传输协议ICMP的安全性解析

江 嘉
(昆明理工大学 计算中心,云南 昆明 650051)

摘要:介绍了Internet传输协议(ICMP)的构成及各部分的具体功能.论述了当前黑客利用ICMP对Internet共享资源进行攻击的机理.为预防和阻止黑客利用ICMP协议对网络进行攻击提供了技术支持,使网络更加安全.实践证明,ICMP的安全性是十分重要的.

关键词:网络;黑客;ICMP;安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1007-855X(2003)01-0102-04

Analysis on the ICMP Security

JIANG-Jia
(Computer Center, Kunming University of Science and Technology, Kunming 650051, China)

Abstract: The compostion and specific function of ICMP are introduced. The mechanism of the hackers attacking Internet by using ICMP is discussed. To stop or prevent the hackers from providing the technological suport to attack the Internet, it is extremely important to ensure the security of ICMP.

Key words: network; hacker; ICMP; security

0 引 言

20世纪90年代以来,计算机网络的发展速度十分迅速,并且应用在各行各业中,给人类的生活和工作带来了极大的方便.在网络给人们带来诸多好处的同时,也带来了不可避免的负面影响,特别是计算机网络遭受黑客(Hacker)攻击,重要信息和数据被窃取,计算机资源遭到严重破坏等,这已经成为社会的一个严重问题.

虽然计算机网络系统从各方面逐渐完善,减少非法者的入侵,但网络系统难免有缺陷或漏洞,这就给黑客留下可乘之机.为了有效地防范网络攻击,维护自己的权益不受侵犯,就需要我们尽量了解网络攻击的各种原理和手段,网络中存在的各种漏洞,以便及时维护系统.本文就传输协议ICMP的原理及存在的漏洞进行了分析,并给出了防范黑客利用ICMP进行攻击的方法和实践经验.

1 ICMP的介绍及原理

ICMP的全名是Internet Control and Message Protocol,这个协议主要是用来进行错误信息和控制信息的传递.它属于TCP/IP协议包中的网络层协议.例如Ping和Tracent工具都是利用ICMP协议中的ECHO Request报文进行的.ICMP报文类型如表1.

表1 ICMP报文类型表

报文类型	描述	报文类型	描述	报文类型	描述	报文类型	描述
0	Echo响应	3	目的地不可达	4	源抑制	5	重定向报文
8	Echo请求	11	超时	12	参数问题	13	时间戳请求
14	时间戳应答	15	信息请求	16	信息应答	17	地址掩码请求
18	地址掩码响应						

ICMP协议有一个特点就是它是无连结的,也就是说只要发送端完成ICMP报文的封装并传递给路由

收稿日期:2002-04-08.
作者简介:江嘉(1966.8~),男,实验师;主要研究方向:网络安全.

器,这个报文就会象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明显的缺陷——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 直接改写报文 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.根据这个原理,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,也有使用非常大的报文堵塞网络的,有利用 ICMP 碎片攻击消耗服务器 CPU 的,甚至将 ICMP 协议用来进行通讯,可以制作出不需要任何 TCP/UDP 端口的木马.

2 ICMP 可能被黑客利用的漏洞和攻击方法

2.1 Type = 0 (Echo reply)

发送者在回应由源地址发送的 Ping,可能是由于以下原因:

(1) 有人在使用 Ping:防火墙后面有人在 Ping 目标;

(2) 自动 Ping:许多程序为了不同目的而使用 Ping,如测试联系对象是否在线或反应时,类似 Vital Sign 的软件,它会发送不同大小的 Ping 包以确定连接速度;

(3) 诱骗 Ping 扫描:有人在利用源 IP 地址进行 Ping 扫描;

(4) 转变通讯信道:很多网络阻挡 Ping(type = 8),但是允许 Ping(type = 0).因此 Hacker 可以利用 Ping 的回应穿透防火墙.例如针对 Internet 站点的 Ddos 攻击,其命令被嵌入 Ping 的回应中,然后洪水般地回应将发向这些站点,而其它的 Internet 连接将被忽略.

2.2 Type = 3 (Destination Unreachable)

在无法到达的包中含有的代码(code)很重要,可以用于击败"SYN 洪水攻击",即如果正在和你通讯的主机受到"SYN 洪水攻击",只要禁止 Ping(type = 3)进入,就无法连接该主机.如果受到来自从未听说过的主机的 Ping(type = 3)包,通常意味着"诱骗扫描".攻击者使用很多源地址向目标发送伪造的包,其中有一个是真正的地址.黑客的理论是:受害者不会费大的力量从许多假地址中搜寻真正的地址.解决这个问题的最好办法是:检查你看到的模式是否与"诱骗扫描"一致.比如在 ICMP 包中的 TCP 或 UDP 头部分寻找交互的端口.

2.2.1 Type = 3, code = 0 (Destination Net Unreachable)

无路由器或主机:即一个路由器对主机或客户说:"我根本不知道在网络中如何路由! 包括正连接的主机".这意味着不是客户选错了 IP 地址,就是某处的路由表配置错误.

2.2.2 Type = 3, code = 3 (Destination Port Unreachable)

这是当客户端试图连接一个并不存在的 UDP 端口时,服务器所发送的包.例如:如果你向 161 端口发送 SNMP 包,但机器并不支持 SNMP 服务,你就会收到 ICMP Destination Port Unreachable 包.为什么会发生这一情况呢? 原因在于:

(1) 诱骗 UDP 扫描:有人在扫描向你发送 ICMP 的机器.他们伪造源地址,其中之一是你的 IP 地址.他们实际上伪造了许多不同的源地址使受害者无法确定谁是攻击者.如果你在短时间内收到大量来自同一地址的这种包,很有可能是上述情况.检查 UDP 源端口,它总在变化的话,很可能是 Scenario.

"陈旧 DNS": 客户端会向服务器发送 DNS 请求,这将花很长时间解析.当你的 DNS 服务器回应时,客户端可能已经忘记并关闭了用于接受回应的 UDP 端口.如果发现 UDP 端口值是 53,就发生了这种情况.服务器可能在解析一个递归请求,但是它自己的包丢失了.所以它只能超时,然后再试.当回到客户时,客户认为超时了.许多客户程序自己做 DNS 解析.即自己建立 SOCKET 进行 DNS 解析.如果把要求交给操作系统, 端口就会一直处于打开状态.

(2) 多重 DNS 回应:另一种情况是客户收到对于一个请求的多重回应.收到第一个回应,端口就关闭了,后序的回应无法达到.一个编写得很糟糕的客户端程序,有时发送多重请求,收到第一个回应后就关闭了 Socket.但是,这也可能是 DNS 欺骗,攻击者发送请求又发送回应,企图使解析缓存崩溃.

(3) NetBIOS 解析:如果 Windows 机器接收到 ICMP 包,看看 UDP 目标端口是否是 137.如果是,那就是 Windows 机器企图执行 gethostbyaddr()函数,它将会同时使用 DNS 和 NetBIOS 解析 IP 地址.DNS 请求

被发送到某处的DNS服务器,但NetBIOS直接发往目标机器,如果目标机器不支持NetBIOS,目标机器将发送ICMP unreachable.

(4) TRACEROUTE:大多数Traceroute程序向关闭的端口发送UDP包.这就引起一系列的ICMP Port Unreachable包发回来.因此你看到防火墙显示这样ICMP包,可能是防火墙后面的人在运行Traceroute,你也会看到TTL增加.

2.2.3 Type=3,Code=4 (Fragmention Needed AND don't Fragment was Set)

这是由于路由器打算发送标记有DF(不允许片断)的IP报文引起的.IP和TCP都将报文分成片断.TCP在管理片断方面比IP有效得多.因此,栈堆趋向于找到"Path MTU".在这个过程中将发送这种ICMP包.

2.3 Type=4 (Source Quench)

这种包可能是当网络通讯超过极限时,有的路由器或目的主机发送的,但是许多系统不生成这些包.原因是现在简单包丢失是网络阻塞的最后信号.现在Source Quenches的规则是(RFC 1122):

(1) 路由器不许生成包;

(2) 主机可以生成包;

(3) 主机不能随便生成包;

(4) 防火墙应该丢弃包;

但是,主机遇到Source Quench仍然减慢通讯,因此这被用于Ddos攻击.防火墙应该过滤它们.如果怀疑发生Ddos攻击,包中的源地址是毫无意义的,因为IP地址肯定是虚构的.

2.4 Type=8(Echo Ping)

这是Ping请求包.有很多场合使用.它可能意味着某人恶意扫描你的机器,但它也可能是正常网络功能的一部分.很多网络管理扫描器会生成特定的Ping包.包括IIS扫描器,WhatsUP监视器等.这在扫描器的有效载荷中可以看见.许多防火墙并不记录这些,因此你需要一些嗅探器捕捉它们或使用入侵检测系统(IDS)来标记它们.但是阻挡Ping进入并不意味着黑客不能扫描你的网络.有许多方法可以代替.例如:TCP ACK扫描越来越流行.它们通常能穿透防火墙而引起目标系统不正常的反应.发送到广播地址的Ping可能在你的网络中用于smurf放大.

2.5 Type=11(Time Exceeded In Transit)

2.5.1 Type=11,Code=0 (TTL Exceeded In Transit)

这可能由许多事情引起.如果有人从你的站点traceroute到Internet,你会看到许多来自路由器TTL增加的包.这就是traceroute的工作原理:强迫路由器生成TTL的信息来发现路由器.

防火墙管理员看到这种情况的原因是Internet上发生路由循环.路由器Flapping是一个常见的问题,常会导致循环.这意味着当一个IP包朝目的地前进时,这个包被一个路由器错误引导至一个它曾经通过的路由器.如果路由器在包经过的时候把TTL值减1,这个包只好循环运动.直至当TTL值为0时它被丢弃.

造成这种情况的另一个原因是距离.许多机器的默认TTL值是127或更低.路由器也常常将TTL值减去大于1的值,诸如电话拨号或跨洋连接的慢速连接.因此,可能由于初始TTL值的大小,而使站点无法到达.此外,一些黑客也会使用这种办法使站点无法到达.

2.5.2 Type=11,Code=1 (Ftagment Reassembly Time Exceeded)

当发送分割成片断的IP报文时,而发送者并不接收片断.通常,大多数TCP/IP通讯甚至不分割片断,这种情况必定是采用了分割片断而且你和目的地之间有阻塞.

2.6 Type=12 (Parameter Problem)

有许多脚印技术会生成这种包.

(下转第111页)

$$B = (0.8354 \quad 0.81 \quad 0.8474 \quad 0.8583)$$

根据最大隶属原则知 4 个支护方案的优劣顺序为:D > C > A > B 故优选 D 方案.

4 结束语

从上面的分析可知:两种决策方法对深基坑支护方案评价,具有方法简单、概念清晰、结果可靠等特点.

参考文献:

[1] 邓聚龙.灰色系统基本方法[M].武汉:华中理工大学出版社,1987.19~30.
[2] 邓聚龙.灰色控制系统·第二版[M].武汉:华中理工大学出版社,1993.315.
[3] 谢季坚,刘承平.模糊数学方法及其应用·第二版[M].武汉:华中理工大学出版杜,1999.190~199.
[4] 冯玉国.深基坑支护方案评价灰色优化理论模型与应用[J].岩土工程师,1999,11(1).
[5] 黄运飞.深基坑工程实用技术[M].兵器工业出版社,1996.

(上接第 104 页)

3 应用实例及解决方法

著名的"死亡之 Ping"攻击是属于拒绝服务攻击的一种.它就是通过向目标端口发送大量的超大尺寸的 ICMP 包来实现的.当目标收到这些 ICMP 碎片包后,会在缓冲区里重新组合它们,由于这些包的尺寸实在太大以致于造成缓冲区溢出,从而导致系统崩溃.解决的方法很简单,Windows 2000 自带一个 ROUTING & REMOTE ACCESS 工具,在这个工具中可以轻易的定义输入输出包过滤器,我们设定输入 ICMP 代码 255 丢弃就表示丢弃所有的外来的 ICMP 包.这样就可以阻止"死亡之 Ping"的攻击.

4 结束语

以上的论述和实例证明,计算机网络有其脆弱的一面,而以上所述只是许多种黑客攻击中的一种.笔者建议:

(1) 建议慎重选择第三方程序.应该尽量选择有信用的大公司的软件,绝对不要选择公布源代码的应用程序,因为这种程序的漏洞很容易被发现;

(2) 要经常注意国际安全网站公布的漏洞,并根据建议进行修补.这一点对于安全来讲是至关重要的,因为网络上绝大多数的攻击都是利用已知的漏洞进行的;

(3) 要认识到 CGI 安全问题的至关重要性.只有加强安全意识,通过不断研究网络系统的安全漏洞并弥补它,才能保证网络的安全使用.

参考文献:

[1] www.rootshell.com[OL].
[2] www.esecurityonline.com[OL].
[3] www.starkun.com[OL].
[4] [美]Robert Cowart Brian Knittel. Windows2000 Professional 中文版使用大全 [M].北京:人民邮电出版社,2001.703-733,1079~1100.
[5] 赵斌斌.网络安全与黑客工具防范[M].北京:科技出版社,2001.7~13,19~116,241~256.
[6] 董玉格,等.攻击与防护-网络安全与实用防护技术[M].北京:人民邮电出版社,2002.7~22,79~99,155~182.
[7] [美]匿名.网络安全技术内幕[M] .北京:机械工业出版社,1999.27~39,197~205,345~380.
[8] 阎雪.黑客就这么几招[M].万方数据电子出版社,2000.19~23,88~127,184~214.