服务，确定攻击程序。进入重点怀疑的计算机系统，使用 netstat 命令查看系统连接，因为 SYN Flooding 攻击会造成很多处于 SYN_RECV 状态的连接，如果系统上有很多这样的连接存在，那该系统很可能就是攻击源。进一步查找异常进程或服务，确定攻击使用的工具或程序并立即予以清除。接下来的工作很重要，要对该计算机进行彻底的安全漏洞检查并采取相应的补救措施，在确认系统安全之前，该计算机不能再接入到网络中。

攻击查找的过程是很复杂的，可能需要反复应用以上过程，在排查中要做好每次检查结果和分析结论的记录，避免做重复的无用功。有的攻击并不一定造成很大的突发网络流量，但超大量的连接请求会吞噬安全设备、网络设备的 CPU、内存资源，造成网络中断。此类攻击的排查也是很困难的；如果网络已经被攻击并陷入瘫痪状态，明确故障现象后，在网络层次建设良好的网络中，可以采用逐级物理网络隔离的办法来迅速查找攻击源，如逐个拔除接入交换机的上连网络线缆，一旦攻击源所在的网络接入交换机被拔除，受攻击造成的网络故障将很快被解除，然后再在被剥离的小范围内查找攻击源，将攻击带来的危害降到最低。

如果攻击是分布式的，处理起来会更加困难，但仍可以借鉴上述排查方法，所不同的是，找到实施攻击的“攻击源”后，并没有完成所有的攻击查找工作，还需要继续查找主控制点和真正的攻击者。

5 结束语

应对 DoS 攻击是一个系统化、长期的安全问题，任一环节都不能有任何疏漏。限于篇幅，本文未对 DDoS 攻击做详细深入的分析，但文中的防御措施和攻击处理办法对处理 DDoS 攻击也有很好的借鉴意义。

参考文献

1 Denial of Service Attacks [EB/OL]. http://www.cert.org/tech_tips/denial_of_service.html, CERT Coordination Center, Oct. 1997.

2 McClure, Secmbray, Kurtz, 《网络安全机密与解决方案》[M], 清华大学出版社, 2000.9。

3 Jelena? Mirkovic, Sven? Dietrich, David? Dittrich, Peter? Reiher . Internet Denial of Service: Attack and Defense Mechanisms[EB/OL]. 2004.5.