基于Libpcap的局域网ARP攻击与防御系统

夏 磊,杨善林,褚 伟
(合肥工业大学 计算机网络所,安徽 合肥 230009)

摘 要:针对局域网中ARP的攻击,从ARP协议的角度,分析了ARP攻击的原理和它们导致终端用户访问服务器时出现异常中断的情况。同时,围绕该协议内在的缺陷,详细说明了ARP攻击的过程,并利用Libpcap对网络数据进行抓包分析,实现了对ARP攻击的一种有效的检测系统。最后提出了ARP攻击的几种防御方法。

关键词:ARP协议; 数据包; Libpcap; 检测系统
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)03-0164-04

ARP Attacks and Defense System Based on Libpcap

XIA Lei, YANG Shan-lin, CHU Wei
(Institute of Computer Network, Hefei University of Technology, Hefei 230009, China)

Abstract: For the ARP attacks and from the point of its protocol, analyzes the principle of ARP attacks and the failed access to server caused by it. Meanwhile, through analysing the deficiency of the protocol, illustrates the ARP attacks course and grabs the data packets by making use of the Libpcap, then realizes a kind of detecting system of ARP attacks effectively. Finally, proposes some solutions and strategies to solve the problem.

Key words: ARP protocol; data packet; Libpcap; detecting system

0 引 言

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,内网的病毒攻击的种类也是多种多样。在大部分的病毒攻击行为中,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(ARP, Address Resolution Protocol)就是局域网中解决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攻击。

分析了常见的ARP欺骗攻击的表现形式、主要危害及运作原理,提出了一种实际可操作的、比较完善的ARP病毒检测系统。

1 ARP协议

1.1 ARP协议在协议族中的地位及其工作原理

由表1可以看出,ARP协议 位于TCP/IP协议族群中网际层的底部。

表1 ARP协议在TCP/IP协议族中的位置

FTP,TELNET,SMTP等	应用层
TCP, UDP	传输层
ICMP, IGMP	网际层
IP	
ARP, RARP	
各种网络接口	网络接口层

在网络中,一个计算机要与另外一台计算机进行数据通讯的话就必须知道对方的MAC地址。MAC地址就是通过ARP协议获取的。每台安装有TCP/IP协议的计算机都有一个存放在缓存中的ARP列表,表内的MAC地址和IP地址是一一对应的。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[1]。一台计算机A要与另一台计算机B进行通讯时,会首先检查自己ARP列表中是否存在计算机B的IP地址对应的MAC地址,如果有就直接将数据包发送到这个MAC地址;反之,就向本地网段发起一个ARP请求的广播包,查询此目的主机对应的MAC地址。此ARP请求数据包里包括源主机的IP地址、硬件地址,以及目的主机的IP地址。当被访问目标B收到广播后它就会自动回应一个信息给发广播的机器A,其它机器则不会给发广播的机器

收稿日期:2008-07-04
基金项目:国家自然科学基金(70471046)
作者简介:夏 磊(1984-),男,安徽合肥人,硕士研究生,研究方向为嵌入式系统与计算机网络;褚 伟,教授,研究方向为计算机网络。

A 回应任何信息,当收到目标 IP 所有者的 ARP 回应后,更新本机的 ARP 列表。这样计算机 A 就可以更新列表并与计算机 B 进行正常通讯。ARP 列表有老化机制,在一定时间后会重新更新[2]。

1.2 ARP 协议的缺陷

ARP 协议默认情况下是信任网络内的所有节点,并且任意节点都可以进行广播。这样,就给 ARP 协议带来了一个从根本上无法解决的缺陷:如果有一个不被信任的节点对本地网络具有写访问许可权,那么就会有某种风险。这样一台机器可以发布虚假的 ARP 报文并将所有通信都转向它自己,然后它就可以扮演某些机器,或者顺便对数据流进行简单的修改,或者进行中间者欺骗[3]。

2 ARP 攻击的原理

2.1 ARP 攻击与欺骗的原理

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[4]。ARP 欺骗主要达到两种攻击效果:

1)攻击者可在两台正在通信的主机 A,B 之间充当中间人(Man - In - The - Middle)。如图 1 所示,病毒机假冒主机 B 的 IP 地址(192.168.14.2),而 MAC 地址为病毒机的 MAC 地址(XX - XX - XX - XX - XX - XX)来欺骗主机 A,使其将数据发往病毒机,并且病毒机可开启 IP 路由功能,将数据包再转发至主机 B。同时,病毒机对主机 B 实施相同的欺骗,因此,主机 A,B 之间的所有通信内容都被病毒机所窃听。

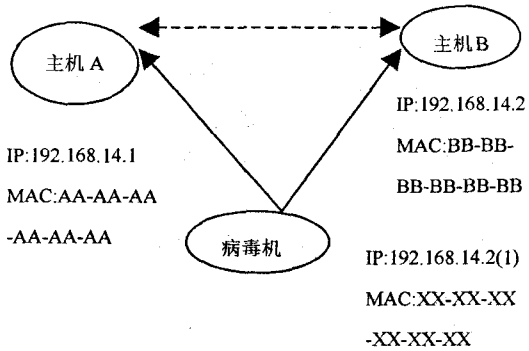

图 1　冒充中间人

2)伪造 ARP 包(请求或应答),迫使目标主机下线。如图 2 所示,病毒机伪造的 ARP 包源 IP 填入主机 A 的 IP 地址(192.168.14.1),源 MAC 可以是病毒机自己的(XX - XX - XX - XX - XX - XX),也可以伪造的,在目标信息中,填入主机 A 的 IP 为 192.168.14.1,MAC 为(AA - AA - AA - AA - AA - AA),然后循环地发送,当主机 A 收到后,发现 IP 地址与自己的冲突,于是产生一个 IP 冲突对话框,同时数据通讯会受到影响。当主机 A 不停地接收这种包时,会使数据通讯处于"不停地中断"的状态,从而迫使主机 A 中断所有联系。

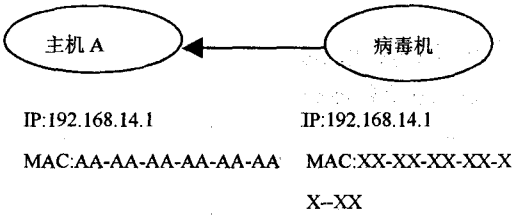

图 2　伪造 ARP 包

3)伪造应答 ARP 包,冒充网关,截获所有出网通讯,使网内所有主机无法通过网关上网。如图 3 所示,病毒机在源 IP 中填入网关的 IP,在源 MAC 中填入自己的 MAC,然后向整个网段发送广播数据包,从而使网段内所有主机原本发往网关的数据全部错误地发往病毒机,这时所有主机均无法上网。

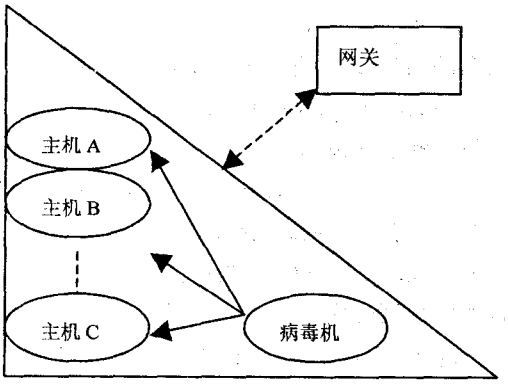

图 3　冒充网关

2.2 ARP 协议的报文格式

表 2 展示了 ARP 协议中的报文格式。

表 2　以太网上的 ARP 报文格式

0　　8　　16　　24　　32

硬件类型		协议类型
硬件地址长度	协议长度	操作类型
发送方首部(八位组 0 - 3)		
发送方首部(八位组 4 - 5)		发送方 IP(八位组 0 - 1)
发送方 IP(八位组 2 - 3)		目标首部(八位组 0 - 1)
目标首部(八位线 2 - 5)		
目标 IP 地址(八位线 0 - 3)		

在表 2 中,硬件类型字段指明了发送方想知道的硬件接口类型,以太网的值为 1。协议类型字段指明了发送方提供的高层协议类型,IP 为 0806(16 进制)。硬件地址长度和协议长度指明了硬件地址和高层协议地址的长度。操作字段用来表示这个报文的目的,ARP 请求为 1,ARP 响应为 2,RARP 请求为 3,RARP

响应为 4。当发出 ARP 请求时，发送方填好发送方首部和发送方 IP 地址，还要填写目标 IP 地址。当目标机器收到这个 ARP 广播包时，就会在响应报文中填上自己的 48 位主机地址。

3 基于 Libpcap 的 ARP 攻击的检测系统

3.1 Libpcap 函数库介绍

Libpcap 是由 Berkeley 大学的 Van Jacobson，Craig Leres 和 Steven McCanne 编写的，该函授库支持 Linux，Solaris 和 BSD 系统平台，是一个独立于具体平台的网络数据捕获开发包。它提供了一个高层的编程接口，隐藏操作系统的细节，可以捕获网络上的所有数据包。Libpcap 支持 BPF 过滤机制，使得它具有捕获特定数据包的功能，即可根据具体需求捕获用户感兴趣的数据包。内核支持“packet”协议，也即在编译内核时打开配置选项 CONFIG_PACKET(选项缺省为打开)。

设计中用到以下几种函数：

1)char * pcap_lookupdev()功能：找到一个非回送的活动的网络接口，并返回其对应的文件名。

2)int pcap_lookupnet()功能：获取指定的网络接口的网络号和子网掩码。

3)pcap－t * pcap_open_live()功能：打开网络接口，根据用户的输入参数对网络接口进行设置。

4)int pcap_compile()功能：将描述性的过滤规则转换成系统识别的代码。

5)int pcap_setfilter()功能：设定一个过滤程序

6)int pcap_loop()功能：收集和处理数据包。

3.2 一种有效的 ARP 攻击检测系统

由于 ARP 攻击是利用 ARP 协议的缺陷进行攻击的，所以可以利用 Libpcap 工具库，将数据抓包的方式设置成混杂模式，这样可以对流经本机器端口的所有数据包进行抓获，然后再通过对所抓数据包里 IP 和 MAC 地址的对应关系的检测，可以很容易知道本网段内是否有 ARP 攻击。

在 Linux 2.6.10 下，利用 Kedevelop 作为开发环境，使用 C 语言开发了一个 ARP 攻击检测系统。系统的具体实施是利用两层结构：第一层结构由一个结构体组成，记录正确的 IP 和 MAC 对应关系；第二层结构由两个小结构体组成，一个用来记录 IP 相同但 MAC 不同的对应关系，一个用来记录 MAC 相同但 IP 不同的对应关系，然后逐一将它们与第一层里的结构体中正确的 IP、MAC 对应关系进行对比，一般可分为四种情况：

1)当新捕获的数据包中 Ip 和 Mac 的值与第一层结构中的每对 Ip 和 Mac 的值均不相同时，便将其作为一个新的对应关系保存起来；否则，当新捕获数据包中 Ip 与 Mac 的值与第一层结构体中某对 Ip 和 Mac 的值均相同时，便放弃此数据包。

2)当新捕获数据包中的 Ip 与第一层结构体中某对对应关系有相同的 Ip 值但 Mac 值不同时，在第二层中的第一个结构体中，将其作为一个新的对应关系保存起来，并表现为“IP 冲突”。

3)当新捕获的数据包中的 Mac 值与第一层结构体中某对 Mac 值相同但 Ip 值不同时，在第二层中的第二个结构体中，将其作为一个新的对应关系保存起来，并表现为“ARP 病毒攻击”。

4)当在整个局域网中病毒主机只在攻击一台主机时，其他主机仍可以正常上网。这时，能正常上网的主机可以 ping 病毒主机，这样病毒主机同样会以相同的方式攻击此主机，从而在该主机上能判断出局域网内是否存在 ARP 病毒攻击。

在整个程序中，第一层与第二层所使用的结构体分别如下所示：

```
Struct Right_IpMac {
  char NewIp[];//记录新的 IP;
  char NewMAC[];//记录新的 MAC;
  struct Ipsame_Macdiffer Ips_Macd;
  struct Macsame_Ipdiffer Macs_Ipd;
}//第一层结构体(记录正确的 Ip、Mac 关系);
Struct Ipsame_Macdiffer {
  char sameIp[];//记录相同 Ip 值;
  char differMac[];//记录不同 Mac 值;
}//第二层结构体(记录 IP 值相同但 MAC 值不同的对应关系);
Struct Macsame_Ipdiffer {
  char sameMac[];//记录相同 Mac 值;
  char differIp[];//记录不同 Ip 值;
}//第二层结构体(记录 MAC 值相同但 IP 值不同的对应关系);
```

通过上述这样的一个简易程序运行，可以很容易判断出该网段内是否有 ARP 病毒的存在。

4 ARP 攻击的几种主要防御方法

1)使用静态 ARP 缓存。

即用 arp －s 命令在各主机上绑定网关的 IP 和 MAC 地址，同时在网关上绑定各主机的 IP 和 MAC 地址[5]。如果是 WIN 主机可编写一个批处理文件。

rarp.bat，内容如下：

```
@echo off
arp －d
arp －s 192.168.14.48 00－22－aa－00－22－bf
```

实际操作时，文件中的将网关 IP 地址和 MAC 地址更改为您自己的网关 IP 地址和 MAC 地址即可。

若想让系统每次启动时都能自动地加载静态ARP,则可将这个批处理软件拖到“windows——开始——程序——启动”中。使用静态ARP缓存增大了网络维护量,在较大或经常移动主机的网络中这样做更为困难。使用静态ARP缓存只能防止ARP欺骗,对IP地址冲突、Flood攻击仍然没有办法阻止。

2)对病毒源头的机器进行处理,杀毒或重装系统。此操作非常重要,因为解决了ARP欺骗的源头PC机的问题,就可以保证内网免受攻击。

3)用可防ARP攻击的交换机(彻底防治)[6]。使用三层交换机,绑定“端口-MAC-IP”,限制ARP流量,及时发现并自动阻断ARP攻击端口,合理划分VLAN,彻底阻止盗用IP、MAC地址,杜绝ARP的攻击,这也是目前防止ARP攻击的最有效方法之一。

5　结束语

网络欺骗攻击作为一种非常专业化的攻击手段,给网络安全管理者带来了严峻的考验。ARP欺骗是一种典型的欺骗攻击类型,它利用了ARP协议存在的安全漏洞,并使用一些专门的攻击工具,使得这种攻击变得普及并有较高的成功率。文中通过分析ARP协议的工作原理,探讨了ARP协议从IP地址到MAC地址解析过程中的安全性,给出了网段内ARP欺骗的实现过程,提出了一种有效的检测系统和几种可行的解决方案,以最大限度地杜绝ARP欺骗攻击的出现。总之,对于ARP欺骗的网络攻击,不仅需要用户自身做好防范工作之外,更需要网络管理员应该时刻保持高度警惕,并不断跟踪防范欺骗类攻击的最新技术,做到防范于未然。

参考文献:

[1] Plummer D C. An Ethernet Address Resolution Protocol[M]. 北京:机械工业出版社,1982.

[2] 谢希仁. 计算机网络[M]. 第4版. 北京:电子工业出版社,2003.

[3] Nachreiner C. Anatomy of an ARP Poisoning Attack[EB/OL]. 1999-07-11. http://www.watchgu-ard.com.

[4] Liruixue. ARP协议的缺陷及ARP欺骗的防范[M]. 北京:机械工业出版社,2007.

[5] 任　侠,吕述望. ARP协议欺骗原理分析与抵御方法[J]. 计算机工程,2003,29(9):127-128.

[6] 宋　志. 一种基于PVLAN的反ARP欺骗的技术实现方法[J]. 计算机安全,2007(10):55-59.

(上接第160页)

跟踪和发现客户的流失趋势,及早采取预防措施,最大限度地降低客户流失率。

4　结束语

研究和实现了决策树分类算法ID3,通过该算法作用于银行数据,得出一个银行客户流失的模型,通过提取模型中的规则,对于银行预测客户流失特征具有一定的辅助作用。

参考文献:

[1] Han Jiawei, Kamber M. Data mining: Concepts and Technique [M]. Beijing: China Machine Press, 2006.

[2] 盛昭瀚,柳炳祥. 客户流失危机分析的决策树方法[J]. 管理科学学报,2005,8(2):20-25.

[3] Tan Pang-Ning, Steinbach M, Kumar V. 数据挖掘导论[M]. 北京:人民邮电出版社,2006:89-193.

[4] Rud O P. 数据挖掘实践[M]. 北京:机械工业出版社,2003:225-264

[5] 王黎明. 决策树学习及其剪枝算法研究[D]. 武汉:武汉理工大学,2007.

[6] 任　伟,丁荣涛. 改进的ID3算法在学习模型的研究与应用[J]. 福建电脑,2007(8):109-110.

[7] 杨　明,张载鸿. 决策树学习算法ID3的研究[J]. 微机发展(现更名:计算机技术与发展),2002,12(5):6-8.

(上接第163页)

海交通大学,2007.

[4] 任　栋,刘连忠. 一种Web应用环境下安全单点登录模型的设计[J]. 计算机工程与应用,2002,38(24):174-176.

[5] 黄　建,倪惜珍. 引入时间特性的角色访问控制[D]. 北京:中国科学院研究生院,2003.

[6] Matheus A. How to declare access control policies for XML structured information objects using OASIS' eXtensible Access Control Markup Language (XACML) [C]//. proceedings of the 38th Hwaii Conference on System Sciences. [s. l.]: [s. n.], 2005.

[7] Chou Shih-Chien. LRBAC: A Multiple-Levelled Role Based Access Control Model for Protecting Privacy in Object-Oriented Systems[J]. Journal of Object Technology, 2004, 3(3): 91-120.

[8] 许　谦,雷咏梅. 一种增强访问控制的服务发现机制[J]. 计算机技术与发展,2007,17(5):99-100.