基于 ARP 欺骗的中间人攻击与防范技术研究

吴 涛 唐宾徽

四川大学锦城学院 计算机与软件学院 四川 成都 611731

【摘 要】ARP 欺骗的中间人攻击是近些年来出现的一种较为常见的网络攻击方式，ARP 欺骗攻击也是一种常见的内网攻击方式，在广泛的计算机网络安全问题中备受瞩目。而传统的网络安全防御技术已经不适用于 ARP 的欺骗攻击。随着网络安全系统中的配置和功能不断完善，难免会存在一些技术故障和系统漏洞问题。对此，如何有效的解决 ARP 的欺骗攻击是当下急需研究的问题。ARP 欺骗攻击已经成为网络安全领域研究的热点问题，为了保证计算网络安全系统通信安全和数据安全，本文在分析 ARP 基本原理的基础上，利用一些工具实现了 ARP 欺骗与中间人攻击（man-in-the-middle attack）的一个过程。并提出 ARP 欺骗在被攻击的过程中提出相应的防范措施。

【关键词】ARP 欺骗；中间人攻击；网络安全

1 中间人攻击的相关理论

1.1ARP 协议简介

ARP 是 Address Resolution Protocol 的缩写，中文翻译为地址解析协议，唯一 OSI 参考模中的第二层协议（数据链路层）。工作原理是将主机的目标逻辑地址（IP 地址）映射为主机的目标物理地址（MAC 地址），最终查询 ARP 缓存信息表，从而保证主机与主机能够正常通信。

1.2ARP 地址解析过程

ARP（Address Resolution Protocol）即地址解析协议，在计算机网络系统中，ARP 根据 IP 地址获取相应的物理地址从而完成一个 TCP/IP 的协议过程。在个人计算机中都会有对应的 ARP 地址表，在这个 ARP 地址缓存表中动态的保存了 IP 地址与 MAC 地址的一一映射关系。当个人主机收到发送端发来的数据包，ARP 就会通过相应的程序在表中查找出于 IP 地址对应的关系。最后根据对应关系在数据包中添加对应的 MAC 地址。若在该地址缓存表中没有找到与之对应的关系，此时，ARP 程序就会在局域网中进行广播，并在网络中询问是否有这样的一个 IP 地址，若有，局域网中的计算机就会与之回应对应的 MAC 地址信息表，从而使得计算机就可以添加到自己 ARP 缓存表中，最后将目的 MAC 地址发送并输出，这就是 ARP 地址解析过程。

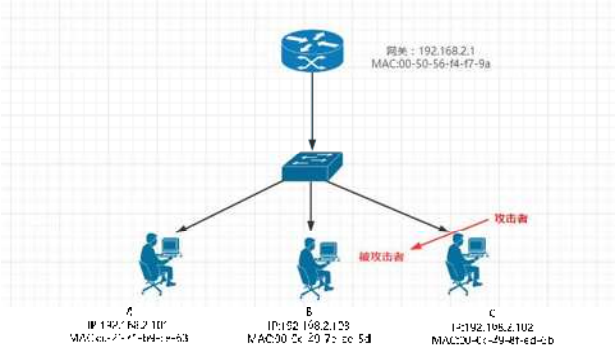
1.3ARP 欺骗原理

当一台主机收到 ARP 请求过来的数据包时，主机会对发送过来的数据包进行相应的防范判断，最后都会将收到的数据包添加到 ARP 表中。从而，一些黑客就会利用这个过程中的一些漏洞来冒充系统中的主机网关等。最终导致计算机失去通信，其系统的所有数据都会被黑客盗取，进而导致通信重定向。从而可以实现中间人攻击。

2 ARP 欺骗与中间人攻击

2.1ARP 欺骗的原理

ARP 欺骗又名 ARP 毒化，当计算机发送 ARP 请求消息时，计算机收到发送方的报文不会检测该信息就直接放入到本地 ARP 缓存信息表中，这就使得 ARP 欺骗攻击者可以在发送的过程中向计算机发送假报文，最终达到目的使得计算机接受的信息是错误的信息，从而达成了一个 ARP 欺骗过程。如图一所示：有三台计算机（A,B,C）



图一 ARP 欺骗拓扑图

如上图所示：在企业局域网中，有 A 和 B 进行访问，A 会向 B 以广播的形式发送 ARP 报文进行请求，查询谁的 IP 是 192.168.2.103，把你主机的 MAC 地址告诉我，对应的 B 会回应：我的 MAC 地址是 00-0c-29-ae-5d。在这个过程中 A 不知道 B 是否被攻击者所攻击，而就有 ARP 攻击者在 IP 地址为 192.168.2.102 的主机上，会应答到我的 MAC 地址是 00-0c-29-8f-ed-6b，对应这种回应 A 和 B 是不知道的，且这种报文传播是不间断的，是大量的，持续性的。主机 A 就会误认为攻击者 C 发送过来的 MAC 地址是 B 发送过来的。并更新了 MAC 地址表，从而攻击者 C 就会就截获了 A 发送给 B 的数据，这样攻击者主机 C 就达到了 ARP 欺骗目的。

2.2 中间人攻击简介

中间人攻击（man-in-the-middle attack）简称中间人。ARP 欺骗主要有两种方式来进行相应的中间人攻击，即欺骗主机和欺骗网关，从而导致接收端的主机与发送端的主机失去网络通信连接，也会导致通信重定

向，从而发送端主机所有数据信息都会被攻击者的主机截取。攻击者对截取的目标主机的网关和 IP 地址进行转发，攻击者主机在这个过程中作为一个中间人，不影响接收端和发送端主机的正常上网目的，就可以达到监听目标和获取相应的数据信息。

2.3ARP 欺骗攻击步骤

2.3.1ARP 欺骗

ARP 欺骗攻击的方式有很多种，其原理是向被攻击者的主机不断发送 ARP 请求并截取相应的信息，从而实现从一个主机到另一个主机数据包重定向的目的。而 ARP 欺骗攻击步骤主要分为三个过程。

2.3.2 攻击步骤

ARP 欺骗的攻击主要分为如下三个步骤：

（1）插入通信线路

作为 ARP 欺骗攻击者的攻击第一步，攻击者需要将自己的主机 C 插入到 A,B 两台主机能够正常进行通信连接的路径之间。为了达到这一目的，利用 ARP 欺骗技术，在不同时间段，攻击者主机 C 分别给 A.B 两台主机发送伪造的 ARP 响应。使得 A,B 两台主机的 ARP 缓存信息表会得到更新。正常通信的情况下，A，B 两台主机会进行数据通信和数据资源的访问。而攻击者主机 C 在插入通信线路的过程中，会让主机 A 将攻击者主机 C 的 MAC 地址作为主机 B 的 MAC 地址。同理主机 B 也会将攻击者主机 C 的 MAC 地址作为主机 A 的 MAC 地址。ARP 信息缓存表是动态更新的，攻击者主机 C 在发送伪造信息的一段时间内会失效，这就使得攻击者 C 需要定时的向主机 A,B 发送伪造的 ARP 响应，这样攻击者主机 C 就会插入到主机 A,B 之间，即作为中间人进行通信。

（2）截取数据帧

当攻击者主机 C 插入到主机 A，B 通信路径中时，主机 A，B 是数据帧在不同时间段内会被攻击者 C 主机截取。攻击者主机 C 将自己的网卡设置为混杂模式的特殊方法来截取这些数据帧，并通过自己所需要的数据进行筛选，对数据帧进行修改时，需要对数据链路层上的协议进行相应的修改，还需重新计算并检验。

（3）转发数据帧

在进行相关攻击时，攻击者主机 C 插入到主机 A,B 之间进行正常的通信，在截取数据帧时。攻击者主机 C 需要把 A,B 的数据帧信息进行修改，才能使得主机 A,B 的目的 MAC 地址误认为是自己真实的 MAC 地址。如：A,B 两台主机进行数据帧的发送时，攻击者主机 C 需要将转发的目的 MAC 地址修改为主机 B 的真实 MAC 地址。

2.4 中间人攻击实施过程

（1）开启路由重定向

攻击者主机 C 首先会开启自己的数据包进行相应的转发，类似路由器那样转发数据包。

命令：修改 /etc/sysctl.com 配置文件，修改 net.ipv4.ip_forward=1。最后使用 sysctl-p 更新生效。

（2）将受害者的流量传送给攻击者

攻击者 C 主机向 ARP 欺骗的主机 B 发送相关欺骗的数据包，网关冒充。

命　令：arpspoof-i eth0-t 192.168.2.103 192.168.2.1

（3）使网关的数据重定向到攻击者的机器

命　令：arpspoof-i eth0-t 192.168.2.1 192.168.2.103

当向网关发送 ARP 欺骗数据包时，被攻击者主机 B 的 IP 地址为 192.168.2.103，源 MAC 地址为计算机 C 网卡接口的 MAC 地址。就会使得被攻击者主机 B 的数据会错误的发送给攻击者主机 C，此时，攻击者主机 C 启用了 IP 数据转发，而被攻击者主机 B 和网关之间的传输数据经过 C 最终转发到对方，C 就成为主机 B 和网关之间通信的中间人。

（4）监听目标计算机，截取数据信息。

攻击者主机 C 通过其他软件进行对目标计算机被攻击者进行监听，如：driftnet 是一款可以从网络数据包提取图片并显示在图形窗口界面上。从而攻击者主机 C 就可以达到监听目标计算机主机。并获取被攻击者的数据信息。

3 ARP 欺骗防范对策

ARP 欺骗的防范技术有很多，目前针对企业局域网的防范方法基于以下两种：一是在个人计算机终端实现，二是通过网络设备实现。

3.1 划分 VLAN

在企业局域网中，利用 VLAN 技术可对自己企业网络规划中划分多个子网。在一定是程度上限制了攻击者攻击的范围

利用划分 VLAN 技术很容易发现 ARP 欺骗的中间人攻击，当被攻击者主机利用命令查看 ARP 缓存信息表，就会发现表中的信息是否存在异常，为了进一步达到防范 ARP 欺骗的中间人攻击，还可将自己主机 ARP 缓存信息表修改为静态设置，并对企业局域网中的主机 IP 地址和 MAC 地址进行相应的静态绑定。即可有效的防止 ARP 攻击，这种方法需要手动设置，且需要花很长时间来设置。在小型企业局域网还可以实现。但是在大型企业局域网中一般不采用。

3.2 设置静态的 ARP 缓存

攻击者主机在进行监听时，通过会修改篡改的网关达到目的。我们可以利用对 IP 地址和 MAC 地址进行相应的绑定。

命令：arp-s 输入对应的静态 IP 地址或 MAC 地址，在这个过程中应该保持有效状态。当出现错误时，可以进行相应的更新。

3.3 对数据信息进行加密处理

当企业局域网中不能及时应对 ARP 欺骗的中间人攻击时，可以对要通信的数据信息进行加密处理，攻击者主机即使监听了被攻击者主机，获取了相应的数据信息，也是很难以获得企业局域网络的数据，也很破解，在这个过程所获得的数据信息是强加密的。

3.4 绑定交换机端口

主机与主机在进行通信时，可以绑定交换机端口，分别给端口设置对应的 MAC 地址，可以有效的防止 ARP 欺骗的攻击。

结语

ARP 欺骗的中间人攻击是随着当下网络发展一种较为常见的高危害性网络攻击方式，传统的网络安全防御技术已经不适用于 ARP 的欺骗攻击。ARP 欺骗的中间人攻击通过篡改，窃取相应的被攻击者的 IP 和 MAC 地址。从而达到目的。而中间人的攻击也属于黑客的攻击方法之一，具有高破坏性，隐匿性强等特点。因此，本文在基于 ARP 原理的基础上对 ARP 中间人攻击进行研究。并给出相关防范措施，从而完善企业局域网中的安全问题。

【参考文献】

[1] 马钺，杨旭．基于 ARP 协议的网络攻防技术实践 [J]. 数码世界 .2018(1):323-325.

[2] 辛志东，李祥和，冉晓旻，等．局域网中的 ARP 重定向攻击及防御措施 [J]. 微计算机信息 （管控一体化),2005, 21(8-3):10-12。

[3]Erik Forsberg. Man in the Middle-at-tack against Microsoft Terminal Services 2003.

[4] 潘家富 .ARP 攻击的原理分析及防范对策研究 [J]. 软件工程，2019.

[5] 任侠，吕述望 .ARP 协议欺骗原理分析与防御方法 [J]. 计算机工程 ,2003,29