第 34 卷 第 2 期 计 算 机 工 程 2008 年 1 月
Vol.34 No.2 Computer Engineering January 2008
·安全技术· 文章编号：1000—3428(2008)02—0103—02 文献标识码：A 中图分类号：TP393.08

ARP 欺骗及 ICMP 重定向攻击技术研究

杨 杨，房 超，刘 辉
（重庆邮电大学通信与信息工程学院，重庆 400065）

摘 要：ARP欺骗及ICMP重定向攻击是以太网中常用的攻击手段，两者都可达到监听网络或对目标主机进行拒绝服务攻击的效果。该文通过分析两者在实现方式、适用范围方面的不同，得出实施ICMP重定向攻击难度更大的结论。根据IP路由原理，反驳了可以跨网段实施ARP欺骗的观点，指出其无法实现的根本原因在于忽略了目标主机要对接收到的ICMP重定向报文进行详细检查，这种攻击手段实际上很难奏效。

关键词：ARP 欺骗；监听；拒绝服务；ICMP 重定向；IP 路由

Research on Technology of ARP Spoofing and ICMP Redirection Attak

YANG Yang, FANG Chao, LIU Hui
(College of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065)

【Abstract】 ARP spoofing and ICMP redirection attack are used frequently, both of them can sniff the Ethernet or attack the target by means of denial of service. Through analyzing the difference of measure and applicable scope between them, a conclusion is made that ICMP redirection attack is more difficult to come true. In terms of mechanism of IP routing, the theory thal ARP spoofing spans the same subnet actually does not realize and the reason is that the target will examine received ICMP redirection message, so this measure is not successful in practice.

【Key words】 ARP spoofing; sniffing; denial of service; ICMP redirection; IP routing

随着互联网的广泛应用，内部网络的安全问题逐渐成为人们关注的焦点。在频繁发生的攻击行为中，利用 TCP/IP 协议的漏洞进行攻击是主要的手段之一。地址解析协议(Address Resolution Protocol, ARP)是局域网中解决 IP 地址到硬件地址映射的协议，攻击者利用 ARP 协议的无连接、无认证的特性很容易实现 ARP 欺骗。另外，路由器用来指示主机重定向路由的 ICMP 重定向协议也成为攻击者的利器，攻击者可冒充路由器，使目标主机将报文转发到攻击者的机器上，达到与 ARP 欺骗类似的效果。

1 ARP 欺骗

在实际网络的链路上传送数据帧时，是采用硬件地址来寻址，地址解析协议解决了从IP地址到硬件地址的映射问题[1]。比如，源主机欲向本网内的主机发送数据包时，先在源主机的ARP高速缓存中查看有无目的主机的硬件地址，如存在，就将目的主机的硬件地址写入MAC帧并发送，如不存在，源主机自动在网内广播一个ARP请求报文来获得目的主机的硬件地址。网内的所有主机都收到此ARP请求，只有目的主机才会发回一个ARP响应报文，并写入自己的硬件地址。当源主机收到目的主机的ARP响应后，就在其ARP高速缓存中写入目的主机的IP地址到硬件地址的映射。

传统的共享式以太网是由集线器进行网络互联，而集线器属于物理层设备，采用广播技术将一个端口接收到的报文广播到本网内的所有机器上，目的主机会接收此报文，而非目的主机则丢弃该报文。但是，如果将网卡设为混杂模式，则非目的主机也可以接收此报文。

交换式以太网络是采用属于数据链路层设备的 2 层交换机进行网络互联，通过读取数据包中的目的MAC地址并查找相应的端口进行转发，如果找不到相应的端口，则把数据包广播到所有端口上，当目的机器回应时交换机就可以学习目的MAC地址与哪个端口对应，这就是交换机的“学习”功能，再次转发数据时就有了依据[2]。

基于 2 层交换机的特点，即使将网卡设为混杂模式，也只能捕获目的 MAC 地址为本机地址的数据包，共享式以太网中的监听手段失效。但是，由于 ARP 协议的无连接、无认证，局域网中的任何主机可随意发送 ARP 请求包，也可以接收 ARP 应答包，并且无条件地根据应答包内的内容刷新本机的 ARP 缓存，因此，ARP 欺骗也可应用于交换式以太网络中。

ARP 欺骗主要达到 2 种攻击效果：

(1)攻击者可在 2 台正在通信的主机 A,B 之间充当中间人(man-in-the-middle)，假冒主机 B 的 IP 地址，而 MAC 地址为攻击者的 MAC 地址来欺骗主机 A 将数据发往攻击者的机器，并且攻击者可开启 IP 路由功能，将数据包再转发至主机 B。同样，对主机 B 可实施类似的欺骗，因此，主机 A,B 之间的所有通信内容都被攻击者窃听。

(2)对主机 A 发送伪造的 ARP 应答报文，假冒主机 B 的 IP 地址，但 MAC 地址设为不存在的一个硬件地址，主机 A 接收此报文后错误地刷新 ARP 高速缓存中主机 B 的 IP 地址与 MAC 地址的映射关系，导致主机 A 与主机 B 的网络通信中断。这种方法属于拒绝服务(Denial of Service, DoS)攻击，

作者简介：杨 杨(1981－)，女，硕士，主研方向：现代通信新技术；房 超，硕士；刘 辉，高级工程师
收稿日期：2007-02-05 **E-mail：**echo_mozhiyan@hotmail.com

网络上流行的网络执法官等软件就是采用 ARP 欺骗机制，发送错误的网关 MAC 地址给非法用户，使其通信中断。

针对 ARP 欺骗，解决办法有很多，例如主机与交换机双向的 MAC 地址绑定，或对数据进行加密处理，以及建立 DHCP 服务器等，而且某些交换机每隔一段时间就会自动向全网播放 ARP 应答，这些措施都可以在一定程度上防止 ARP 欺骗。但是攻击者也可以增强伪 ARP 应答报文的发送频率，使主机的 ARP 缓存即使接收到正确网关的 ARP 应答却又很快被伪造的 ARP 应答所充斥，依旧无法联系到网关。

2 ICMP 重定向攻击

ICMP重定向报文是当主机采用非最优路由发送数据报时，路由器会发回ICMP重定向报文来通知主机最优路由的存在[3]。并且重定向报文必须由路由器生成，当主机作为路由器使用时，必须将其内核配置成可以发送重定向报文。

ICMP 重定向攻击也可以达到类似 ARP 欺骗的攻击效果。假设主机 A(IP 地址为 172.16.1.2)经默认路由器(IP 地址为 172.16.1.1)与另一个网络中的主机 D(IP 地址为 172.16.2.2)通信，与主机 A 同属一个网络的攻击者(IP 地址为 172.16.1.4)，通过修改内核设置，充当与主机 A 直接相连的路由器。攻击者要想监听主机 A 的通信内容，可以构造如图 1 所示的 ICMP 重定向报文，指示主机 A 将数据包转发到攻击者的机器上，攻击者对所有的数据进行过滤后再转发给默认路由器，这就是“中间人”攻击。同样，ICMP 重定向攻击也可以达到拒绝服务(DoS)攻击的目的。

<table>
<tr><td>VER</td><td>HLEN</td><td>Service Type</td><td colspan="2">P ACKET_LEN</td></tr>
<tr><td colspan="3">Identification</td><td>Flag</td><td>Fragmentation offset</td></tr>
<tr><td>Time to live</td><td colspan="2">Protocol (ICMP)</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source IP address (1 72.16.1.1)</td></tr>
<tr><td colspan="5">Destination IP address (172.16.1.2)</td></tr>
<tr><td colspan="5">Option</td></tr>
<tr><td>Type (5)</td><td colspan="2">Code (1)</td><td colspan="2">Checksum</td></tr>
<tr><td colspan="5">IP address of the target router (172.16.1.4)</td></tr>
<tr><td>VER</td><td>HLEN</td><td>Service Type</td><td colspan="2">PACKET_LEN</td></tr>
<tr><td colspan="3">Identification</td><td>Flag</td><td>Fragmentation offset</td></tr>
<tr><td>Time to live</td><td colspan="2">Protocol (IP)</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source IP address (172.16.1.2)</td></tr>
<tr><td colspan="5">Destination IP address (172.16.2.2)</td></tr>
<tr><td colspan="5">Option</td></tr>
<tr><td colspan="5">8 bytes of data</td></tr>
</table>

图 1 ICMP 重定向报文

在实际应用中，无论 ARP 欺骗抑或是 ICMP 重定向攻击，都有可能出现攻击者的机器自动发送 ICMP 重定向报文给目标主机的情况。这种自动生成的 ICMP 重定向报文与攻击者发送的伪 ICMP 重定向报文有所不同，其原理是同一网段内的攻击者为监听网络而开启了 IP 路由功能，对数据包过滤后转发给默认路由器，默认路由器再转发数据包至主机 D。但由于 IP 寻址的原理，攻击者的机器(在此充当路由器)会发现下一跳路由器(即默认路由器)与源主机处在同一子网中，即有一条更优路由的存在，此时攻击者的机器会自动发送 ICMP 重定向报文来指示主机 A 通往网外的主机 D(172.16.2.2)的最优路由是经由默认路由器而不是经由攻击者的机器，结果是使 ARP 欺骗或 ICMP 重定向攻击失败。对 ARP 欺骗来说，可以通过个人防火墙等手段限制有关 ICMP 报文的出包，但对 ICMP 重定向攻击来说，限制 ICMP 报文的出包后也就意味着攻击者也无法发送伪造的 ICMP 重定向报文给目标主机，实现起来更为复杂。

3 ARP 欺骗＋ICMP 重定向

不同于局域网内的ARP欺骗，跨网段的ARP欺骗一直是技术难点。有些学者提出可用“ARP欺骗＋ICMP重定向”解决[4]。比如，假设网络 1 与网络 2 经一个路由器相联，在网络 1 内的两台主机A和B正在通信，网络 2 内的攻击者实施ARP欺骗。

在“ARP 欺骗＋ICMP 重定向”这种观点中，攻击者可先寻找 B 的漏洞当掉 B，然后发送给 A 虚假的 ARP 应答报文来冒充 B 的 IP 地址，而硬件地址是攻击者的本机 MAC 地址。但由于主机 A 只会在网络 1 内寻找主机 B，根本不会把数据包发送给路由器，因此攻击者还要构造一个 ICMP 重定向报文，告诉主机 A“到主机 B 的最短路径是经过路由器。主机 A 需要重新定向路由，将所有发往 B 的数据包都交给路由器转发”，攻击者可在网外接收到来自网内的 IP 包。

这种理论成立的关键是主机 A 接收了伪造的 ICMP 重定向报文，但实际上，主机 A 不会无条件地接收 ICMP 报文。在通常情况下，为防止路由器和主机的误操作或者某些恶意用户的破坏，主机在更改本机路由表之前要做一些检查，以免错误修改本地路由表。

在 4.4BSD 系统中，主机要进行下列检查：

(1)新的路由器必须与网络直接相联。

(2)重定向报文必须来自当前到目的网络所选择的路由器。

(3)重定向报文不能让主机本身作为路由器。

(4)被修改的路由必须是一个间接路由。

在Windows Server 2003 系统中，也有类似的规定以防止主机接收到ICMP重定向报文后错误的修改路由表[5]。比如主机收到ICMP重定向消息后，首先检查ICMP消息的源IP地址，以确认发送ICMP消息的路由器就是原IP路由表中去往目的地址路由的网关，并要确认ICMP重定向消息的源IP地址是直接可达路由器发出的，若不是则该消息被忽略。依据ICMP重定向消息新建的主机路径在路由表中只保留 10 min，10 min后再次进行ICMP重定向。

根据 TCP/IP 协议的规定，被 ICMP 重定向报文修改的路由必须是一个间接路由。间接路由是指源计算机和目的计算机不在同一网络中，中间经过路由器相联。然而，主机 A 与 B 在同一子网内，它们之间的路由不是间接路由，而是直接路由。

根据 IP 路由机制，当主机 A 向任一主机发送分组时，首先将分组的目的地址和主机 A 的子网掩码进行逐比特相“与”的运算。若运算的结果等于主机 A 的网络地址，则说明目的主机与 A 是连接在同一个子网上，可以直接将此分组发送给目的主机。若“与”运算的结果不等于主机 A 的网络地址，则应将分组交给本子网上的一个路由器进行转发。

如上所述，主机 A 不可能接收 ICMP 重定向报文，它只会将分组直接发给主机 B 而不会发给路由器，攻击者也就不可能在网外通过路由器截获主机 A 的分组，跨网段 ARP 欺骗一般也就无法实现。

4 结束语

在日常生活中，人们通常用以太网来连接彼此的主机，局域网内的信息安全时刻提醒防范黑客的攻击。网络安全的攻击与反攻击，一向是此消彼长的过程，网络管理员应该认真分析每种攻击的特点，加强安全防范意识，保护系统安全。

(下转第 107 页)