分布式拒绝服务攻击及防范研究 (1)

摘 要 随着网络应用的日益广泛，网络结构框架已经暴露在众多网络安全的威胁之下， DDoS攻击随处可见，人们为克服 DDoS攻击进行了大量研究，提出了多种解决方案。本文系统分析了 DDoS攻击的原理和方法，在分析具体的攻击工具的基础上给出防御方法。

关键词 拒绝服务攻击；分布式拒绝服务攻击；扫描；黑客

1 引言

随着网络应用的日益广泛，网络结构框架已经暴露在众多网络安全的威胁之下，其中拒绝服务 (DoS)攻击和基于 DoS的分布式拒绝服务 (DDoS)攻击最为常见。例如， 2000年黑客们使用 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、 163等站点也遭到类似的攻击。 2001年 5月对 CERT Co-ordination Center 的攻击， 2002年 5月对 edNET的攻击都造成了很大的损失 [1] 。在 2001年 4月的中美黑客大战中， DDoS也被广泛使用。随着高速网络的不断普及，尤其是随着近年来网络蠕虫的不断发展，更大规模 DDoS攻击的威胁也越来越大。

2 分布式拒绝服务 (DDoS)攻击

DoS是指攻击者在一定时间内向网络发送大量的服务请求，消耗系统资源或网络带宽，占用及超越被攻击主机的处理能力，导致网络或系统不胜负荷，停止对合法用户提供正常的网络服务； DDoS是在 DoS的基础上引入了 Client/Server 机制，使得攻击强度更大，隐藏性更高。

2.1 DDoS 攻击原理

DDoS采用多层的客户 / 服务器模式，一个完整的 DDoS攻击体系一般包含四个部分：攻击控制台、攻击服务器、攻击傀儡机和攻击目标，其攻击体系结构如图 1 所示。

◆ 攻击控制台。攻击者利用它来操纵整个攻击过程，它向攻击服务器下达攻击命令。

◆ 攻击服务器也叫主控端，它是攻击者非法入侵并且安装特定程序的

一些主机。它接收从攻击控制台发过来的各种命令。同时，它也控制了大量的攻击傀儡机，并向它们转发攻击控制台的攻击指令。

◆ 攻击傀儡机也叫代理端，它也是攻击者非法入侵并且安装特定程序的一些主机。它们上面运行攻击程序，用于对目标发起攻击。它受控于主控端，从主控端接收攻击命令，是攻击的执行者。

2.2 DDoS 攻击的特点

DDoS攻击作为一种特殊的 DoS攻击方式，相对于传统的拒绝服务攻击有自己很多的特点：首先，分布式拒绝服务的攻击效果更加明显。使用分布式拒绝服务，可以从多个傀儡主机同时向攻击目标发送攻击数据，可以在很短的时间内发送大量的数据包，使攻击目标的系统无法提供正常的服务。另外，由于采用了多层客户机 / 服务器模式，减少了由攻击者下达攻击命令时可能存在的拥塞，也增加了攻击的紧凑性。即使攻击目标探测到攻击，也可能来不及采取有效措施来应对攻击。其次，分布式拒绝服务攻击更加难以防范。因为分布式拒绝服务的攻击数据流来自很多个源且攻击工具多使用随机 IP 技术，增加了与合法访问数据流的相似性，这使得对攻击更加难以判断和防范。

最后，分布式拒绝服务对于攻击者来说更加安全。由于采用了多层客户机 / 服务器模式，增大了回溯查找攻击者的难度，从而可以更加有效地保护攻击者。另外，采用多层客户机 / 服务器模式，使得下达攻击指令的数据流更加分散，不容易被监控系统察觉，从而暴露攻击者的位置与意图。

3 攻击策略及防范

目前，随着多种 DDoS攻击工具如 TFN、TFN2K、Stacheldraht 、Trinoo 等的广泛传播，所面临 DDoS攻击的风险更是急剧增长 [2] 。所以，如何有效的防御 DDoS攻击成为当前一个亟待解决的问题。下面，本文针对这几种常用的攻击工具给出具体的防范措施。

3.1 TFN(Tribe Flood Network) 攻击及防范

TFN是德国著名黑客 Mixter 编写的，与 Trinoo 相似，都是在互联网的大量 UNIX系统中开发和测试的。它由客户端程序和守护程序组成，通过绑定到 TCP端口的 Root Shell 控制，实施 ICMP Flood，SYN Flood，UDP Flood 等多种拒绝服务的分布式网络攻击。

TFN客户端、主控端和代理端主机相互间通信时使用 IC-MP Echo 和 Icmp EchoReply 数据包。针对 TFN攻击的基本特性可采用如下抵御策略：

◆ 发动 TFN时，攻击者要访问 Master 程序并向它发送一个或多个目标 IP 地址，然后 Master 程序与所有代理程序通信，指示它们发动攻击。Master 程序与代理程序之间的通信使用 ICMP回音 / 应答信息包，实际要执行的指示以二进制形式包含在 16 位 ID 域中。ICMP使信息包协议过滤成为可能，通过配置路由器或入侵检测系统，不允许所有的 ICMP回音或回音 / 应答信息包进入网络就可以达到挫败 TFN代理的目的，但是这样会影响所有使用这些功能的

Internet 程序，如 Ping。Master 程序读取一个 IP 地址列表，其中包含代理程序的位置。这个列表可能使用如“ Blowfish ”的加密程序进行加密，如果没有加密，就可以从这个列表方便地识别出代理信息。

◆ 用于发现系统上 TFN代理程序的是程序 td，发现系统上 Master 程序的是程序 TFN。代理并不查看 ICMP回音 / 应答信息包来自哪里，因此使用伪装 ICMP信息包冲刷掉这些过程是可能的 [9] 。

3.2 TFN2k 攻击及防范

TFN2k代表 TFN 2000版，是 Mixter 编写的 TFN后续版本。这个新的DDoS工具已在原有的基础上大大前进了一步，它也是由两部分组成，即客户端程序和在代理端主机上的守护进程。客户端向守护进程发送攻击指定的目标主机列表，代理端守护进程据此对目标进行拒绝服务攻击。由一个客户端程序控制的多个代理端主机，能够在攻击过程中相互协同，保证攻击的连续性。客户端程序和代理端的网络通信是经过加密的，还可能混杂许多虚假数据包。整个TFN2k网络可能使用不同的 TCP, UDP或 ICMP包进行通信，而且客户端还能伪造其 IP 地址。所有这些特性都使发展防御 TFN2k攻击的策略和技术非常困难或效率低下。

TFN2k非常隐蔽，这些手段使得它很难被检测到。因为没有端口号，所以很难探测，即使在正常的基础上使用端口扫描程序也无法探测到用户的系统正被用作 TFN2k服务器 [10] 。目前仍没有能有效防御 TFN2k拒绝服务攻击的方法，最有效的策略是防止网络资源被用作客户端或代理端。

根据 TFN2k的基本特性，可采用的预防手段有以下几种：

◆ 只使用应用代理型防火墙，这能够有效地阻止所有的 TFN2k通信。但只使用应用代理服务器通常是不切实际的，因此只能尽可能地使用最少的非代理服务。

◆ 禁止不必要的 ICMP, TCP和 UDP通信，特别是对于 ICMP数据，可只允许 ICMP类型 3(Destination Unreachable ，目标不可到达) 数据包通过。如果不能禁止 ICMP协议，那就禁止主动提供或所有的 ICMP EchoReply 包。