DDoS 攻击与防御技术

江苏省电子信息产品质量监督检验研究院　　程恺

摘要：DDoS 全名是 Distribution Denial of service (分布式拒绝服务攻击)，很多 DoS 攻击源一起攻击某台服务器就组成了 DDoS 攻击，DDoS 最早可追述到 1996 年最初，在中国 2002 年开发频繁出现，2003 年已经初具规模。

关键词：DDoS 攻击　DDoS 防御

一、DDoS 攻击概念：

DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。

DDoS 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式的，当攻击目标 CPU 速度低、内存小或者网络带宽小等等各项性能指标不高它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了。目标对恶意攻击包的"消化能力"加强了不少，例如你的攻击软件每秒钟可以发送 3,000 个攻击包，但我的主机与网络带宽每秒钟可以处理 10,000 个攻击包，这样一来攻击就不会产生什么效果。

这时侯分布式的拒绝服务攻击手段（DDoS）就应运而生了。理解了 DoS 攻击的话，它的原理就很简单。如果说计算机与网络的处理能力加大了 10 倍，用一台攻击机来攻击不再能起作用的话，攻击者使用 10 台攻击机同时攻击呢？用 100 台呢？DDoS 就是利用更多的傀儡机来发起进攻，以比从前更大的规模来进攻受害者。

高速广泛连接的网络给大家带来了方便，也为 DDoS 攻击创造了极为有利的条件。在低速网络时代时，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干节点之间的连接都是以 G 为级别的，大城市之间更可以达到 2.5G 的连接，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以在分布在更大的范围，选择起来更灵活了。

二、被 DDoS 攻击时的现象：

1.被攻击主机上有大量等待的 TCP 连接。

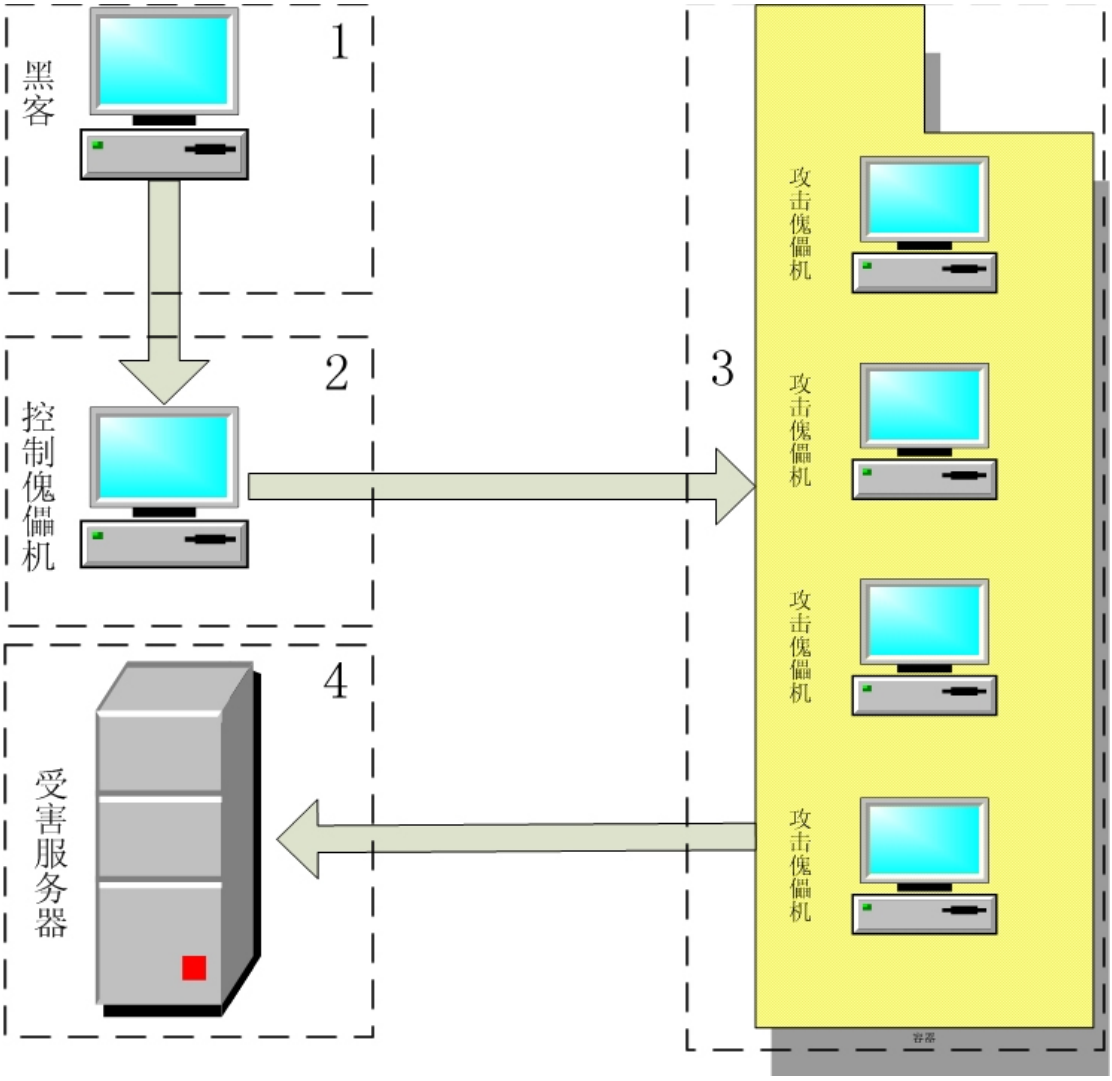
2.网络中充斥着大量的无用的数据包，源地址为假。

3.制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯。

4.利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求。

5.严重时会造成系统死机。

三、攻击运行原理：



图一 DDoS 攻击体系示意图

如图一，一个比较完善的 DDoS 攻击体系分成四大部分，先来看一下最重要的第 2 和第 3 部分：它们分别用做控制和实际发起攻击。请注意控制机与攻击机的区别，对第 4 部分的受害者来说，DDoS 的实际攻击包是从第 3 部分攻击傀儡机上发出的，第 2 部分的控制机只发布命令而不参与实际的攻击。对第 2 和第 3 部分计算机，黑客有控制权或者是部分的控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自黑客的指令，通常它还会利用各种手段隐藏自己不被别人发现。在平时，这些傀儡机器并没

有什么异常，只是一旦黑客连接到它们进行控制，并发出指令的时候，攻击傀儡机就成为害人者去发起攻击了。

为什么黑客不直接去控制攻击傀儡机，而要从控制傀儡机上转一下呢？这就是导致 DDoS 攻击难以追查的原因之一了。做为攻击者的角度来说，肯定不愿意被捉到，而攻击者使用的傀儡机越多，他实际上提供给受害者的分析依据就越多。在占领一台机器后，高水平的攻击者会首先做两件事：1.考虑如何留好后门。（以后还可以回来继续控制）2.如何清理日志。这就是擦掉脚印，不让自己做的事被别人查觉到。比较不专业的黑客会不管三七二十一把日志全都删掉，但这样的话网管员发现日志都没了就会知道有人干了坏事了，顶多无法再从日志发现是谁干的而已。相反，真正的好手会挑有关自己的日志项目删掉，让人看不到异常的情况。这样可以长时间地利用傀儡机。

但是在第 3 部分攻击傀儡机上清理日志实在是一项庞大的工程，即使在有很好的日志清理工具的帮助下，黑客也是对这个任务很头痛的。这就导致了有些攻击机弄得不是很干净，通过它上面的线索找到了控制它的上一级计算机，这上级的计算机如果是黑客自己的机器，那么他就会被揪出来了。但如果这是控制用的傀儡机的话，黑客自身还是安全的。控制傀儡机的数目相对很少，一般一台就可以控制几十台攻击机，清理一台计算机的日志对黑客来讲就轻松多了，这样从控制机再找到黑客的可能性也大大降低。

四、黑客是如何组织一次 DDoS 攻击的？

这里用"组织"这个词，是因为 DDoS 并不象入侵一台主机那样简单。一般来说，黑客进行 DDoS 攻击时会经过这样的步骤：

1.搜集了解目标的情况：

黑客最关心以下一些信息：被攻击目标主机数目、地址情况；目标主机的配置、性能；目标的带宽。

对于 DDoS 攻击者来说，攻击互联网上的某个站点，如 http://www.mytarget.com，有一个重点就是确定到底有多少台主机在支持这个站点，一个大的网站可能有很多台主机利用负载均衡技术提供同一个网站的 www 服务。以 yahoo 为例，一般会有下列地址都是提供 http://www.yahoo.com 服务的：

66.218.71.87

66.218.71.88

66.218.71.89

66.218.71.80

66.218.71.81

66.218.71.83

66.218.71.84

66.218.71.86

如果要进行 DDoS 攻击的话，应该攻击哪一个地址呢？使 66.218.71.87 这台机器瘫掉，但其他的主机还是能向外提供 www 服务，所以想让别人访问不到 http://www.yahoo.com 的话，要所有这些 IP 地址的机器都瘫掉才行。在实际的应用中，一个 IP 地址往往还代表着数台机器：网站维护者使用了四层或七层交换机来做负载均衡，把对一个 IP 地址的访问以特定的算法分配到下属的每个主机上去。这时对于 DDoS 攻击者来说情况就更复杂了，他面对的任务可能是让几十台主机的服务都不正常。

所以说事先搜集情报对 DDoS 攻击者来说是非常重要的，这关系到使用多少台傀儡机才能达到效果的问题。简单地考虑一下，在相同的条件下，攻击同一站点的 2 台主机需要 2 台傀儡机的话，攻击 5 台主机可能就需要 5 台以上的傀儡机。有人说做攻击的傀儡机越多越好，不管你有多少台主机我都用尽量多的傀儡机来攻就是了。

但在实际过程中，有很多黑客并不进行情报的搜集而直接进行 DDoS 的攻击，这时候攻击的盲目性就很大了，效果如何也要靠运气。其实做黑客也象网管员一样，是不能偷懒的。一件事做得好与坏，态度最重要，水平还在其次。

2.占领傀儡机：

黑客最感兴趣的是有下列情况的主机：链路状态好的主机；性能好的主机；安全管理水平差的主机。

这一部分实际上是使用了另一大类的攻击手段：利用形攻击。这是和 DDoS 并列的攻击方式。简单地说，就是占领和控制被攻击的主机。取得最高的管理权限，或者至少得到一个有权限完成 DDoS 攻击任务的帐号。对于一个 DDoS 攻击者来说，准备好一定数量的傀儡机是一个必要的条件，下面说一下他是如何攻击并占领它们的。

首先，黑客做的工作一般是扫描，随机地或者是有针对性地利用扫描器去发现互联网上那些有漏洞的机器，象程序的溢出漏洞、cgi、Unicode、ftp、数据库漏洞…(简直举不胜举啊)，都是黑客希望看到的扫描结果。随后就是尝试入侵了，具体的手段就不在这里多说了，感兴趣的话网上有很多关于这些内容的文章。

总之黑客现在占领了一台傀儡机了!然后他做什么呢？除了上面说过留后门擦脚印这些基本

工作之外，他会把 DDoS 攻击用的程序上载过去，一般是利用 ftp。在攻击机上，会有一个 DDoS 的发包程序，黑客就是利用它来向受害目标发送恶意攻击包的。

3.实际攻击：

经过前 2 个阶段的精心准备之后，黑客就开始瞄准目标准备发射了。前面的准备做得好的话，实际攻击过程反而是比较简单的。就象图示里的那样，黑客登录到做为控制台的傀儡机，向所有的攻击机发出命令，这时候埋伏在攻击机中的 DDoS 攻击程序就会响应控制台的命令，一起向受害主机以高速度发送大量的数据包，导致它死机或是无法响应正常的请求。黑客一般会以远远超出受害方处理能力的速度进行攻击。

老到的攻击者一边攻击，还会用各种手段来监视攻击的效果，在需要的时候进行一些调整。简单些就是开个窗口不断地 ping 目标主机，在能接到回应的时候就再加大一些流量或是再命令更多的傀儡机来加入攻击。

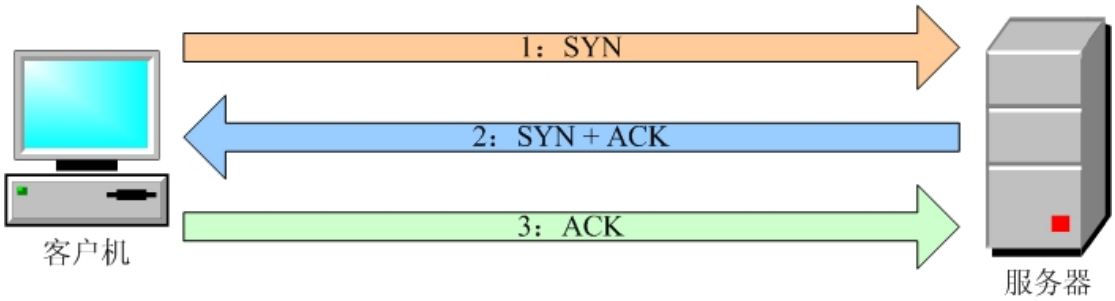
五、DDoS 攻击方式 - SYN Flood 攻击：

SYN-Flood 是目前最流行的 DDoS 攻击手段，早先的 DoS 的手段在向分布式这一阶段发展的时候也经历了浪里淘沙的过程。SYN-Flood 的攻击效果最好，应该是众黑客不约而同选择它的原因吧。那么我们一起来看看 SYN-Flood 的详细情况。

Syn Flood 原理 - 三次握手：

Syn Flood 利用了 TCP/IP 协议的固有漏洞。面向连接的 TCP 三次握手是 Syn Flood 存在的基础。

TCP 连接的三次握手：

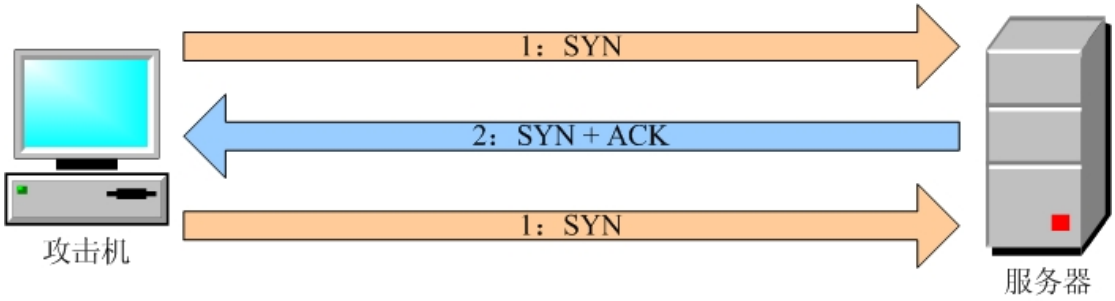


图二 TCP 三次握手

如图二，在第一步中，客户端向服务端提出连接请求。这时 TCP SYN 标志置位。客户端告诉服务端序列号区域合法，需要检查。客户端在 TCP 报头的序列号区中插入自己的 ISN。服务端收到该 TCP 分段后，在第二步以自己的 ISN 回应(SYN 标志置位)，同时确认收到客户

端的第一个 TCP 分段(ACK 标志置位)。在第三步中，客户端确认收到服务端的 ISN(ACK 标志置位)。到此为止建立完整的 TCP 连接，开始全双工模式的数据传输过程。

Syn Flood 攻击者不会完成三次握手：



图三 SYN Flood 恶意地不完成三次握手

假设一个用户向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的（第三次握手无法完成），这种情况下服务器端一般会重试（再次发送 SYN+ACK 给客户端）并等待一段时间后丢弃这个未完成的连接，这段时间的长度我们称为 SYN Timeout，一般来说这个时间是分钟的数量级（大约为 30 秒-2 分钟）；一个用户出现异常导致服务器的一个线程等待 1 分钟并不是什么很大的问题，但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源----数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的 CPU 时间和内存，何况还要不断对这个列表中的 IP 进行 SYN+ACK 的重试。实际上如果服务器的 TCP/IP 栈不够强大，最后的结果往往是堆栈溢出崩溃---即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求(毕竟客户端的正常请求比率非常之小)，此时从正常客户的角度看来，服务器失去响应，这种情况我们称做：服务器端受到了 SYN Flood 攻击（SYN 洪水攻击)。

六、DDoS 的防范：

到目前为止，进行 DDoS 攻击的防御还是比较困难的。首先，这种攻击的特点是它利用了 TCP/IP 协议的漏洞，除非你不用 TCP/IP，才有可能完全抵御住 DDoS 攻击。一位资深的安全专家给了个形象的比喻：DDoS 就好象有 1,000 个人同时给你家里打电话，这时候你的朋友还打得进来吗？

不过即使它难于防范，也不是说我们就应该逆来顺受，实际上防止 DDoS 并不是绝对不可行的事情。互联网的使用者是各种各样的，与 DDoS 做斗争，不同的角色有不同的任务。

我们以下面几种角色为例：

1.企业网管理员：

网管员做为一个企业内部网的管理者，往往也是安全员、守护神。在他维护的网络中有一些服务器需要向外提供 WWW 服务,因而不可避免地成为 DDoS 的攻击目标,他该如何做呢？可以从主机与网络设备两个角度去考虑。

（1）主机上的设置：几乎所有的主机平台都有抵御 DoS 的设置，总结一下，基本的有几种：关闭不必要的服务；限制同时打开的 Syn 半连接数目；缩短 Syn 半连接的 time out 时间；及时更新系统补丁。

（2）网络设备上的设置：企业网的网络设备可以从防火墙与路由器上考虑。这两个设备是到外界的接口设备，在进行防 DDoS 设置的同时，要注意一下这是以多大的效率牺牲为代价的，对你来说是否值得。

防火墙设置：禁止对主机的非开放服务的访问；限制同时打开的 SYN 最大连接数；限制特定 IP 地址的访问;启用防火墙的防 DDoS 的属性;严格限制对外开放的服务器的向外访问，主要是防止自己的服务器被当做工具去害人。

路由器：以 Cisco 路由器为例。Cisco Express Forwarding（CEF）；使用 unicast reverse-path；访问控制列表（ACL）过滤；设置 SYN 数据包流量速率；升级版本过低的 ISO；为路由器建立 log server。其中使用 CEF 和 Unicast 设置时要特别注意，使用不当会造成路由器工作效率严重下降，升级 IOS 也应谨慎。路由器是网络的核心设备，与大家分享一下进行设置修改时的小经验，就是先不保存。Cisco 路由器有两份配置 startup config 和 running config，修改的时候改变的是 running config，可以让这个配置先跑一段时间（三五天的就随意啦），觉得可行后再保存配置到 startup config；而如果不满意想恢复原来的配置，用 copy start run 就行了。

2.ISP / ICP 管理员：

ISP / ICP 为很多中小型企业提供了各种规模的主机托管业务，所以在防 DDoS 时，除了与企业网管理员一样的手段外,还要特别注意自己管理范围内的客户托管主机不要成为傀儡机。客观上说，这些托管主机的安全性普遍是很差的，有的连基本的补丁都没有打就赤膊上阵了，成为黑客最喜欢的"肉鸡"，因为不管这台机器黑客怎么用都不会有被发现的危险，它的安全管理太差了;还不必说托管的主机都是高性能、高带宽的-简直就是为 DDoS 定制的。而做为 ISP 的管理员，对托管主机是没有直接管理的权力的，只能通知让客户来处理。在实际情况时，有很多客户与自己的托管主机服务商配合得不是很好，造成 ISP 管理员明知自己

负责的一台托管主机成为了傀儡机，却没有什么办法的局面。而托管业务又是买方市场，ISP 还不敢得罪客户，怎么办？咱们管理员和客户搞好关系吧。客户多配合一些，ISP 的主机更安全一些，被别人告状的可能性也小一些。

3.骨干网络运营商：

他们提供了互联网存在的物理基础。如果骨干网络运营商可以很好地合作的话，DDoS 攻击可以很好地被预防。在 2000 年 yahoo 等知名网站被攻击后，美国的网络安全研究机构提出了骨干运营商联手来解决 DDoS 攻击的方案。其实方法很简单，就是每家运营商在自己的出口路由器上进行源 IP 地址的验证，如果在自己的路由表中没有到这个数据包源 IP 的路由，就丢掉这个包。这种方法可以阻止黑客利用伪造的源 IP 来进行 DDoS 攻击。不过同样，这样做会降低路由器的效率，这也是骨干运营商非常关注的问题，所以这种做法真正采用起来还很困难。

对 DDoS 的原理与应付方法的研究一直在进行中，找到一个既有效又切实可行的方案不是一朝一夕的事情。但目前我们至少可以做到把自己的网络与主机维护好，首先让自己的主机不成为别人利用的对象去攻击别人；其次，在受到攻击的时候，要尽量地保存证据，以便事后追查，一个良好的网络和日志系统是必要的。无论 DDoS 的防御向何处发展，这都将是一个社会工程，需要 IT 界的同行们一起关注，通力合作。