文章编号：2096-1472(2019)-05-25-06
DOI:10.19644/j.cnki.issn2096-1472.2019.05.006

ARP攻击的原理分析及防范对策研究

潘家富
(岭南师范学院信息工程学院，广东 湛江 524048)

摘　要：计算机网络的迅猛发展和普及，改变了人们的工作与生活，但同时也给人们带来了新的隐患，网络安全事件层出不穷。在目前计算机网络运行与使用中，ARP攻击成为最为常见的问题。本文结合自身实际工作经验，提出了一种新的ARP防御方案，在介绍IP地址和MAC地址的基础上，阐述了ARP协议的工作过程，剖析了ARP协议存在的弊端，分析了ARP攻击的原理。从网管中心端和用户端两个角度讨论防范ARP攻击的策略，并在网络环境中演示了这些策略防范ARP攻击的效果。

关键词：地址解析协议；安全防范；网络攻击
中图分类号：TP393　**文献标识码**：A

Research on the Principle of ARP Attack and Its Countermeasures

PAN Jiafu
(*School of Information Engineering*,*Lingnan Normal University*,*Zhanjiang* 524048,*China*)

Abstract: The rapid development and popularization of computer network have changed people's work and life,but also brought people new hidden troubles-endless network security events.In the current computer network operation and application,ARP attack constitutes the most common problem.The paper proposes a new ARP defense scheme based on practical experience.On the basis of introducing IP address and MAC address,this paper elaborates on the working process of ARP protocol,expounds the disadvantages of ARP,and analyzes the principle of ARP attack.This paper discusses the strategies of preventing ARP attack from both the network tube center and the user,and demonstrates these strategies in the network environment to prevent the effects of ARP attack.

Keywords:address resolution protocol;security;cyber attacks

1 引言(Introduction)

自2005年首例ARP(Address Resolution Protoco)病毒被发现起，到目前ARP病毒已经排在危害病毒的前五位，ARP病毒极大地威胁着计算机网络中用户的安全。ARP攻击的危害很大，较简单的ARP攻击会使计算机网络掉线，重要数据的丢失或密码被盗窃，具体的表现状况如下：主机网络的网速时快时慢，非常不稳定，会导致网络的通讯质量不稳定；主机死机，主机容易出现IP冲突；会导致被攻击的主机通讯困难。较复杂的ARP攻击会使核心资料被盗或出现严重的死机情况，ARP攻击使得局域网中整个计算机网络上网的用户账户信息被盗，可能会被用于进行一些其他的非法活动，给计算机网络用户造成巨大的损失；破坏计算机的屏保。ARP攻击会造成IP地址冲突，危害级别高于屏保可保护的级别，所以ARP攻击导致很多不安全问题[1]。

本论文从ARP协议和IP协议本身出发，在分析IP地址和MAC地址，以及ARP攻击原理的基础上，指出ARP协议的不安全因素，并基于网管中心端和用户端的防范策略，针对存在的安全问题给出简单可行的防御方法，达到在一定范围内解决局域网内ARP攻击的目的。

2 研究的背景和意义(Background and significance of the study)

当前，计算机网络已成为人们日常工作生活的重要基础。计算机网络通过互连和资源整合，给我们的日常工作生活带来了便利的同时，也给我们提供了丰富多彩的娱乐方式，从而极大地满足了人们相互交换信息和相互寻求帮助的需要，不断地提高人们的日常工作效率的同时，也改变人们的日常生活方式。虽然计算机网络已慢慢地成了人们日常工作生活中必不可少的“日常用品”，但是计算机网络同时也给人们带来了许多麻烦。因为使用计算机网络应用而造成的各种安全问题数量逐年上升。

如今，在我们越来越忽视局域网内的安全问题的情况下，我们却越来越依赖于互联网通讯，特别是局域网内安全的通讯。许多公司或者校园会十分重视防范局域网外的攻击，但是似乎都认为局域网内的ARP攻击扮演着一个不怎么重要的角色，因此一般对ARP攻击关注的程度都不够。总之，如何更好地防御ARP攻击显得迫在眉睫。

3 国内外研究现状(Studies at home and abroad)

目前，国内外学者采取积极的态度来对待ARP攻击,而不是被动地等待问题的出现。许多国内外学者对ARP攻击的原理进行深入研究，并提出了相应的防御措施。

在基于用户端的防范策略方面。郑文兵和李成忠提出了一种改进的ARP协议算法，对 ARP协议报文进行控制 ,使其更加安全[2]。陈曙(山东大学信息科学与工程学院副教授)提出，通过修改TCP IP内核源代码，主要是修改广播ARP请求函数arprequest和处理接收到的ARP报文的函数in_arpinput得以实现防范ARP攻击[3]。

在基于网管中心端的防范策略方面。刘亚丽和邓高峰提出，借助ARP服务器处理技术，限制局域网内部的其他主机只能接收来自ARP服务器发出的ARP响应[4]。Seung Yeob Nam、Dongwon Kim、Jeongeun Kim提出了一种增强版的ARP协议来防止基于ARP病毒的中间人攻击[5]。

在网管中心端和用户端结合的防范策略方面，Han-Wei Hsiao、Cathy S.Lin、Ssu-Yang Chang提出了一种对SNMP流数据进行挖掘的ARP攻击检测系统[6]。吴小平,周建中和方晓惠提出，基于SNMP协议主动防御ARP欺骗的基本原理[7]。

这些防范对策都在一定程度上有效缓解了ARP攻击的危害。

4 研究内容(Research contents)

本文主要研究以下内容：

(1)ARP攻击的原理分析。先讲解ARP协议的工作过程，指出该过程中可能存在的漏洞，再详细分析ARP攻击的原理。

(2)阐述基于网管中心端的防范策略。先讲解VLAN(Virtual Local Area Network)划分工作过程，再在局域网的网管中心端实施VLAN划分以实现ARP的防御。

(3)阐述基于用户端的防范策略。先讲解360局域网防火墙，ARP缓存内容和静态ARP记录的工作过程，再在局域网内用户端安装360局域网防火墙，实现实时删除ARP缓存内容和添加静态ARP记录。

(4)演示ARP攻击及防范实例。使用攻击软件“WinArpAttacker3.72”伪装成其他主机的MAC地址进行ARP攻击。利用在局域网内网管中心端实现VLAN划分，或在局域网内用户端开启360局域网防火墙，实现实时删除ARP缓存内容，以及添加静态ARP记录的防范方法进行防范ARP攻击。

5 ARP攻击原理分析(ARP attack principle analysis)

5.1 IP地址和MAC地址简介

(1)IP地址。为了确保网络上每台计算机间能够方便地进行相互间通信,TCP/IP协议(Transmission Control Protocol/Internet Protocol)规定用一串32位的二进制地址来标识相互通信的每台主机[8],这串32位的数字就是我们俗称每台计算机的IP地址。如图1所示，IP数据包由32位源IP地址和32位目的IP地址等构成，通过分析IP数据包可知发出该数据包的源主机和接收该数据包的目的主机。

图1 IP数据包的结构

Fig.1 IP packet structure

(2)MAC地址。所有可以联接到网络的计算机都必须要配置一块网卡,网卡上有一串地址,这串地址叫作物理地址(MAC地址)。如图2所示，TCP/IP四层模型的第二层(数据链路层)中需要使用到MAC地址。网络层需要通过使用ARP协议，把IP地址转换成MAC地址，如此才能将数据包传递到数据链路层。如图3所示，MAC地址采用一串48位的二进制地址来标识相互通信的每台主机，有时为方便书写,会用六个字节的十六进制表示MAC地址,每两个字节间用冒号隔开。由生产商编号和设备编号这两部分构成MAC地址，生产商编号由前三个字节来表示，设备编号由后三个字节来表示。

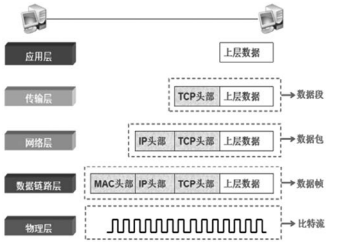

图2 TCP/IP五层网络体系结构

Fig.2 TCP/IP five-tier network architecture

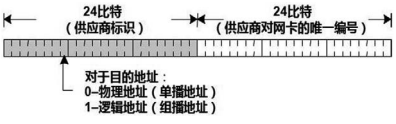

图3 MAC地址的构成

Fig.3 Composition of MAC address

5.2 ARP工作过程简介

在局域网中,一台主机要和另外一台主机进行直接通信前就需要先判断与目的主机是否是同一个网段。例如图4所示，源主机先把目标主机的IP地址与自己的子网掩码进行“与”

操作，以此判断目标主机与自己是否在同一网段(目标主机的IP地址为172.16.2.160，源主机的IP地址为172.16.34.10，源主机的子网掩码为255.255.0.0)。

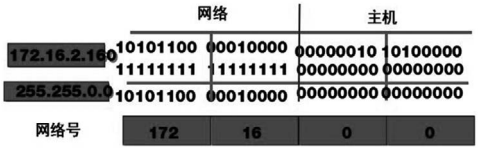

图4 目标主机的IP地址与源主机的子网掩码进行“与”操作

Fig.4 IP address of the target host and the subnet mask of the source host carry out "and" operations

如果是同一网段，那么要请求的是目的主机的MAC地址。并且在源主机的ARP缓冲区没有与目标IP地址相对应的物理地址(MAC地址)信息，则启用ARP协议工作。ARP基本功能就是通过目标计算机的IP地址，查询目标计算机的MAC地址[9]。假设局域网内有两台主机A和B，当主机A需要与主机B进行通信时，主机A首先利用ARP协议获得主机B的MAC地址，为后续进行通信做准备。现主机A已经知道主机B的IP地址且主机A需要与主机B进行通信，此时需要查询目标主机的MAC地址。如图5所示，主机请求的是同一网段的目的主机的MAC地址。

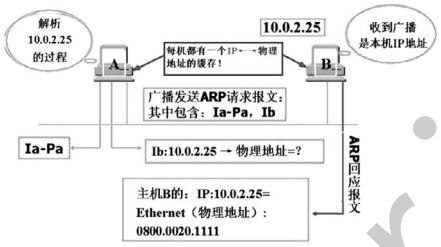

图5 主机请求的是同一网段的目的主机的MAC地址

Fig.5 Host requests the MAC address of the destination host of the same segment

如果不同网段，那么要请求的是默认网关的MAC地址，在源主机的ARP缓冲区没有与默认网关的IP地址相对应的物理地址(MAC地址)信息，则启用ARP协议工作。与源主机在同一网段中的其他所有主机都能收到ARP请求报文并能够对这个ARP请求报文进行分析，默认网关发现报文中的目标IP地址与自己的IP地址相同，则它向源主机发送ARP响应报文[10]。如图6所示，主机请求的是网关的MAC地址。

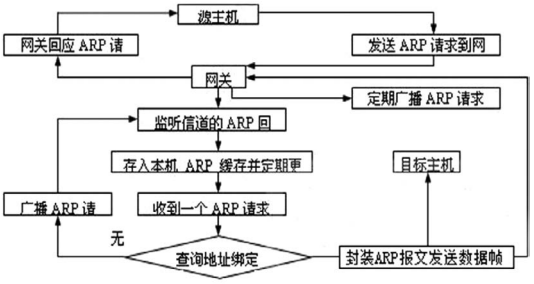

图6 主机请求的是网关的MAC地址

Fig.6 Host requests the MAC address of the gateway

通过以上ARP协议的工作原理的分析可以发现，ARP协议是建立在局域网中主机可以相互通信的基础之上，因而，ARP具有广播性、无连接性、无序性、无认证字段、无关性和动态性等一系列的安全漏洞[11]。因为这些安全问题的存在，所以利用ARP协议漏洞进行网络攻击是相对有效网络攻击方法，并且是比较难以预防的网络攻击方式。

5.3 ARP攻击原理分析

由于ARP协议并不会对报文信息的真实性进行校验，而且某主机没有发出ARP请求报文给其他任何主机的情况下，该主机同样可以接受任意主机发出的请求ARP报文的响应报文，并且该主机会更新自己的ARP缓存，把新的地址映射信息加入ARP高速缓存中。这种缺陷使得伪造别人的物理地址可以实现ARP攻击，进而使得破坏局域网安全通信成为一种可能。如图7所示，下面通过具体的例子来观察ARP攻击实现的具体过程：三台计算机连接到一台交换机。二层交换机的工作机制：交换机经过自动学习，将把它的端口号和主机的MAC地址建立对应关系。在此假设主机PC1的IP地址为IP1，MAC地址为MAC1；主机PC2的IP地址为IP2，MAC地址为MAC2；主机PC3的IP地址为IP3，MAC地址为MAC3。

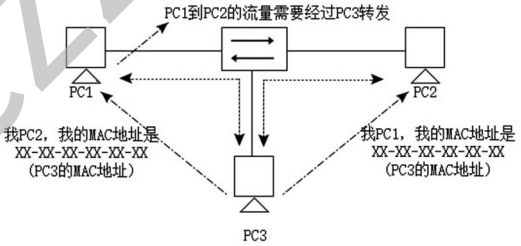

图7 ARP攻击过程

Fig.7 ARP attack process

在该网络中，假定主机PC1和主机PC2可以合法的进行通信，此时不合法的主机PC3就可以利用ARP攻击，窃听主机PC1和主机PC2的通信。过程如下：主机PC3伪装成主机PC2，主动给主机PC1发送ARP请求的响应包；数据包源IP地址为主机PC2的IP，源MAC地址为主机PC3的物理地址。目标MAC地址为主机PC1的物理地址。主机PC1接受主机PC3发出的请求ARP报文的响应报文，并且主机PC1刷新ARP高速缓存，最终主机PC1的ARP表存在主机PC3的MAC地址与主机PC2的IP地址存在映射。同理，主机PC3伪装成主机PC1，主动给主机PC2发送ARP请求的响应包；最终主机PC2的ARP表存在主机PC3的MAC地址与主机PC1的IP地址存在映射。此时不合法的主机PC3就可以利用ARP攻击。窃听主机PC1和主机PC3的通信。

经过对ARP攻击原理的分析，我们能够发现ARP攻击比较容易实现。在这个例子中因为ARP攻击发生在局域网内，所以只有内部的机器才能够互相监听。对于本来就存在严重的安全漏洞的网络来说，ARP攻击是一个较为严重的安全隐患。如果攻击方入侵到局域网内的某台主机上，并行进行ARP

攻击，如果ARP攻击成功。那么所有数据都将流经原本不应该流经的主机，将给网络造成更大的破坏。

6 ARP攻击的防范对策(Countermeasures for ARP attack)

6.1 网管中心端的防范策略

局域网内主机被恶意修改ARP表后就不会把数据包发送给正确的主机，而是发送给一个错误的MAC地址的主机，造成网络非正常通讯及网络窃听。所以需要对网管中心端进行ARP攻击防范，因为大部分的网管中心端由交换机构成，所以我们可以在交换机上创建虚拟局域网进行ARP攻击防范。

虚拟局域网(Virtual Local Area Network,VLAN)，建立在物理局域网基础之上，通过支持VLAN功能的网络设备及其管理软件构成的，可以跨越不同网段，不同网络的逻辑网络。因为广播信息只在本VLAN中传播并且划分VLAN技术可以增加广播域的数量，减少广播域的范围，使得广播信息只有在本VLAN内传播，所以增加了网络的有效带宽，提高了网络性能。可以将局域网划分成为多个不同的较小范围的VLAN，一个VLAN内发生的ARP攻击不会影响到其他VLAN内的主机通信，这个方法可以缩小ARP欺骗攻击受影响的范围。即使在局域网中出现了ARP欺骗攻击事件，判别攻击源的范围会比较容易。与此同时，网络管理员可以采用划分VLAN技术，简化管理的网络，在局域网中通过划分多个VLAN，可以增加广播域的数量，减少广播域的范围，这样可以有效地抑制广播风暴的出现，提高了网络的安全性。

6.2 用户端的防范策略

(1)实时删除ARP缓存内容

在局域网中,一台主机要和另外一台主机进行直接通信时就必须要知道目标主机的MAC地址,这个目标主机的MAC地址需要通过ARP获得的。由于ARP协议并不会对报文信息的真实性进行校验,可以接受ARP报文的响应报文，并且更新自己的ARP缓存,把新的地址映射信息加入ARP高速缓存中，这种缺陷使得伪造别人的物理地址可以实现ARP攻击。所以可以通过不断的清除主机ARP缓存中的信息，这样错误的ARP缓存信息就被删除了，以此达到防范ARP攻击的目的。

(2)启用360局域网防火墙

目前大多数网络公司在防火墙这类安全产品中加入对ARP攻击的防范，通常是从底层驱动对所有ARP攻击数据包进行识别和屏蔽，可以防御ARP攻击。启动360局域网防火墙主要功能有拦截外部ARP攻击，拦截IP冲突和主动防御[12]。

(3)添加静态ARP记录

由于ARP协议并不会对报文信息的真实性进行校验。主机可以接受其他任意主机发出的请求ARP报文的响应报文，并且该主机会更新自己的ARP缓存,把新的地址映射信息加入ARP高速缓存中。这种缺陷使得伪造别人的物理地址可以实现ARP攻击。如果在ARP表中添加静态ARP记录则可以避免ARP攻击。添加静态ARP记录又被称为ARP绑定。它的主要特点是ARP纪录永远不过期。ARP攻击的漏洞是数据在传输过程中对应的IP地址和MAC地址的关系被更改，只需要手工将局域网中其他主机的IP地址和与其对应的物理地址进行绑定，这种方法可以防止主机再受到ARP欺骗攻击，但是采用添加静态地址的方法防止ARP欺骗攻击的前提条件，是网络中所有主机的IP地址和物理地址是固定不变的。如果在网络环境中增加新的主机或新的主机网卡的时候，需要相应的改变IP地址和物理地址。ARP绑定是对局域网内的主机IP地址和对应的MAC地址进行绑定，是防止ARP攻击的有效方式之一。依据ARP攻击的原理，若需要解决ARP攻击事件，对用户端主机都进行ARP绑定是可以解决问题的。

7 ARP攻击及防范实例(Examples of ARP attack and prevention)

7.1 网络环境搭建

如图8所示，是用来演示ARP攻击及防范的网络环境，其包括一台交换机和三台主机。交换机模拟网管中心端，三台主机分别为用于模拟用户端的主机A，模拟攻击者的主机B和模拟用户端的主机C。主机A的IP地址为192.168.1.102，MAC地址为a4-17-31-c0-75-2f；主机B的IP地址为192.168.1.108，MAC地址为24-0a-64-cd-f2-2f；主机C的IP地址为192.168.1.105，MAC地址为80-a5-89-51-49-6。

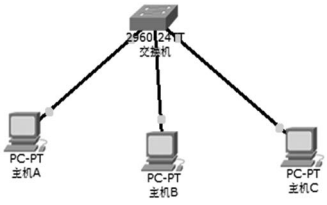

图8 网络拓扑图

Fig.8 Network topology

7.2 ARP攻击过程演示

以下演示攻击者主机B伪装成用户端主机C，并且告诉用户端主机A自己是主机C，以此对用户端主机A进行ARP攻击。

(1)主机B伪装成主机C：主机B主动给主机A发送ARP请求的响应包。数据包源IP地址为主机C的IP，源MAC地址为主机B的MAC地址。目标MAC地址为主机A的MAC地址。如图9所示，在Dst Hardware Mac中写入主机A的MAC地址，Arp op中选择Reverse reply，Src Protocol Mac中写入主机B的MAC地址，Src IP中写入主机C的IP地址。

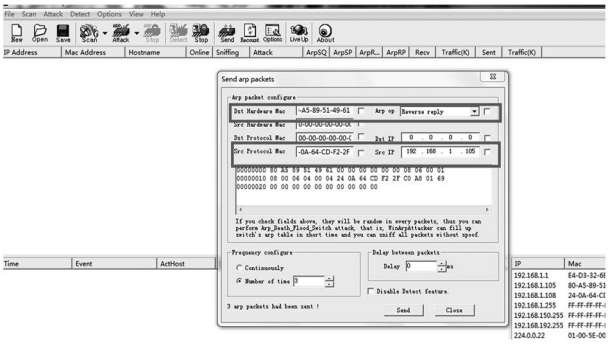

图9 在主机B使用软件伪装MAC地址

Fig.9 Software camouflage MAC address used on host B

(2)验证主机B成功发送出伪装成主机C的ARP请求响应数据包：在主机A上使用抓包工具，抓取ARP数据包。如图10所示，有一个ARP请求响应数据包发到主机A上，告诉主机A，IP地址为192.168.1.105的主机的MAC地址为24−0a−64−cd−f2−2f。

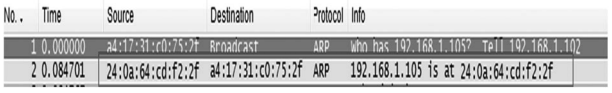

图10 在主机A上抓取的ARP请求响应数据包

Fig.10 Responsive packet to ARP request crawled on host A

(3)主机B攻击成功：如图11所示，用命令arp−a显示主机A的ARP表，主机B的MAC地址与主机C的IP地址存在映射。

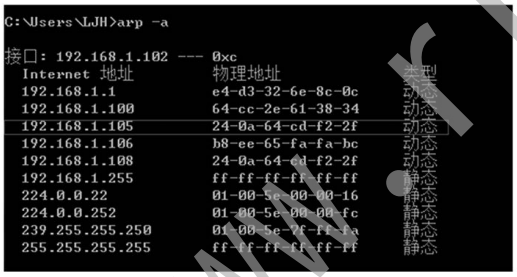

图11 主机A的ARP表

Fig.11 ARP table of host A

(4)验证攻击者主机B伪装成用户端主机C，如图12所示，在主机A上访问主机C(ping主机C的IP地址)。如图13所示，在主机A上使用抓包工具，抓取ICMP数据包，发现目的IP为主机B的IP地址，说明此时主机A是与主机B通讯。

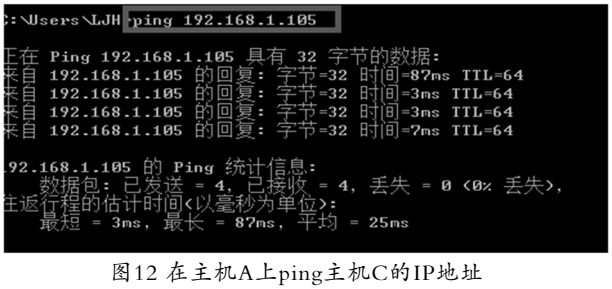

图12 在主机A上ping主机C的IP地址

Fig.12 IP address of ping host C on host A

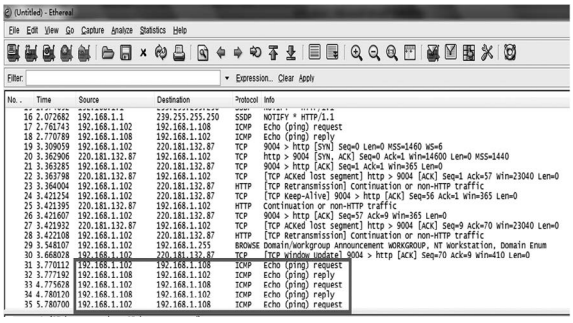

图13 在主机A上抓取的ICMP数据包

Fig.13 ICMP packets crawled on host A

同理，攻击者主机B可以伪装成用户端主机A，并且告诉用户端主机C自己是主机A。只需要主机B主动给主机C发送ARP请求的响应包。数据包源IP地址为主机A的IP，源MAC地址为主机B的MAC地址，目标MAC地址为主机C的MAC地址。

7.3 网管中心端防范结果

(1)在网管中心端交换机上划分两个VLAN，端口0/1与端口0/2划分为VLAN 1，端口0/5划分为VLAN 2，如图14所示，因为VLAN 1是所有端口默认的VLAN模式，所以只需要用命令switchport access vlan 2把端口0/5划分为VLAN 2。

图14 把交换机的端口0/5划分为VLAN 2

Fig.14 Port 0/5 of the switch is divided into VLAN 2

(2)在网管中心端交换机上给VLAN 1和VLAN 2分配IP地址和网段，如图15所示，VLAN 1的IP地址为172.16.1.1，所在网段为172.16.1.0；VLAN 2的IP地址为172.16.2.1，所在网段为172.16.2.0。

图15 在交换机上做VLAN网段的划分

Fig.15 Dividing VLAN network segments on switches

(3)验证主机B对主机C的ARP攻击失效：在主机C上使用抓包工具，抓取ICMP数据包，并且在主机C上访问主机A(ping主机A的IP地址)。如图16所示，发现目的IP为主机A的IP地址，说明此时主机A是与主机C通讯。

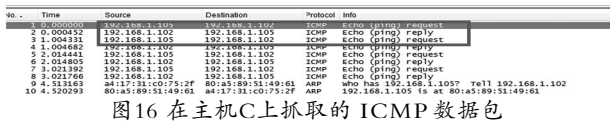

图16 在主机C上抓取的ICMP数据包

Fig.16 ICMP packets crawled on host C

7.4 用户端防范结果

7.4.1 实时删除ARP缓存内容的防范结果

(1)删除缓存在ARP表的动态表项：在主机A上使用命令

netsh i i show in查找连接网络的端口；使用命令netsh–c “i i” delete neighbors端口号来删除缓存在ARP表的ARP信息的表项。如图17所示，主机A的无线连接网络的端口为12。

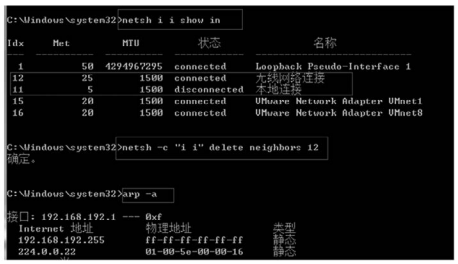

图17 在主机A上删除缓存在ARP表的所有动态表项

Fig.17 Deleting all dynamic table items cached on the ARP table on the host A

(2)验证主机B对主机A的ARP攻击失效：在主机A上使用抓包工具，抓取ICMP数据包，并且在主机A上访问主机C(ping主机C的IP地址)。如图18所示，发现目的IP为主机C的IP地址，说明此时主机A是与主机C通讯。

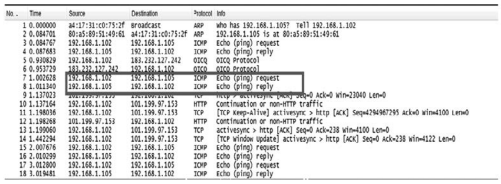

图18 在主机A上抓取的ICMP数据包

Fig.18 ICMP packets crawled on host A

7.4.2 启用360局域网防火墙的防范结果

(1)在主机A上启用360局域网防火墙，如图19所示。

图19 在主机A上开启360局域网防火墙

Fig.19 Open 360 LAN firewall on host A

(2)验证主机B对主机A的ARP攻击失效：在主机A上使用抓包工具，抓取ICMP数据包，并且在主机A上访问主机C(ping主机C的IP地址)。如图20所示，发现目的IP为主机C的IP地址，说明此时主机A是与主机C通讯。

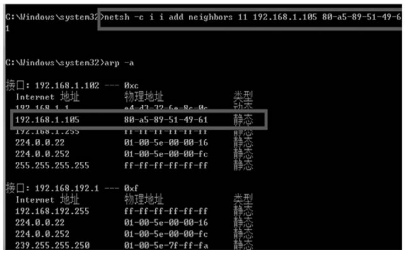

图20 在主机A上抓取的ICMP数据包

Fig.20 CMP packets crawled on host A

7.4.3 添加静态ARP记录防范结果

(1)在主机A上使用命令netsh–c i i add neighbors 11 192.168.1.105 80–a5–89–51–49–61添加静态ARP记录(主机C的IP地址与主机C的MAC地址进行绑定)。如图21所示，添加静态ARP记录，IP地址为192.168.1.105与MAC地址为80–a5–89–51–49–61。

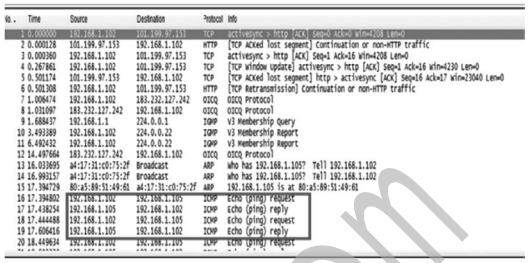

图21 主机A的ARP表

Fig.21 ARP table of host A

(2)在主机C上使用命令netsh–c i i add neighbors 11 192.168.1.105 80–a5–89–51–49–61添加静态ARP记录(IP地址为192.168.1.105与物理地址为80–a5–89–51–49–61进行绑定)，如图22所示。

图22 主机C的ARP表

Fig.22 ARP table of host C

(3)验证主机B对主机A的ARP攻击失效：在主机A上使用抓包工具，抓取ICMP数据包，并且在主机A上访问主机C(ping主机C的IP地址)。如图23所示，发现目的IP为主机C的IP地址，说明此时主机A是与主机C通讯。

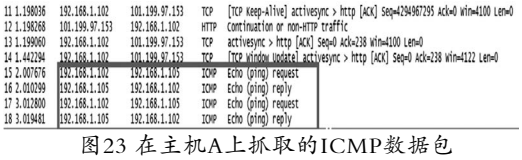

图23 在主机A上抓取的ICMP数据包

Fig.23 ICMP packets crawled on host A

(4)验证主机B对主机C的ARP攻击失效：在主机C上使用抓包工具，抓取ICMP数据包，并且在主机C上访问主机A(ping主机A的IP地址)。如图24所示，发现目的IP为主机A的IP地址，说明此时主机A是与主机C通讯。

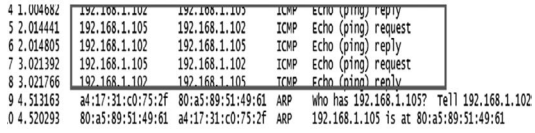

图24 在主机C上抓取的ICMP数据包

Fig.24 ICMP packets crawled on host C

8 结论(Conclusion)

当前，计算机网络已成为人们日常工作生活的重要基础。由于ARP协议并不会对报文信息的真实性进行校验，使得ARP协议存在严重的安全问题。本论文基于网管中心端、用户端的综合防范策略，针对存在的安全问题给出简单可行的防御方法，达到在一定范围内解决局域网内ARP攻击的目的。但是仍然存在许多的不足，例如本文中提供的防御方法实施过程较为烦琐，对用户的要求较高；其次本文中提供的防御方法很难防范复杂的ARP攻击。在以后的学习生活中，我将继续探索ARP攻击的原理及防范对策，让自己掌握更多关于ARP攻击防范的技能。

参考文献(References)

[1] 温卓然.ARP防御系统的设计和实现[D].北京邮电大学,2009,35.

[2] 曹洪武.ARP欺骗入侵的检测与防范策略[J].塔里木大学学报,2007(02):88-91.

[3] 徐功文,陈曙,时研会.ARP协议攻击原理及其防范措施[J].信息技术与信息化,2005(01):4-6.

[4] 孟晓明.基于ARP的网络欺骗的检测与防范[J].信息技术,2005(05):41-44;75.

[5] Curriculum vitae Alissa Jan Arp[J].Romberg Tiburon Center for Environmental Studies San Francisco State University,2005(4):40-42.

[6] 王小玲,周刚.一种扩展的ARP协议设计[J].四川理工学院学报(自然科学版),2011(02):178-181.

[7] 吴小平,周建中,方晓惠.基于SNMP的ARP欺骗主动防御机制[J].华中师范大学学报(自然科学版),2007(04):512-514.

[8] 何显文.基于ARP协议的网络欺骗与防范[J].通化师范学院学报,2011(06):22-24.

[9] 潘晓君.基于缓存超时的ARP欺骗攻击协议的研究[J].计算机技术与发展,2009(10):167-169.

[10] 姚小兵.ARP协议简析及ARP病毒攻击的防御[J].信息网络安全,2009(09):49-50;55.

[11] 沈涛.基于入侵检测的网络安全研究[D].重庆大学,2012:240-228.

[12] 樊景博,刘爱军.ARP病毒的原理及防御方法[J].商洛学院学报,2007(02):37-41.

作者简介：

潘家富(1977-)，男，硕士，经济师.研究领域：信息化建设，WEB前端开发.

(上接第45页)

收。由于在数据服务端，每一个完整的数据报文被拆分成若干个128kB的小文件，文件名中包含标识先后顺序的数字，每一个完整数据报文除最后一个小文件外，其他文件的体积若不等于128kB，该模块则向数据通信服务模块请求重传。

多源数据融合模块负责对已下载的数据进行解压缩，再进行融合计算。举例来说，当用户单指在屏幕上划过雷达回波的范围，该模块则计算雷达体扫数据的垂直剖面，再将计算结果交由图形绘制模块进行图形绘制并展现在终端屏幕上。再如，当用户在终端上设定了预报时效，该模块则使用已下载的雷达数据进行雷达回波的外推预报，以及定量降水估测等。

综上所述，本系统的用户通过智能应用端的用户交互模块，实现对当前实况天气的监测、诊断和分析，对短时临近天气和灾害性天气进行预报、预警，以及其他满足行业需求的主观天气分析工作。

4 结论(Conclusion)

本系统的设计与实现，可为在近海、海上和高原等移动数据传输不发达区域且对天气条件敏感的行业用户，提供面向智能移动终端的短时临近天气主观分析交互平台，用较小的无线数据传输量，通过便捷的移动设备，向户外作业的专业人员提供可交互、可视化的天气实况监测、主观天气分析、预报服务及应用。

参考文献(References)

[1] Voosen P.Storms await weather executive at climate agency[J].Science,2017,358(6361):287.

[2] 华韵子,林红.华东区域自动站数据实时融合显示与多级警示技术研究[J].软件工程,2016,19(5):26-29 .

[3] 张小雯,郑永光,吴蕾.风廓线雷达资料在天气业务中的应用现状与展望[J].气象科技,2017,45(2):285-297.

[4] 郭莹莹,黄鹏宇,黄鹏飞.基于Android的气象服务App的设计与实现[J].软件工程,2018,21(04):43-45.

[5] 贾斌,李又君,衣霞,等.城区防汛智慧气象系统设计与实现[J].软件工程,2018,21(10):46-49.

[6] Xiong B,Tan H F.A robust and efficient structural reliability method combining radial-based importance sampling and Kriging[J].Science China Technological Sciences,2018(05):1-11.

[7] 王兴,张琳焓,王丽娟,等.基于Kriging的加密自动气象站要素场插值与改进[J].软件工程,2015(11):6-10.

[8] 万玉铸,徐志江,卢为党,等.具有高吞吐量的可靠UDP协议[J].计算机工程与设计,2017(12):3202-3206.

作者简介：

王　兴(1983-)，男，博士，高级工程师.研究领域：气象信息与安全，人工智能.

朱　彬(1969-)，男，博士，教授.研究领域：大气物理，气象工程.

毛雅萍(1998-)，女，本科生.研究领域：大气科学.

王　晖(1981-)，男，硕士，高级工程师.研究领域：计算机应用，软件工程.