文章编号:1005－0523(2007)05－0139－03

如何预防和处理 ARP 地址欺骗和攻击

章海亮

(华东交通大学 机电工程学院,江西 南昌 330013)

摘要:描述了基于 ARP 地址欺骗和攻击的特点和原理,阐述了如何预防 ARP 地址欺骗和攻击的方法以及如何处理已经受到感染 ARP 病毒的计算机,论文最后介绍了采用网关 MAC 地址绑定的方法,保证发送的文件每次都能经过正确的网关.实验结果表明论文介绍的方法能有效拦截 ARP 攻击.

关 键 词:ARP 欺骗;预防;绑定;网关 MAC 地址

中图分类号:TP393.08　　**文献标识码**:A

1 概述

在局域网中,通信前必须通过 ARP 协议来完成 IP 地址转换为第二层物理地址,即 MAC 地址.ARP 协议对网络安全具有重要的意义.通过伪造 IP 地址实现 ARP 欺骗,对网络的正常传输和安全都是一个很严峻的考验.

“怎么老是掉线!!”每当听到同学们的抱怨声一片响起,网络管理员就坐立不安,如果此时给机房断电一分钟后再通电的话,上网又恢复正常.其实,此起彼伏的瞬间掉线或大面积的断网现象大都是 ARP 欺骗在作怪.如果用户发现上网时断时续的情况,可以通过如下操作进行判断是否是 ARP 欺骗在作怪:点击“开始”按钮－>选择“运行”－>输入“arp－d”－>点击“确定”按钮,然后重新尝试上网,如果能恢复正常,则说明此次掉线可能是受 ARP 欺骗所致.“arp－d”命令用于清除并重建本机 arp 表.“arp－d”命令并不能抵御 ARP 欺骗,执行后仍有可能再次遭受 ARP 攻击.

2 ARP 地址欺骗和攻击原理

要理解因 ARP 地址欺骗而不能上网的故障原理,我们先来了解一下 ARP 协议.ARP 协议是“Address Resolution Protocol”(地址解析协议)的缩写.在局域网中,网络中实际传输的是“帧”,帧里面是有目标主机的 MAC 地址的.在以太网中,一个主机要和另一个主机进行直接通信,必须要知道目标主机的 MAC 地址.但这个目标 MAC 地址是如何获得的呢?它就是通过地址解析协议获得的.所谓“地址解析”就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程.ARP 协议的基本功能就是通过目标设备的 IP 地址,查询目标设备的 MAC 地址,以保证通信的顺利进行.

每台安装有 TCP/IP 协议的电脑里都有一个 ARP 缓存表,表里的 IP 地址与 MAC 地址是一一对应的,比如有计算机 A、B、C,它们的 IP 地址和 MAC 地址分别如下:

A 172.16.26.215 aa－aa－aa－aa－aa－aa

B 172.16.26.254 bb－bb－bb－bb－bb－bb

C 172.16.26.139 cc－cc－cc－cc－cc－cc

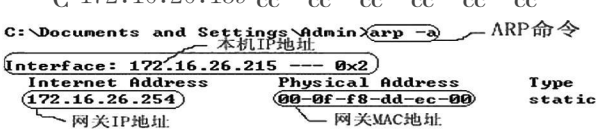

图 1 网关 IP 地址和 MAC 地址

局域内计算机上网都是通过网关发送数据的,

收稿日期:2007－06－10

作者简介:章海亮(1977－),男,南昌人,华东交通大学讲师.

本文中所述实验环境网关IP地址是172.16.26.254.查询网关IP地址和MAC地址用命令arp－a.具体为开始－＞运行,输入cmd,切入到DOS命令环境下,再输入命令arp－a.如图1所示:

现在我们以主机A(172.16.26.215)向主机B(172.16.26.254)也即网关发送数据为例.当发送数据时,主机A会在自己的ARP缓存表中寻找是否有目标IP地址.如果找到了,也就知道了目标MAC地址,直接把目标MAC地址写入帧里面发送就可以了;如果在ARP缓存表中没有找到相对应的IP地址,主机A就会在网络上发送一个广播,向同一网段内的所有主机发出这样的询问:"172.16.26.254的MAC地址是什么?"网络上其他主机并不响应ARP询问,只有主机B接收到这个帧时,才向主机A做出这样的回应:"172.16.26.254的MAC地址是bb－bb－bb－bb－bb－bb".这样,主机A就知道了主机B的MAC地址,它就可以向主机B发送信息了.同时它还更新了自己的ARP缓存表,下次再向主机B发送信息时,直接从ARP缓存表里查找就可以了.ARP缓存表采用了老化机制,在一段时间内如果表中的某一行没有使用,就会被删除,这样可以大大减少ARP缓存表的长度,加快查询速度.

从上面可以看出,ARP协议的基础就是信任局域网内所有的人,那么就很容易实现基于以太网上的计算机进行ARP地址欺骗.比如计算机C对目标计算机A进行欺骗,A发送数据到地址bb－bb－bb－bb－bb－bb却发送到了cc－cc－cc－cc－cc－cc这个地址上.那么是怎么实现欺骗的呢?计算机C进行欺骗的时候,把它自己的IP地址伪装为172.16.26.254,于是A发送到B上的数据包都变成发送给C的了.表现为A和B连接不上了.此时计算机B的MAC地址bb－bb－bb－bb－bb－bb为网段内的网关,最终结果是A主机上不了网.如果计算机C对局域网段内所有主机都进行ARP地址欺骗的话,就出现了一台主机中毒,局域网内所有主机都上不去网的情况,危害相当大,因为一般情况下一台主机中毒大不了本机A不能上网,如果局域网内所有主机都不能上网的话,这对网络经营者来说损失是相当大的.

3 预防和处理ARP地址欺骗和攻击

那么出现了局域网内大面积断网的话,应做如下处理,对于中毒的计算机:使用ARP病毒专杀工具查杀ARP病毒,http://www.ctbu.edu.cn/temp/TSC.rar下载后解压缩,运行包内TSC.exe文件,不要关让它一直运行完,最后查看report文档便知是否中毒.

对于被攻击的计算机:使用AntiArp防火墙软件抵御ARP攻击,我们可以从网站下载http://download.antiarp.com/tmp/antiarp4.1.1.exe,运行antiarp4.1.1.exe,安装完成后,双击桌面图标AntiARP,如下图2所示:

图2 ARP统计数据和攻击统计

从图2左上角可以知道网关IP和MAC地址,如果受到ARP攻击,会提示攻击被拦截,抓包多少,AntiArp防火墙软件功能非常强大,它不但能够拦截其它计算机发送到本机的ARP攻击,如果本机中了ARP病毒,AntiArp防火墙软件还能拦截本机向网内其它计算机发送的ARP攻击,这就很大程度上解决了一台计算机中毒,局域网内所有的计算机都不能上网的问题.AntiArp防火墙软件会在提示框内出现病毒主机的IP地址和MAC地址,如下图3所示:

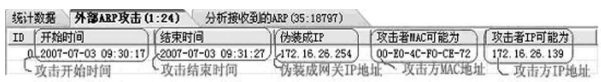

图3 分析接收到的ARP攻击

从图3第一行ID为0知道,某计算机IP地址为172.16.26.139,其MAC地址为00－E0－4C－F0－CE－72,它的IP地址伪装为172.16.26.254,那么我们就可以判断这台计算机中了ARP病毒,因为这个IP地址是网关的IP地址,这台计算机随时都有可能对局域网内其它计算机发起ARP地址攻击,导致局域网内其它计算机上不了网.从图3我们还可以看出攻击开始时间和攻击结束时间,这是ARP攻击的特点,隔一段时间发送一次攻击,对计算机用户来说表现就是一会儿能上网,一会儿又不能上网.AntiArp防火墙软件只能防止ARP攻击,但却不能查杀ARP病毒,它能找到中了ARP病毒的计算机的IP地址,这对于我们进一步处理奠定了良好的基础,那么对于找到已感染ARP病毒的计算机,就应立即进行杀毒处理或者重装系统.

4　静态绑定 IP 地址和网关的 MAC 地址

还有一种处理 ARP 攻击的方法就是绑定计算机用户的 IP 地址与网关的 MAC 地址,使得计算机发送和接收的数据每次都经过正确的网关,绑定后 ARP 攻击不能够改变已经绑定好的路径,绑定网内计算机 IP 与网关的 MAC 地址的方法使用命令 arp －s,比如要绑定计算机用户 IP 地址为 172.16.26.215 与网关 MAC 地址,应为 arp －s 172.16.26.215　00－0F－F8－DD－EC－00,这样这个条目就变成静态 ARP 条目永远不会失效,如下图 4 所示:

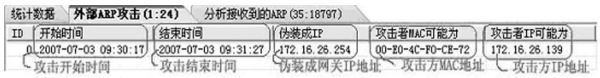

图 4　ARP 地址绑定

这样绑定的好处就是可以防止 ARP 病毒攻击.不过值得注意的是:这里绑定过后的条目在重启计算机后将失效,如何使其能每次重启后都有这样的绑定呢? 我们可以新建一个记事本文件,把它保存为批处理文件如 arp.bat,注意后缀名为 bat.编辑它,在里面加入我们刚才的命令,保存就可以了,以后可以通过双击它来执行这条命令,还可以把它放置到系统的启动目录下来实现启动时自己执行.打开电脑"开始"－>"程序",双击"启动"打开启动的文件夹目录,把刚才建立的 arp.bat 复制到里面去:

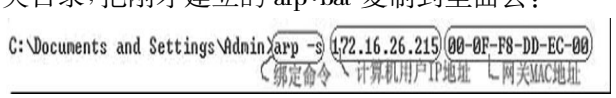

图 5　开机启动 ARP 地址绑定

好了,以后计算机每次启动时就会自己执行 arp －s 命令了.

5　结论和小结

实验结果证明,采用安装 ARP 防火墙和静态绑定 IP 地址和网关的 MAC 地址能有效预防 ARP 地址欺骗和攻击.对于已经发现中了 ARP 病毒的主机,可以采用杀毒软件杀毒或重装操作系统的办法.最后要强调的就是要想防止计算机中 ARP 毒,还要做到以下几点:一是更新杀毒软件病毒库,以便能查杀最新出现的 ARP 病毒;二是要养成良好的上网习惯,不要登陆不健康的网站,不要打开不清楚来历的邮件,很多病毒和木马都是通过邮件传播的;三是安装最新的布丁,安装一个布丁意味着少了一个或几个漏洞,减少了被攻击的可能性.

参考文献:

[1] 蔡立军.计算机网络安全技术[M].北京:中国水利水电出版社,2005,7:87～98.
[2] 梁亚声,汪永益.计算机网络安全技术教程[M].北京:机械工业出版社,2004.
[3] 谢希仁.计算机网络[M].北京:电子工业出版社,2003.
[4] 章海亮.构建安全 web 服务器探析[J].华东交通大学学报,2005,(4):65～68.
[5] 北京启明星辰信息技术有限公司.网络信息安全技术基础[M].北京:电子工业出版社,2002.
[6] Tony Kenyon.Routing, Seurity, and Performance Optimization [M].Publisher:Digital Press;1st edition 2002.

How to Defend and Deal with ARP Address Cheat and Attack

ZHANG Hai-Liang

(East China Jiaotong University, Nanchang 330013, China)

Abstract: This paper describes the characters and theory of cheat and attack based on ARP address, and presents how to defend cheat and attack based on ARP address, and how to deal with the computer that is infected with ARP virus. The paper finally introduces the way of banding gateway MAC address which can assure the file would be sent to the correct gateway. The experiment results show that the way described in the paper can defend ARP attack.

Key words: ARP cheat; defend; banding; gateway MAC address