Windows(2000/XP)系统中怎样防止 Ping 的攻击

吴成茂，陈世琼

（西昌学院 信息技术系，四川 西昌 615013）

【摘 要】Ping 是用来检测网络连接性、可到达性和名称解析的主要 TCP/IP 命令，其主要用处就是检测目标主机是否可连通。黑客要入侵，首先需锁定目标，通常情况下使用 Ping 命令来检测主机，获取相关信息，然后再进行漏洞扫描。如何不受别人的攻击？那就是阻止别人 Ping 自己的电脑，让攻击无从着手。

【关键词】Ping；安全策略；防火墙；TCP/IP；ICMP

【中图分类号】TP309 【文献标识码】A 【文章编号】1673-1891(2006)01-0096-03

1 利用 ICMP 协议攻击的基本原理

ICMP 的全名是 Internet Control and Message Protocal，即因特网控制消息/错误报文协议，这个协议主要是用来进行错误信息和控制信息的传递，著名的 Ping 和 Tracert 工具都是利用 ICMP 协议中的 ECHO request 报文进行的。

ICMP 协议有一个特点——它是无连结的，也就是说只要发送端完成 ICMP 报文的封装并传递给路由器，这个报文将会像邮包一样自己去寻找目的地址，这个特点使得 ICMP 协议非常灵活快捷，但是同时也带来一个致命的缺陷——易伪造，任何人都可以伪造一个 ICMP 报文并发送出去，伪造者可以利用 SOCK_RAW 编程直接改写报文的 ICMP 首部和 IP 首部，这样的报文携带的源地址是伪造的，在目的端根本无法追查，基于这个原理，出现了不少基于 ICMP 的攻击软件，有通过网络架构缺陷制造 ICMP 风暴的、有使用非常大的报文堵塞网络的(如 2001 年的中美黑客大战)、有利用 ICMP 碎片攻击消耗服务器 CPU 的、甚至如果将 ICMP 协议用来进行通讯，制作出不需要任何 TCP/UDP 端口的木马，既然 ICMP 协议这么危险，那么为什么不关闭它呢？

2 阻止 Ping 的方法

2.1 用高级设置法预防 Ping

默认情况下，所有 Internet 控制消息协议(ICMP)选项均被禁用。如果启用 ICMP 选项，您的网络将在 Internet 中是可视的，因而易于受到攻击。

如果要启用 ICMP，必须以管理员或 Administrators 组成员身份登录计算机，右击“网上邻居”，在弹出的快捷菜单中选择“属性”即打开了“网络连接”，选定已启用 Internet 连接防火墙的连接，打开其属性窗口，并切换到“高级”选项页，点击下方的“设置”，这样就出现了“高级设置”对话窗口，在“ICMP”选项卡上，勾选希望计算机响应的请求信息类型，旁边的复选框即表示启用此类型请求，如果要禁用请清除相应请求信息类型即可。

2.2 用网络防火墙阻隔 Ping

使用防火墙来阻隔 Ping 是最简单有效的方法，现在基本上所有的防火墙都具有 ICMP 过滤的功能。在此，以天网防火墙 2.77 版为例来说明。

首先安装并运行天网防火墙，在其主界面上点击“IP 规则管理”，然后勾选“防止别人用 ping 命令探测”规则和“防御 ICMP 攻击”规则，然后点击“保存规则”按钮即可。

2.3 启用 IP 安全策略防 Ping

收稿日期：2005－07－05

作者简介：吴成茂(1976－　)，男，助教，主要从事计算机专业课的教学和研究工作。

IP 安全机制(IP Security)即 IPSec 策略，用来配置 IPSec 安全服务。这些策略可为现有网络中的多数通信类型提供各种级别的保护。您可配置 IPSec 策略以满足计算机、应用程序、组织单位、域、站点或全局企业的安全需要。可使用 Windows XP 中提供的“IP 安全策略”管理单元来为 Active Directory 中的计算机或本地计算机定义 IPSec 策略。

在此以 WINDOWS XP 为例，通过“控制面板”->“管理工具”来打开“本地安全策略”，选择“IP 安全策略”，在这里，我们可以定义自己的 IP 安全策略，一个 IP 安全过滤器由两个部分组成：过滤策略和过滤操作。要新建 IP 安全过滤器，必须新建自己的过滤策略和过滤操作，右击窗口左侧的“IP 安全策略，在本地机器”，在弹出的快捷菜单中选择“创建 IP 安全策略”，单击“下一步”，然后输入策略名称和策略描述。单击“下一步”，选中“激活默认响应规则”复选项，单击“下一步”。开始设置响应规则身份验证方式，选中“此字符串用来保护密钥交换(预共享密钥)”选项，然后随便输入一些字符(后面还会用到这些字符的)，单击“下一步”，就会提示已完成 IP 安全策略，确认选中了“编辑属性”复选框，单击“完成”按钮，会打开其属性对话框。

接下来就要进行此新建安全策略的配置。在“Goodbye Ping 属性”对话窗口的“规则”选项页中单击“添加”按钮，并在打开安全规则向导中单击“下一步”进行隧道终结设置，在这里选择“此规则不指定隧道”。单击“下一步”，并选择“所有网络连接”以保证所有的计算机都 Ping 不通。单击“下一步”，设置身份验证方式，与上面一样选择第三个选项“此字符串用来保护密钥交换(预共享密钥)”并填入与刚才上面相同的内容。单击“下一步”即打开“IP 筛选器列表”窗口，在“IP 筛选器列表”中选择“新 IP 筛选器列表”，单击右侧的“编辑”，在出现的窗口中点击“添加”，单击“下一步”，设置“源地址”为“我的 IP 地址”，单击“下一步”，设置“目标地址”为“任何 IP 地址”，单击“下一步”，选择协议类型为 ICMP，单击“完成”后再点“确定”返回，单击“下一步”，选择筛选器操作为“要求安全”选项，然后依次点击“下一步”、“完成”、“确定”、“关闭”按钮保存相关的设置返回管理控制台。最后在“本地安全设置”中右击配置好的“Goodbye Ping”策略，在弹出的快捷菜单中选择“指派”命令使配置生效。

经过以上设置，当其他计算机再 Ping 该计算机时，就不再 Ping 通了。但如果自己 Ping 本地计算机，仍可 Ping 通。在 Windows 2000 中操作基本相同。

2.4 修改 TTL 值防 Ping

TTL(Time To Live，即生存时间)是 IP 协议包中的一个值，它告诉网络路由器包在网络中的时间是否太长而应被丢弃。许多入侵者喜欢用 TTL 值来判断操作系统，他们首先会 Ping 一下你的计算机，如果看到 TTL 值为 128 就认为你的系统为 Windows NT/2000/XP，如果 TTL 值为 32 则认为目标主机操作系统为 Windows 95/98，如果为 TTL 值为 255/64 就认为是 UNIX/Linux 操作系统。既然入侵者相信 TTL 值所反应出来的结果，那么不妨修改 TTL 值来欺骗入侵者，达到保护系统的目的，方法如下：

点击“开始→运行”，在“运行”对话框中输入“regedit”命令并回车，弹出“注册表编辑器”对话框，展开下列分支：“HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/Tcpip/Parameters”，找到“DefaultTTL”，将该值修改为十进制的“255”，重新启动系统即可。

2.5 关闭操作系统的 ICMP 协议防击 Ping 攻击

Windows2000/XP 中自带了一个 TCP/IP 过滤器，可以用来关闭 ICMP 协议，操作方法：在桌面上右击网上邻居 -> 属性 -> 右击你要配置的网卡 -> 属性 -> TCP/IP -> 高级 -> 选项 -> TCP/IP 过滤，这里有三个过滤器，分别为：TCP 端口、UDP 端口和 IP 协议，先允许 TCP/IP 过滤，然后逐个来配置，先是 TCP 端口，点击“只允许”，然后在下面加上你需要开放的端口，一般来说 WEB 服务器只需要开 80(www)、FTP 服务器需要开 21(FTP Control)、邮件服务器需要打开 25(SMTP)、110(POP3)、以此类推……接着是 UDP，UDP 协议和 ICMP 协议一样是基于无连结的，一样容易伪造，所以如果不是必要，应该选择全部不允许，避免受到洪水（Flood）或碎片(Fragment)攻击。

3　结束语

经过设置后我们的计算机就可以防止 Ping 攻击了，并且对很多攻击手段都有了一定的防范及免疫功能，系统安全级别也大大提高了。当然没有绝对安全的网络系统，网络信息对抗是一个长期的研究课题，安全问题多种多样，且随着时间技术的变化而变化，而黑客的侵入手段也随之不断变化，所以安全

防护也是非常重要的，保持清醒正确的认识，同时掌握最新的安全问题情况，再加上完善有效的安全策略，是可以阻止大部分的网络入侵，从而保持最小程度的损失。

参考文献：

[1]顾巧论等．计算机网络安全．清华大学出版社，2004.
[2]李明柱等．黑客攻击与安全防范技巧及实例．北京航空航天大学出版社，2002.
[3]欧培中等．常见漏洞攻击与防范实战．四川电子音像出版中心，2002.
[4]叶丹．网络安全实用技术．清华大学出版社，2002.
[5]杨国强．中国电脑教育报．中国电脑教育报社，2005.

致谢：本文写作过程中得到了信息技术系伍治林副教授和高志坚副教授的热情指导，在此表示衷心的感谢！

How to Prevent the Attack from Ping in the Windows 2000/xp System

WU Cheng - mao, CHEN Shi - qiong

(*Xichang College, Xichang 615013, Sichuan*)

Abstract: Ping is the main TCP/ IP order used to examine network connectivity、accessibility and the name analysis , it is mainly used to examine whether the target computer can be connected or not, if the hacker invades, firstly he needs to lock the object and generally uses Ping order to examine the host computer to gain correlative information, then conduct the loophole scanning. How to avoid such attack? The answers is to prevent others ping your personal computer so that the attack cannot continue.

Key words: Ping; Security strategy; Firewall; TCP/IP; ICMP