中国青年黑客联盟站长 **flyingfox**又一力作!

黑客攻防技术内幕

II

张兴虎 王智贤 张新霞 编著

西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

张兴虎　王智贤　张新霞　编著

黑客攻防技术内幕

II

西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

内容提要

本书详细地介绍了目前黑客最新的攻击手法，并给出了相应的防范措施和应对办法。全部内容都采用具体实例进行讲解，使原本深奥、神秘的黑客攻击手段变得形象直观，生动有趣。

本书共分 10 章，主要是结合黑客技术的攻与防来讲解，具体内容包括 DOS 攻击、嗅探监听攻击、E-mail 攻击、缓冲区溢出攻击、木马攻击、QQ 攻防、系统漏洞攻击、密码破解技术、黑客攻击技巧等。

本书图文并茂，理论与实践相结合，注重黑客技术攻与防的可操作性，可作为广大计算机网络安全爱好者的学习指导书。随书赠送光盘一张，书中所涉及到的所有工具都在随书光盘中给出。

图书在版编目(CIP)数据

黑客攻防技术内幕. 2 / 张兴虎，王智贤，张新霞编著. —西安：西安交通大学出版社，2006. 9
ISBN 7 - 5605 - 2319 - 6

Ⅰ. 黑... Ⅱ. ①张... ②王... ③张 Ⅲ. 计算机网络-安全技术 Ⅳ. TP393. 08

中国版本图书馆 CIP 数据核字(2006)第 114349 号

书　　名	黑客攻防技术内幕Ⅱ
编　　著	张兴虎　王智贤　张新霞
出版发行	西安交通大学出版社
地　　址	西安市兴庆南路 25 号(邮编：710049)
电　　话	(029)82668357　82667874(发行部) (029)82668315　82669096(总编办)
印　　刷	陕西江源印刷科技有限公司
字　　数	468 千字
开　　本	787mm×1 092mm　1/16
印　　张	19. 375
版　　次	2006 年 9 月第 1 版　2006 年 9 月第 1 次印刷
书　　号	ISBN 7 - 5605 - 2319 - 6/TP・464
定　　价	32. 00 元(含工具软件 CD-ROM 一张)

前　言

《黑客攻防技术内幕》出版发行后得了广大读者的好评，也收到了广大读者诚恳的建议。该书在多次印刷热卖之后，授权 SOHU、网易同时连载，一时间国内外数百家黑客网站、网络安全网站纷纷转载，缔造了网络上最热门的计算机安全读物，作者也由此深受鼓舞，在此对一直关心《黑客攻防技术内幕》的读者表示感谢。计算机的发展每半年时间相当于人类的一个世纪，《黑客攻防技术内幕》出版五年之后，在众多网友的要求和朋友的支持下，作者针对目前黑客新的攻击手法并与《黑客攻防技术内幕》中的相关内容相结合编著了此书，也可以说该书是在原有《黑客攻防技术内幕》基础上的一次升级和完善。

网络安全发展到今天在无数个 IT 安全专家的努力下不断地得到了健全，而 DOS 攻击一直以来都没有可行的解决方案，它的来临如同洪水猛兽一样凶猛无阻，全球有不计其数的大网络都瘫痪于此攻击之下，在本书的第 1 章中我们将详细地向大家介绍 DOS 攻击的原理及演示。

当你的计算机在没有感染任何病毒、木马的情况下，你管理 Web 服务器的 FTP 密码被黑客盗取！你的电子信箱密码也被盗取！甚至你同别人 MSN 聊天的记录也被黑客知道！这到底是怎么一回事呢？其实这是一种来源于黑客嗅探监听的攻击，在本书的第 2、第 3 章将以各种实例来详细地介绍基于黑客的嗅探监听的攻与防。

E-mail 是全球互联网中使用最多的网络服务，除了手机、电话通信外，E-mail 是全球第二大通信方式，利用 E-mail 不但拉近了人与人之间交流的距离，更大的意义在于这是人类社会交流方式的革命性变化，然而黑客针对 E-mail 的攻击也随之而来，具体内容本书在第 4 章将详细介绍。

缓冲区溢出攻击一直以来是计算机安全防卫的弱点，本书第 5 章就黑客针对缓冲区溢出攻击做了非常全面的介绍，从一个个缓冲区溢出漏洞的发现到被黑客利用该漏洞对全球计算机安全的挑战；从最早的 IIS 缓冲区溢出到最新的系统服务缓冲区溢出；从 Windows DCOM RPC 存在缓冲区溢出漏洞和 Microsoft SQL 存在缓冲区溢出到“冲击波”病毒和“SQL 蠕虫王”病毒对全球上亿台计算机的攻击等等，这些内容都将在本书中尽收读者的眼底。在介绍每一个缓冲区溢出攻击时，作者都专门架设了一台存在漏洞的主机，针对该溢出漏洞进行攻击演示，并提出相应的修补方案。通过每一步利用缓冲区溢出漏洞攻击计算机的截图与细致的文字讲解相结合，让读者更为全面地去了解、去认识缓冲区溢出漏洞的攻与防。

木马攻击是黑客所熟练掌握的一门技术，它仍然是一种对网络安全具极高威胁的黑客攻击技术，面对今天屡见不鲜的木马攻击，本书第 6 章详细介绍几款木马的使用及攻击演示，并针对目前木马攻击的防范、查杀提出合理有效的解决方案

QQ 是一个已被中国网民所熟知的即时通信工具，已拥有 1 亿多注册用户，达到最高在线人数超过 340 万人的超规模，名列亚洲即时通信软件首位，世界即时通信软件第三位。然而针

对 QQ 隐私的攻击也越来越受到国内黑客的关注，本书在第 7 章中将介绍关于 QQ 隐私保护的攻与防。

Word 加密密码忘记怎么办？Excel 加密密码忘记怎么办？可能这些问题你也经历过，在面对这些问题时令人深感头疼，其实大家不用着急，阅读本书的第 9 章内容，相信会给你一个满意的答案。

网络安全是一个永恒的话题，本书着眼于理论与实践相结合的方法，以图文并茂的方式介绍黑客的各种攻击及防范措施，让黑客不再神秘，让安全驾驭我们的电脑。因此，这是一本为每一位热爱网络安全研究的电脑爱好者“量身定制”的书籍。

最后，我要感谢对我工作、生活上一直给予帮助的李民仓叔叔和我的上级领导及我所在单位的同事王继军、刘小炜，在这里深深地感谢他们过去和现在对我的帮助与支持。

由于时间仓促，加之作者水平有限，书中难免有疏漏和不足之处，恳请广大读者批评指正。如果对本书内容有所疑问，可与作者联系。

网站：http://www.54hack.org

QQ：569962

张兴虎（网名：flyingfox）、王智贤、张新霞

2006 年 7 月

目　录

第1章　基于黑客DOS攻击

DOS攻击是目前比较有效而又非常难于防御的一种网络攻击方式，它的目的就是使服务器不能够为正常访问的用户提供服务。所以，DOS攻击对一些紧密依靠互联网开展业务的企业和组织带来了致命的威胁。本章将重点介绍DOS攻击原理、DOS攻击演示及相关解决方案。对DOS攻击的总体了解，将为有效避免攻击、查找攻击原因、制订相应对策提供有用的帮助。

1.1　初识DOS攻击

进入2000年以来，网络遭受攻击事件不断发生，全球许多著名网站如yahoo、cnn、buy、ebay、fbi，包括中国的新浪网相继遭到不明身份的黑客攻击。值得注意的是，在这些攻击行为中，黑客摈弃了以往常常采用的更改主页这一对网站实际破坏性有限的做法，取而代之的是，在一定时间内，彻底使被攻击的网络丧失正常服务功能，这种攻击手法为DOS攻击。

DOS(Denial of Service，拒绝服务)攻击由于攻击简单、容易达到目的、难于防止和追查，越来越成为常见的攻击方式，这种攻击行动使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪，而停止提供正常的网络服务。

“拒绝服务”的攻击方式为：用户传送众多要求确认的信息到服务器，使服务器里充斥着这种无用的信息。所有的信息都有需回复的虚假地址，以至于当服务器试图回传时，却无法找到用户。服务器于是暂时等候，有时超过一分钟，然后再切断连接。服务器切断连接时，黑客再度传送新一批需要确认的信息，这个过程周而复始，最终导致服务器无法工作。

DOS攻击可以有各种分类方法，如果按照攻击方式可以分为：资源消耗、服务中止和物理破坏 。资源消耗指攻击者试图消耗目标的合法资源，例如网络带宽、内存和磁盘空间、CPU使用率等等。服务中止则是指攻击者利用服务中的某些缺陷导致服务崩溃或中止。物理破坏则是指雷击、电流、水火等物理接触的方式导致的拒绝服务攻击。

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时它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速提高，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，例如你的攻击软件每秒钟可以发送2 000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。

这时候分布式的拒绝服务攻击手段(DDOS)就应运而生了。你理解了DOS攻击，DDOS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，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，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分布在更大的范围，选择起来更灵活了。

从上面可以看出 DOS 攻击分为 3 层：攻击者、主控端、代理端，三者在攻击中扮演着不同的角色。

(1) 攻击者　攻击者所用的计算机是攻击主控台，可以是网络上的任何一台主机，甚至可以是一个活动的便携机。攻击者操纵整个攻击过程，它向主控端发送攻击命令。

(2) 主控端　主控端是攻击者非法侵入并控制的一些主机，这些主机还分别控制大量的代理主机。主控端主机的上面安装了特定的程序，因此它们可以接受攻击者发来的特殊指令，并且可以把这些命令发送到代理主机上。

(3)代理端　代理端同样也是攻击者侵入并控制的一批主机，在它们上面运行攻击器程序，接受和运行主控端发来的命令。代理端主机是攻击的执行者，真正向受害者主机发送攻击。攻击者发起 DDOS 攻击的第一步，就是寻找在 Internet 上有漏洞的主机，进入系统后在其上面安装后门程序，攻击者入侵的主机越多，它的攻击队伍就越庞大。第二步在入侵主机上安装攻击程序，其中一部分主机充当攻击的主控端，一部分主机充当攻击的代理端。最后各部分主机各司其职，在攻击者的调遣下对攻击对象发起攻击。由于攻击者在幕后操纵，所以在攻击时不会受到监控系统的跟踪，身份不容易被发现。

通过上面的分析，对 DOS 的攻击有了初步的了解，接下来具体看看常见 DOS 攻击原理及演示。

1.2　常见 DOS 攻击原理及演示

通过前面对 DOS 攻击概念的了解，本节将重点介绍三种常见的 DOS 攻击原理及演示。

1. SYN Flood

SYN Flood 是当前最流行的 DOS 攻击与 DDOS 攻击的方式之一。这是一种利用 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)的攻击方式。SYN Flood 由于其攻击效果好，已经成为目前最流行的 DOS 和 DDOS 攻击手段。

SYN Flood 利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，使得被攻击方资源耗尽，无法及时回应或处理正常的服务请求。一个正常的 TCP 连接需要三次握手，首先客户端发送一个包含 SYN 标志的数据包，其后服务器返回一个 SYN/ACK 的应答包，表示客户端的请求被接受，最后客户端再返回一个确认包 ACK，这样才完成 TCP 连接，如图 1-1 所示。

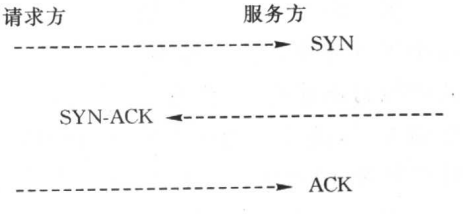

图 1-1　SYN Flood 攻击

问题就出在 TCP 连接的三次握手中，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，这段时间的长度称为 SYN Timeout，一般来说这个时间是分钟的数量级（大约为 30 秒至 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，期间这些半连接状态都保存在一个空间有限的缓存队列中，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，服务器端的 TCP 资源迅速耗尽，导致正常的连接不能进入，服务器失去响应，甚至会导致服务器的系统崩溃，这种情况称作：服务器端受到了 SYN Flood 攻击。

SYN Flood 攻击就是攻击者利用伪造的 IP 地址，连续向被攻击的服务器发送大量的 SYN 包。被攻击的服务器收到这些 SYN 包后，连续向那些虚假的客户机（伪造的 IP 地址指向的客户机）发送 ACK 确认包。很显然，服务器是不会收到 ACK 确认包的，于是服务器就只能等待了。当服务器因超时而丢弃这个包后，攻击者虚假的 SYN 包又源源不断地补充过来。在这个过程中，由于服务器不停顿地处理攻击者的 SYN 包，从而正常用户发送的 SYN 包会被丢弃，得不到处理，从而造成了服务器的拒绝服务。

下面以一个实例来看看 SYN Flood 攻击。

所用程序：X-DOS

演示说明：对 www.54hack.org 网站发动 SYN Flood 攻击。

操作演示：

（1）首先在命令提示符下对该网站执行 ping 命令测试，如图 1－2 所示，可以看到 www.54hack.org 网站正常。

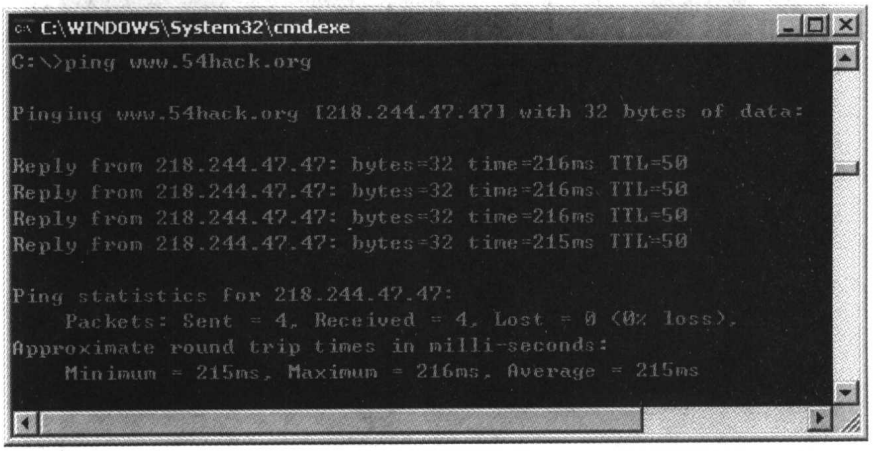

图 1－2　执行 ping 命令测试网站

(2)在命令提示符下运行 X-DOS 程序,X-DOS 共提供了两种攻击方法(如图 1-3 所示):

xdos <目标计算机> <端口>

xdos <目标计算机> <端口范围> <-t 每次发送攻击包数量> <-s 伪造的 IP 地址,* 为随机产生>

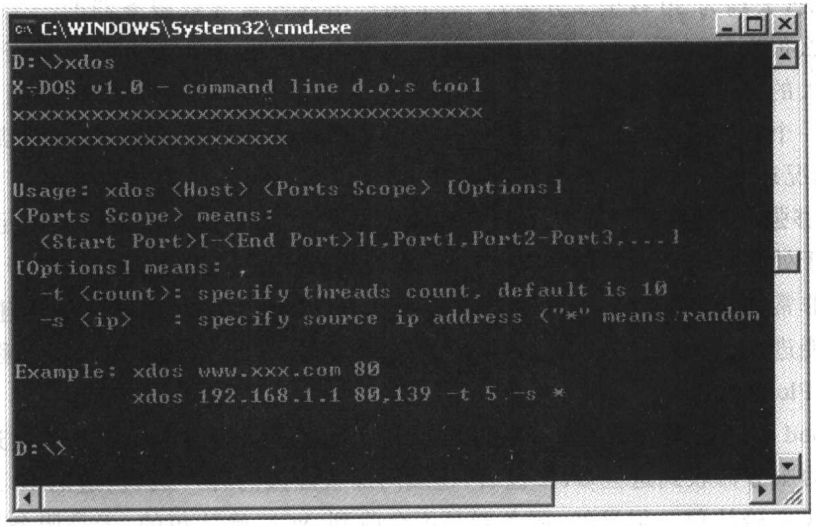

图 1-3 X-DOS 使用说明

(3)首先看看利用 X-DOS 程序第一种攻击方法来攻击 www.54hack.org 网站服务器,即在命令提示符下执行如下命令:

xdos www.54hack.org 80

命令解释:攻击目标服务器的 80 端口,即 Web 服务端口。

输入完成后,按【回车】键执行,从图 1-4 中可以看到,X-DOS 将以指定的 C 类 IP 地址 10.168.1.1,向目标网站 www.54hack.org 的服务器每次发送 10 个合法的 SYN 报文进行远程

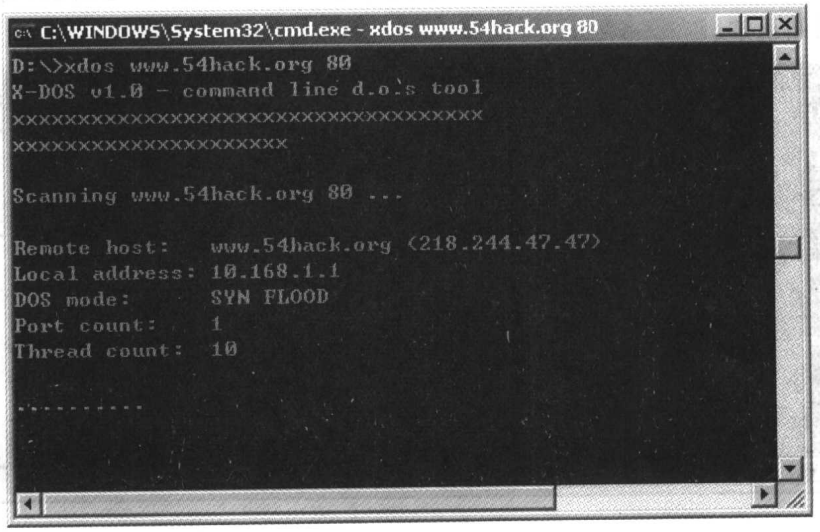

图 1-4 向目标计算机发动 SYN Flood 攻击

DOS 攻击。

(4)这时回到 www.54hack.org 所在的服务器上，发现服务器反应相当缓慢。在服务器上运行【命令提示符】程序，然后在命令提示符下执行“netstat-an”命令来查看当前服务器的网络连接，从如图 1－5 中可以看到：10.168.1.1 的 C 类 IP 地址段向服务器发送了大量的 SYN 包请求。

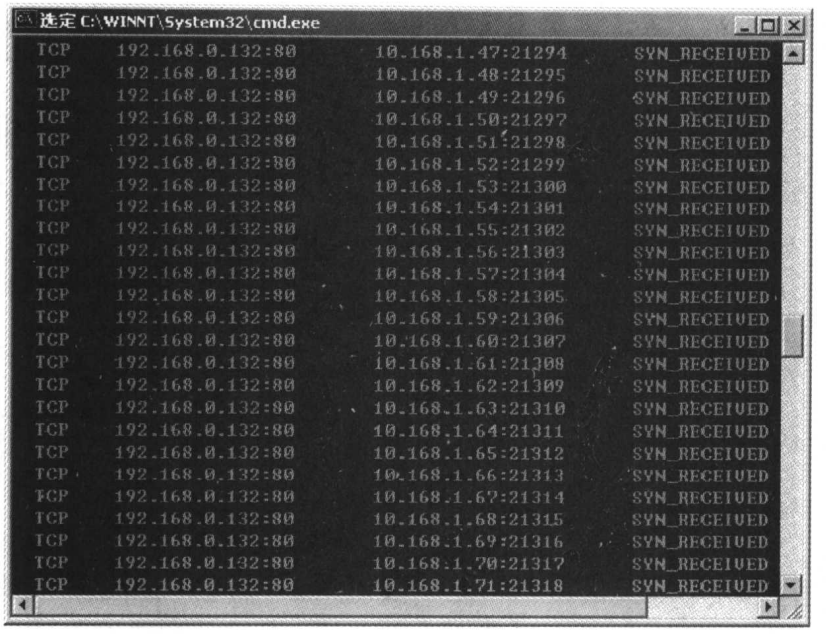

图 1－5　被 SYN Flood 攻击的计算机

(5)接下来看看利用 X-DOS 程序第二种攻击方法来攻击 www.54hack.org 网站服务器，即在命令提示符下执行如下命令：

xdos www.54hack.org 80－t 5－s*

输入完成后，按【回车】键执行，从图 1－6 中可以看到，X-DOS 将以随机产生的 IP 地址向

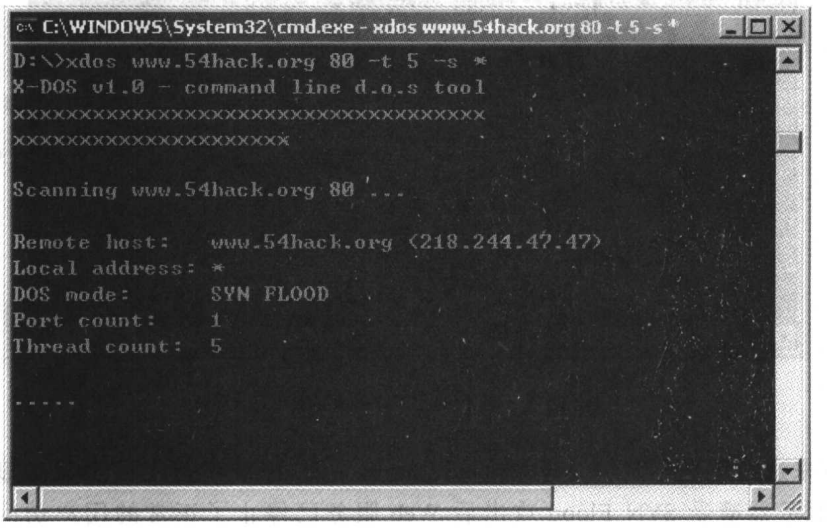

图 1－6　向目标计算机发动 SYN Flood 攻击

目标网站 www.54hack.org 的服务器每次发送 5 个合法的 SYN 报文进行攻击。

(6)这时再回到 www.54hack.org 所在的服务器上,在服务器上运行【命令提示符】程序,然后在命令提示符下执行“netstat-an”命令来查看当前服务器的网络连接,从图 1-7 可以看到:大量的 IP 地址段向服务器发送了极多的 SYN 请求。

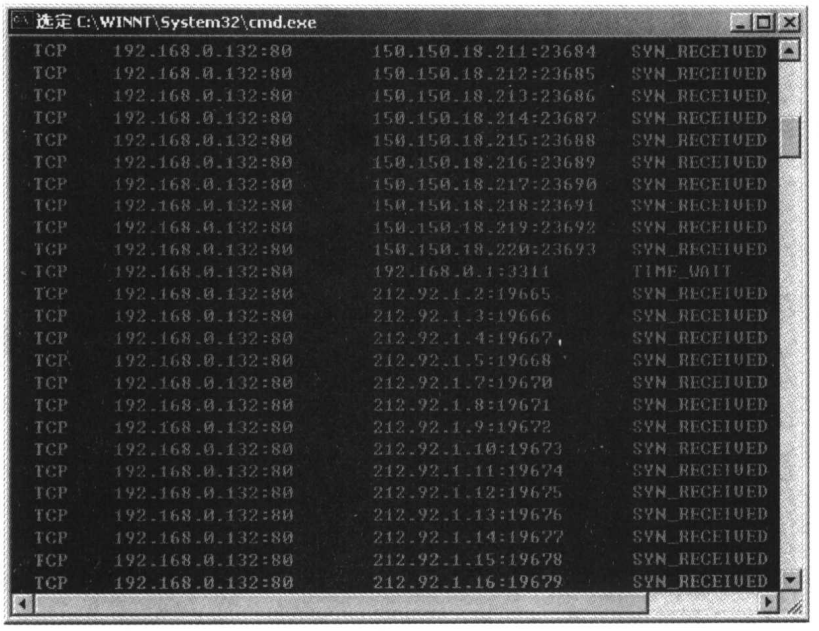

图 1-7 被 SYN Flood 攻击的计算机

(7)在以上两种攻击下,通过 ping 命令测试 www.54hack.org 网站,这时发现该网站网络极不稳定,出现了访问超时情况,如图 1-8 所示。

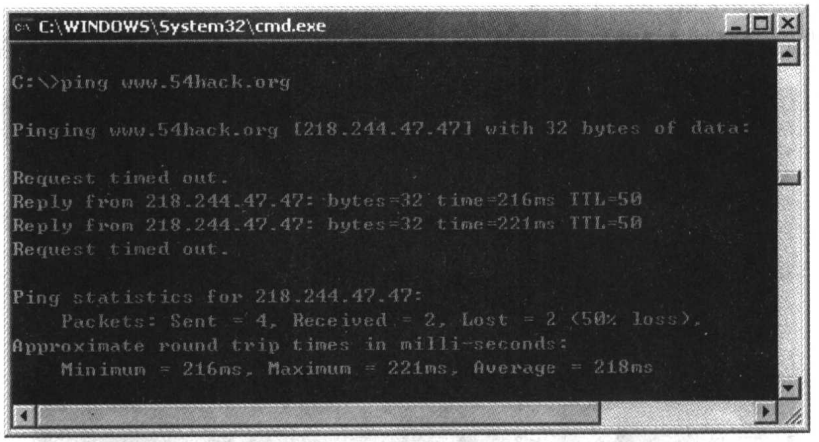

图 1-8 通过 ping 命令检测对方网络

(8)接下来通过浏览器打开 www.54hack.org 网站时,系统将显示该页无法显示(如图 1-9 所示),即该服务器遭受 SYN Flood 攻击后 Web 服务已停止了正常的用户访问响应,即 SYN Flood 攻击演示完成。

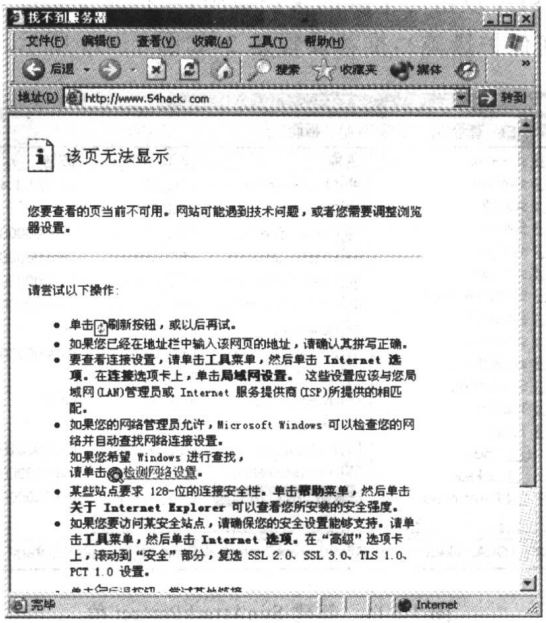

图 1-9　服务器停止响应

服务器忙于处理大量虚假的 SYN 包，已无法正常响应其它的工作了，通过以上攻击可以看到，SYN Flood 攻击力量是多么的巨大，一台计算机就可以把一个普通的网站攻击瘫痪。

SYN Flood 攻击给互联网造成重大影响，从防御角度来说，有如下几种简单的解决方法。

第一种是缩短 SYN Timeout 时间，由于 SYN Flood 攻击的效果取决于服务器上保持的 SYN 半连接数，这个值等于 SYN 攻击的频度乘以 SYN Timeout，所以通过缩短从接收到 SYN 报文到确定这个报文无效并丢弃该连接的时间，例如设置为 20 秒以下（过低的 SYN Timeout 设置可能会影响客户的正常访问），可以成倍地降低服务器的负荷，具体操作如下。

(1)选择【开始】→【运行】命令，在【打开】的下拉文本框中输入“regedit.exe”，单击【确定】按钮，运行【注册表编辑器】程序，如图 1-10 所示。

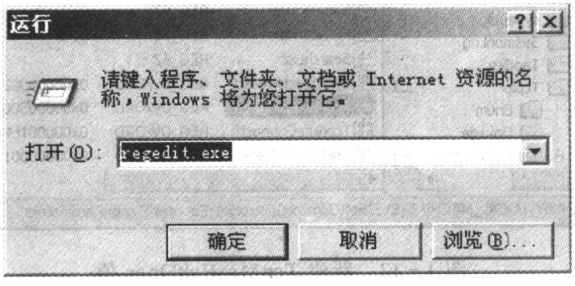

图 1-10　运行【注册表编辑器】程序

(2)依次展开以下键值：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

在右边窗口中新建一个 DWORD 值，其名称为 SynAttackProtect，设置其键值范围是0～2，