ICMP 攻击技术分析

1. ICMP 协议的概述

对于 TCP/IP 协议我们一定非常熟悉，但是对 ICMP 协议可能不是太了解。ICMP 协议是一个非常重要的协议,它对于网络安全具有极其重要的意义。ICMP 协议本身的特点决定了它非常容易被用于攻击网络上的路由和主机。

1.1. 什么是 ICMP 协议

ICMP 是“Internet Control Message Protocol”(Internet 控制消息协议)的缩写。它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据,但是对于用户数据的传递起着重要的作用。我们在网络中经常会使用到 ICMP 协议,只不过觉察不到而已。比如我们经常用的用于检查网络通不通的 Ping 命令，这个“Ping”的过程实际上就是 ICMP 协议的过程。还有其他的网络命令例如跟踪路由的 Tracert 命令也是基于 ICMP 协议的。

从因特网的角度看，它是由收发数据的主机和中转数据的路由器组成。在通信系统中，IP 协议被用来实现主机之间的数据报传递,而路由器用来连接网络设备。但是,IP 通信过程中总会碰上各种各样的原因导致通信失败,比如:目的地址不正确。IP 协议虽然提供尽力传递的能力,但并不表示数据报一定能够投递到目的地,并且 IP 协议并不负责数据报的丢失、重复、延迟和乱序等情况。因此为了提高 IP 数据报交付成功的机会,反映数据报的投递情况，因特网增加了因特网控制报文协议（ICMP）,来向源发主机告知网络环境中出现的问题。

引进 ICMP 协议之后,当某个网关发现传输错误时，会立即向信源主机发送 ICMP 报文,自动返回有用的描述错误的信息,报告出错情况，信源主机必须将有关的差错交给一个应用程序或采取其他措施来纠正问题。引进 ICMP 协议还可以获得网络通不通、主机是否可达、路由是否可用等网络本身的消息,帮助网络管理员了解网络状况。因此,ICMP 报文虽然并不传输用户数据,但是对于用户数据的传递起着重要的作用。

ICMP 主要是由连接在因特网上的某个结点（一般为路由器）检测到 IP 数据因为某种原因无法继续转发或投递时启动 ICMP 报文的传输,一般 ICMP 消息在以下几种情况下会被发送出来:

(1) 当数据报不能到达目的地时。

(2) 当网亲失去缓存和转发数据报功能时。

(3) 当网关发现并能够引导主机在更短的路由上发送数据报时。

ICMP 协议虽然在实际上使用 IP 作为底层支持,但实际上它是 IP 的一部分,所有系统的 IP 模块必须实现这个协议。ICMP 报文的最终目标不是应用程序或目的用户,而是该机上处理它的 Internet 协议软件模块。也就是说:Inetrnet 控制报文协议允许路由向其它路由器或主机发送差错或控制报文;ICMP 在两台主机的 Internet 协议软件之间提供通信。

1.2. ICMP 的消息格式和代码组合

像其它所有的通信业务一样,ICMP 报文是放在一个 IP 数据报的数据部分中传送的。ICMP 报文要求两级封装,如图 1-1 所示。每个 ICMP 报文放在 IP 数据报的数据部分中通过互联网，而数据报本身放在帧的数据部分中通过物理网络。携带 IMCP 报文的 IP 数据报在传输过程中不具有任何优先级,与正常的 IP 数据

报一样进行转发,唯一不同的是如果携带 ICMP 报文的 IP 数据报在传输过程中出现故障,转发该 IP 数据报的路由将不产生任何关于该差错的报文。

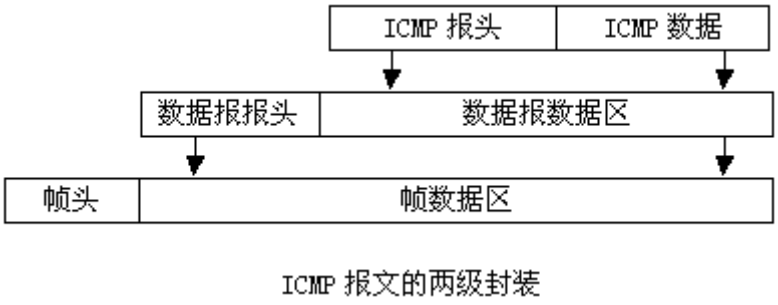


图 1-1 ICMP 保温的两级封装

从上图中可以看出 ICMP 消息格式为 IP 头加上自己的消息包。

简单的说就是:

IP Header + ICMP Message,

ICMP Message=Type（1）+Code（1）+CheckSum（2）+others

每个 ICMP 报文都以相同的 3 个字段开始: 1 个 16 位校验和字段用来识别报文,1 个 8 位的代码（CODE）字段提供有关报文类型的进一步信息, 1 个 16 位验证字段。CODE 域的值在不同的 TYPE 下有不同的解释,而 OTHERS 部分则根据 TYPE 的不同而不同, 所以,数据长度是跟 ICMP 报文的类型有关。此外,报告差错的 ICMP 报文还总是包括产生问题的数据报首部开头的 8 个字节的数据。在差错报告中返回 8 字节用户数据,可以使得接收方能够更精确地判断是哪个应用程序对该数据报负责。

下表列出了部分 ICMP 消息中类型和代码的组合:

表 1-1 ICMP 消息类型和代码组合

类型	代码	描述
0	0	回应应答（Ping,与类型 8 的 Ping 请求一起使用）
3	0~15	目的不可达
4	0	源端被关闭（基本流控制）
5	0~3	重定向
8	0	回应请求(Ping 请求,与类型 0 的 Ping 应答一起使用）
9	0	路由器请求（与类型 10 一起使用）
10	0	路由器请求（与类型 9 一起使用）
11	0~1	超时
12	0~1	参数问题
13	0	时间戳请求（与类型 14 一起使用）
14	0	时间戳应答（与类型 13 一起使用）
17	0	地址掩码请求（与类型 18 一起使用）
18	0	地址掩码应答（与类型 17 一起使用）

1.3. 使用 ICMP 协议搜集信息

ICMP 的使用者主要是路由器，接收者为 IP 数据报的源发主机端,但也可以由主机向一个特定的目的主机发出查询报文。ICMP 协议有一个特点：它是面向无连接的。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。根据这个原理,出现了不少基于 ICMP 的攻击软件,有的制造 ICMP 风暴;有的使用非常大的报文堵塞网络;有的利用 ICMP 碎片攻击消耗服务器 CPU;有的扫描网络,为发动 Dos 攻击搜集信息。

一般黑客在入侵之前，要先对目标主机进行详尽的分析,找出主机可以利用的安全漏洞或弱点,然后乘虚而入。在这里我们利用 ICMP 协议的不同类型可以搜集目标主机的很多信息:

(1) 网络 Ping 扫射,寻找活动主机

获取一个真实网络的最基本步骤之一是在某一个 IP 地址和网络块范围内执行一轮自动 Ping 扫射,以确定某个具体的系统是否存活。Ping 命令,就是向某个目标发送响应请求（Type=8）报文,并期待由此产生表明目标存活的 ICMP 应答（Type=0）报文。一台主机向一个节点发送一个 Type=8 的 ICMP 报文,TCP 协议需要的 ICMP 消息做出响应,如果途中没有异常（如果路由器丢弃、目标不回应 ICMP 或传输失败）,则目标返回 Type=0 的 ICMP 报文,说明这台主机存在。

(2) ICMP 查询

请某个主机或路由回答当前的日期和时间。如果入侵者向目的系统发送时间戳（Type=13）报文,请求返回目的系统的时间,可以获得目标系统所在的时区。从子网掩码服务器得到某个接口的地址掩码。发送地址屏蔽码（Type=17）报文,请求返回设备的子网掩码,据此可以确定将要用到的所有子网。

(3) 利用 ICMP 协议最基本的用途: 报错,来获取目标主机的其他信息根据网络协议,如果按照协议出现了错误,那么接收端将产生一个 ICMP 的错误报文。这个错误报文并不是主动发送的,而是由于错误,根据协议自动产生。当我们设计一些有缺陷的 ICMP 报文发送到目标系统后,目标将发回报告错误的报文。

还有以下的几种情况:

① 向目标主机发送一个只有 IP 头的 IP 数据包,目标将返回 Destination Unreachable 的 ICMP 错误报文。

② 向目标主机发送一个坏 IP 数据报,比如,不正确的 IP 头长度,目标主机将返回 Parameter Problem 的 ICMP 错误报文。

③ 当数据包分片,但却没有给接收端足够的分片,接收端分片装超时会发送分片组装超时的 ICMP 数据报。

④ 向目标主机发送一个 IP 数据报,但是协议是错误的,如协议项不可用,那么目标将返回 Destination Unreachable 的 ICMP 报文。

但是如是在目标主机前有一个防火墙或者一个其他的过滤装置,可能过滤掉信源发出的数据包,从而接收不到任何回应。如果没有 ICMP 数据报返回的错误提示,那么就说明被防火墙或者其他设备过滤了, 我们也可以用这个办法来探测是否有防火墙或者其他过滤设备存在。

1.4. ICMP 攻击及欺骗技术

使用 ICMP 攻击的原理实际上就是通过 Ping 产生大量的数据包使得计算机的 CPU 使用率居高不下而导致崩溃。一般情况下黑客通常在一个时段内连续向计算机发出大量的请求使 CUP 因占用率太高而死机。

基于 ICMP 的攻击可以分为两大类:一是 ICMP 攻击导致拒绝服务(DOS);另外一个是基于重定向(redirect)的路由欺骗技术。

服务拒绝攻击是最容易实施的攻击行为。目前,基于 ICMP 的攻击大部分都可以归类为拒绝服务攻击,其又可以分为以下几类:

(1) 针对带宽的 DoS 攻击

针对带宽的 DoS 攻击,主要是利用无用的数据来耗尽网络带宽。Pingflood、pong、echok、flushot、fraggle 和 bloop 是常用的 ICMP 攻击工具。通过高速度的 ICMP Echo Reply 数据包,目标网络的带宽瞬间就会被耗尽,阻止合法的数据通过网络。ICMP Echo Reply 数据包具有较高的优先级,在一般情况下, 网络总是允许内部主机使用 PING 命令。

这种攻击仅限于攻击网络带宽,单个攻击都就能发起这种攻击。当攻击目标的各项性能指标不高时,如 CPU 速度低,内存小或者网络带宽小,这种攻击效果是明显的。更厉害的攻击形式,可以使整个子网内的主机对目标主机进行攻击,从而扩大 ICMP 流量,形成 Ddos 攻击。使用适当的路由过滤则可以部分防止此类攻击,如果完全防止这种攻击,就需要使用基于状态检测的防火墙。

(2) 针对连接的 DoS 攻击

针对连接的 DoS 攻击,可以终止有的网络连接。针对的网络连接的 IP 设备,因为它使用了合法的 ICMP 消息。Nuke 通过发送一个伪造的 ICMP Destination Unreachable 或者 Redirect 消息来终止合法的网络连接,更具有恶意的攻击。如 puke 和 smack,会给某一个范围内的端口发送大量的数据包,毁掉大量的网络连接,同时还会消耗受害主机 CPU 的时钟周期。

还有一些攻击使用 ICMP Source Quench 消息,导致网络流量变慢,甚至停止。Redirect 和 Router Announcement 消息被利用来强制受害主机使用一个并不存在的路由器,或者把数据包路由到攻击者的机器,进行攻击。针对连接的 DoS 攻击不能通过打补丁的方式加以解决,通过过滤适当的 ICMP 消息类型,一般防火墙可以阻止此类攻击。

2．配置系统带的默认防火墙以预防攻击

虽然很多防火墙可以对 ICMP 数据包进行过滤,但没有安装防火墙的主机,我们可以使用系统自带的防火墙。

配置系统自带的默认防火墙的方法如下(以 WindowsXP 为例):

(1) 打开在电脑的桌面,右键点击:

①开始;
②连接到;
③显示所有连接;
④本地连接;
⑤属性;
⑥Internet 协议(TCP/IP);
⑦属性;
⑧高级;
⑨选项 TCP/IP 筛选;
⑩属性

如下图 2-1 所示:

图 2-1

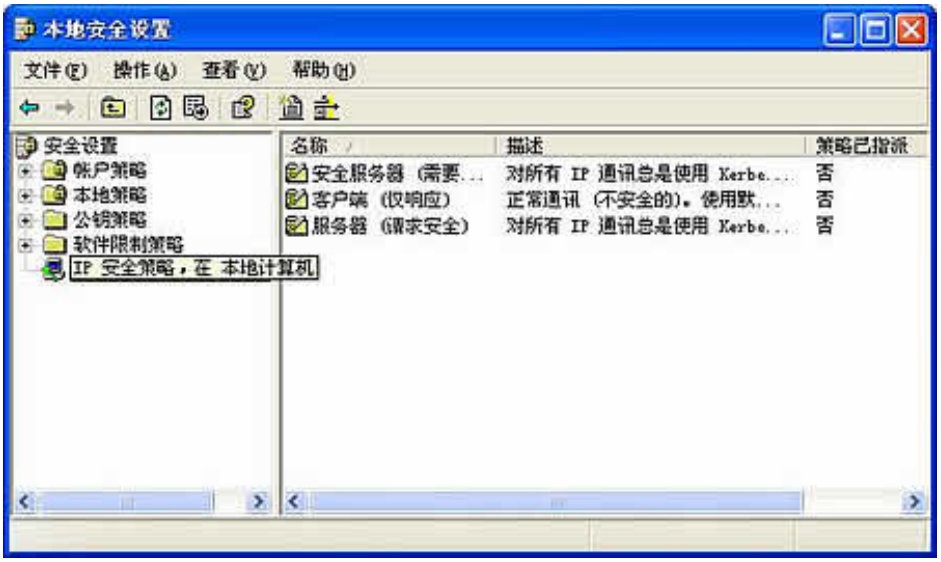
(2) 在“TCP/IP 筛选”窗口中,点击选中“启用 TCP/IP 筛选(所有适配器)”。然后分别在“TCP 端口、UDP 端口和 IP 协议”的添加框上,点击“只允许”,后按添加按钮,然后在跳出的对话框中输入端口,通常用来上网的端口是:80、8080,而邮件服务器的端口是:25、110, FTP 的端口是 20、21,同样将 UDP 端口和 IP 协议相关进行添加。

如图 2-2 所示:

图 2-2 TCP/IP 筛选

(3) 打开“①控制面板;②性能管理;③管理工具;④本地安全策略”,然后右键单击“IP 安全策略,在本地机器”选“管理 IP 筛选器和 IP 筛选器操作”,在“管理 IP 筛选器和 IP 筛选器操作”列表中添加一个新的过滤规则,名称输入“防止 ICMP 攻击”,然后按“添加”按钮,在“寻址”页中设置地址,在源地址选“任何 IP 地址”,目标地址选“我的 IP 地址”,在“协议”页设置协议类型为“ICMP”,设置完毕。

如图 2-3 所示:



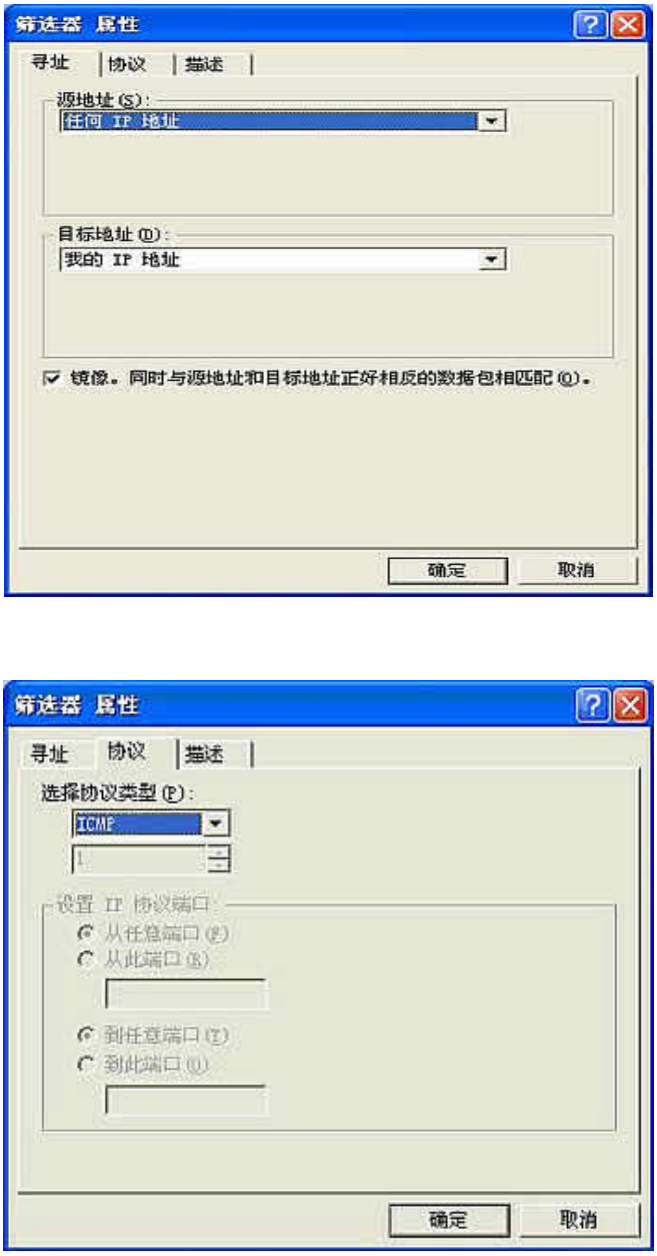


图 2-3 本地安全设置

(4) 在“管理筛选操作”中,取消选中“使用添加向导”,单击“添加”按钮,在“常规”页中输入名称为“Deny 操作”,在“安全措施”页中设置为“阻止”。这样我们就有了一个关注所有进入 ICMP 报文的过滤策略和丢弃所有报文的过滤操作了。

如图 2-4 所示:

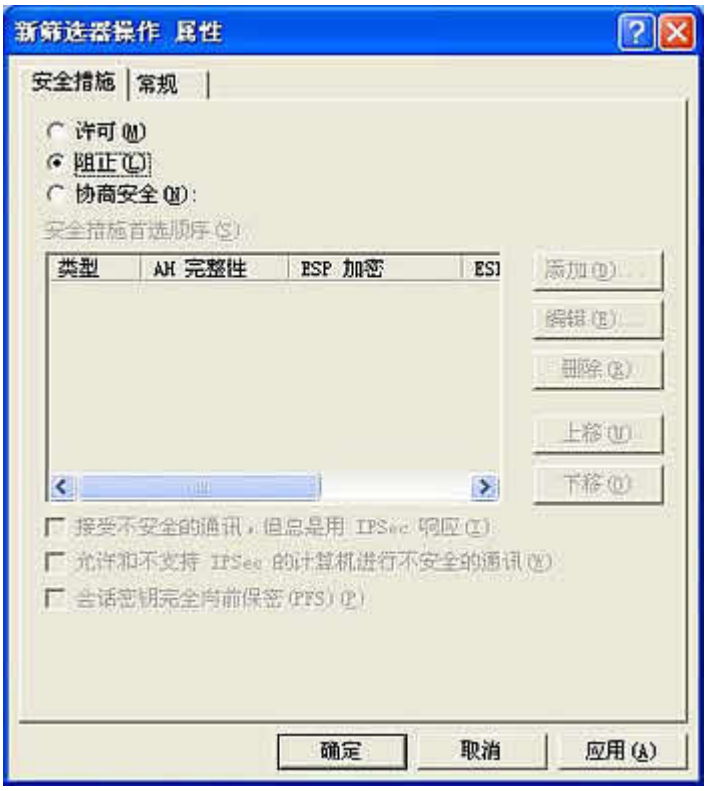


图 2-4 新筛选器操作

(5) 点击“IP 安全策略,在本地机器”,选择

①创建 IP 安全策略;
②下一步;
③输入名称为 ICMP 过滤器

通过增加过滤规则向导,把刚刚定义的 “防止 ICMP 攻击”过滤策略指定给 ICMP 过滤器,然后选择刚刚定义“Deny 的操作”。

如图 2-5 所示:

图 2-5 创建 ICMP 过滤器

（6）最后启用设定好的安全策略,即“指派”策略。

如图 2-6 所示:

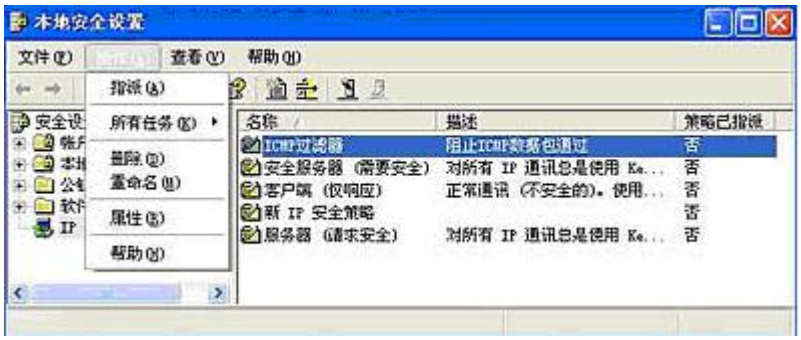


图 2-6 设置指派

经过这样设置后,我们就完成了一个关注所有进入系统的 ICMP 报文的过滤策略和丢弃所有报文的过滤操作,从而有效阻挡了攻击者使用 ICMP 报文进行的攻击。

3. 结论

随着计算机网络技术的发展和人们对 Internet 的依赖性不断增加, DoS 攻击的危害性也在不断加剧。通过网络攻击手段,可以直接攻击大量的联网机器,所以我们对黑客的攻击必须加以重视和防范。不少安全专家都曾指出及早发现系统存在的攻击漏洞、及时安装系统补丁程序,以及不断提升网络安全策略,都是防范 DoS 攻击的有效办法。