杭州应用工程技术学院学报,第 13 卷第 2 期,2001 年 6 月
Journal of Hangzhou Institute of Applied Engineering
Vol.13 No.2, Jun. 2001

警惕网络 Sniffer 的危害

沈海娟
(杭州职业技术学院,杭州 310015)

摘 要 Sniffer,又称网络嗅探器,是利用网络数据传输机制而工作的一种网管工具,但也可以成为一种黑客的攻击工具.本文分析了 Sniffer 的工作机制,提出了若干防范措施.

关键词 Sniffer 网管 网络安全 黑客
中图分类号 TP316.8

1 Sniffer 的含义

在网络中,当信息进行传输时,我们可以利用工具将网络接口设置在监听模式下,这样就可以将网络中正在传输的信息截获,从而进行处理.Sniffer 就是利用计算机的网络接口截获在网络中传输的数据信息的一种工具.

商用化的工具产品如美国网络联盟公司的 Sniffer 网络协议分析仪对网管具有重要意义.网管通过 Sniffer 可以方便地确定某种网络协议拥有的通讯量、哪台主机是主要的通讯目的地、主机相互间发送报文的时间间隔、发送报文占用的时间等等,这些信息为网管判断网络问题、管理网络提供了非常宝贵的信息,但所谓网络黑客也可以编制 Sniffer 的软件来获取信息,如用户密码、金融帐号、机密数据等,从而危害网络的安全.

2 Sniffer 的工作原理及危害方式

下面我们来分析一下 Sniffer 的工作原理,在讲述 Sniffer 原理之前,有必要先了解一下局域网、以太网、网卡、HUB 的工作原理.

2.1 局域网

局域网有 4 项基本技术:

(1) 传输介质:传输介质是连接发送方和接收方的物理通路,是网络数据传输的载体,局域网中常用的传输介质有同轴电缆、双绞线、光纤三种.

(2) 拓扑结构:网络物理拓扑结构就是用物理线路连接起来时所形成的物理上的几何形状;网络逻辑拓扑结构则是指介质访问控制策略采用的网络几何形状.常见的物理拓扑结构有:总线型、

收稿日期:2001 - 01 - 12

星型、环型.

(3) 信号技术:信号技术指的是在网络传输介质中传输的是数字信号还是模拟信号及信号的编码、调制方式.一般局域网中常用数字信号进行传输.

(4) 介质访问控制:它是局域网中最重要的技术之一,介质访问控制的任务就是保证网上站点能有效地、公平地利用共享通信介质发送和接收数据.目前局域网中常用 CSMA/CD(载波监听多路访问/冲突检测)、Token-Ring(令牌环)、Token-Bus(令牌总线)三种介质访问控制方法.

2.2 以太网的基本工作原理

首先我们先了解一下基于以太网的数据格式(见表1).

表1 以太网的数据格式

先导字段	帧始符	目的地址	源地址	帧格式	数 据	填充段	校验和
7字节	1字节	6字节	6字节	2字节	0-1500字节	0-46字节	4字节

先导字段各字节值为10101010,目的是使接收器与发送器的时钟同步;其后字节为10101011,标志着帧的开始;目的地址为接收端的物理(MAC)地址;源地址为发送端的物理(MAC)地址;数据长度字段(包括填充段)为46-1500字节,为了区别有效的短数据帧和残缺帧,IEEE802.3规定有效帧中从目的地址到校验和的最短长度为64字节;校验和可确定数据是否出错.帧格式字段的值标明帧数据的类型,若是0800(十六进制),说明是IP数据包;若是0806(十六进制),说明是RARP数据包,等等.通过判断帧格式字段的值可以提取出IP数据包,此时帧数据区的内容格式见表2.

表2 IP报文格式

版本(4bits)	头长(4bits)	服务类型(8bits)	总 长(16bits)	
标 识(16bits)			标志(3bits)	片偏移(13bits)
生存时间(8bits)		协议(8bits)	头校验和(16bits)	
源 IP 地 址 (32bits)				
目 的 IP 地 址 (32bits)				
选 项 或 数 据				

其中,协议字段的值标明了IP数据区的内容类型,若为6说明为TCP包,若为17说明为UDP包,若为1说明为ICMP包,若为2说明为IGMP包,等等.Http数据是通过TCP进行传输的,通过判断IP报头中协议字段的值可以提出TCP包,它的格式见表3.

表3 TCP报文格式

源端口(16bits)			目的端口(16bits)
序 列 号 (32bits)			
确 认 号 (32bits)			
头长(4bits)	保留(6bits)	标志(6bits)	窗 口(16bits)
校 验 和 (16bits)			紧急数据指针(16bits)
选 项 或 数 据			

因为Http服务的端口号是80,所以通过检查TCP报头中的端口号就可以知道是不是Http数据,若目的端口号为80,则说明是Http连接请求包,就可以采取一些相应的措施.

基于总线型以太网的介质访问控制技术,大多采用CSMA/CD(Carrier Sence Multiple Access/Collision Detection)——载波监听多路访问/冲突检测,基本原理可简述为

(1) 先听后说:PC机在发送数据前,先监听信道是否空闲,若空闲,则立即发送数据;

(2) 边听边说:即边发送数据边监听,这主要为了防止两台以上的PC机都发现信道空闲而同时发送数据,产生冲突;

(3) 冲突检测:若发送的数据在信道中产生冲突,则停止发送数据,等待信道空闲时重新发送.

2.3 网卡的工作原理

网卡的工作模式可分为

(1) 广播模式：即目的地址是 OXFFFFFF 的帧被称为广播帧，工作在广播模式的网卡接收广播帧.

(2) 多播传送(组内广播)模式：D 类 IP 地址是用于组内广播的，也就是一个人发出的包可以同时被其他多个有资格的人接收，这个人和那些有资格的人就形成了一个组，他们在组内的通信是广播式的.与此相对应，在物理层也存在着多播传送(或组内广播)，以多播传送地址作为目的物理地址的帧可以被组内的其他主机同时接收，而组外主机却接收不到.但是，如果将网卡设置为多播传送模式，它可以接收所有的多播传送帧，而不论它是不是组内成员.

(3) 直接模式：工作在直接模式下的网卡只接收目的地址是自己的地址的帧.

(4) 混杂模式：工作在混杂模式下的网卡接收所有的流过网卡的帧，监控程序就是在这种模式下运行的.

网卡的缺省工作模式包含广播模式和直接模式，即它只接收广播帧和发给自己的帧.

2.4 HUB 的工作原理

HUB 可分为共享 HUB 与交换 HUB，以共享 HUB 连接的以太网等网络是基于总线方式的，网络上数据的传输方式是广播形式的，即当某台 PC 机向另一台 PC 机发送数据时，共享 HUB 先将数据接收再广播发给网络中其余的 PC 机，因此在共享 HUB 下同一网络中所有 PC 机的网卡均能接收到数据，这也决定了在共享 HUB 下同一网络在同一时间只能有一对 PC 机进行数据传输.而交换 HUB 的内部单片程序能记住每台 PC 机的 MAC 地址，因此交换 HUB 可以根据目的 MAC 地址将数据发往目的 PC 机，这就决定了在交换 HUB 下，同一时间允许对不同的 PC 机间进行数据传输.

当 PC 机上的网卡收到网络中传输来的数据后，网卡内的单片程序先接收数据报的目的 MAC 地址，根据计算机上的网卡驱动程序设置的接收模式判断是否接收.如果该接收，就在接收后产生中断信号通知 CPU，CPU 得到中断信号后产生中断，操作系统就根据网卡的驱动程序设置的网卡中断程序地址调用驱动程序接收数据，放入信号堆栈让操作系统处理.如果不该接收则丢弃，所以不该接收的数据在网卡处就被截断，计算机根本不知道.

一般我们所讲的 Sniffer 程序就是把 NIC(网络适配卡，一般如以太网卡)设置为一种叫混杂模式(promiscuous)状态，一旦网卡设置为这种模式，它就能使 Sniffer 程序接收传输在网络上的每一个数据包(无论是在共享 HUB 还是交换 HUB 下).

基于混杂模式来获取数据，通过分析各种数据包，可以很清楚地描述出网络的结构和使用的机器，由于它接收同一网络中传输的任何一个数据包，所以 Sniffer 可以用来捕获密码、E-mail 信息、秘密文档等一些没有加密的信息，成为黑客常用的手段.

3 传输介质被监听的可能性

下面分析一些传输介质被监听的可能性：

(1) 以太网：监听的可能性比较高，因为以太网是一个广播型的网络.

(2) 令牌环网：监听的可能性也比较高.虽然令牌环网内并不是一个广播型网络，但实际上带有令牌的那些包在传输过程中，平均要经过网络上一半的计算机.但如果传输率很高，监听将变得困难.

(3) 有线电视信道：监听的可能性比较高.通过有线电视信道发送 IP 数据包时如果没有加密，可以被能访问到有线电视信道电缆的人截获.

(4) 微波：监听的可能性比较高.因为微波本身是一个广播型的传输媒介.

4 如何发现网络被 Sniffer

网络 sniffer 是很难被发现的,因为运行 sniffer 程序的主机在监听的过程中只是被动的接收在以太网中传输的信息,它不会跟其它的主机交换信息,也不能修改在网络中传输的信息包.因此网络 sniffer 的检测是非常困难的.

一是如果你怀疑某台机器正在运行 sniffer 程序,可以用正确的 IP 地址和错误的物理地址去 Ping 它,这样正在运行的 sniffer 程序就会做出响应.因为正常的机器一般不接收错误的物理地址的 Ping 信息,但正在监听的机器就可以接收,只要它的 IP Stack 不再次反向检查的话就会响应.由于这依赖于系统的 IP Stack,这种方法对很多系统是无效的.

二是向网上发大量不存在的物理地址的包,而监听程序往往就会将这些包进行处理,这样就会导致机器性能下降,可以通过 icmp echo delay 来比较和判断,也可以通过搜索网内所有主机上运行的程序,但这样做要耗费很大的工作量,而且还不能同时检查所有主机上的进程.但对管理员来说有很大的必要性,那就是可以确定是否有一个进程是从管理员机器上启动的.

5 阻止 sniffer 的措施

目前阻止 sniffer 的措施如下:

(1) 加密

一般情况下,黑客对用户的口令信息比较敏感,所以可以采用对用户信息和口令进行加密.目前有许多软件包可用于加密连接,从而使入侵者即使捕获到数据,但无法将数据解密而失去监听的意义.

现代网络中,SSH(Secure Shell)是一种在应用程序中提供保密通信的协议,它建立在客户/服务器模型上,SSH 所使用的端口是 22,连接是通过使用一种来自 RSA 的算法建立的,它排除了在不安全信道上通信的信息,授权结束后,所有的传输都用 IDEA 技术加密,通过 Sniffer 收集到的信息无法解密,sniffer 也就失去了意义.

(2) 安全的网络拓扑结构

一个网段必须有足够的理由才能信任另一个网段,网段应在考虑数据之间的信任关系上来设计,而不是硬件需要.这样,一个网络段仅由能相互信任的计算机组成,每台机器再通过硬连接线接到 HUB,HUB 再接到交换机上.随着交换机的成本和价格大幅下降,交换机已成为非常有效的使 sniffer 失效的设备.目前最常见的交换机在第三层(网络层)根据数据包目标地址进行转发,而不太采取集线器的广播方式,从而使 sniffer 失去了用武之地.由于网络分段了,数据包只能在这个网段上被 sniffe,其余的网段将不可能被 sniffe.

参 考 文 献

1 曾瑶辉等著.实用网络技术.北京:电子工业出版社,2000

2 顾尚杰等著.计算机通信网基础.北京:电子工业出版社,2000

3 谢希仁著.计算机网络.北京:电子工业出版社,1999

4 倪鹏云著.计算机网络系统结构分析.北京:国防工业出版社,2000

(下转第 31 页)

(上接第 26 页)

Taking precautions against sniffer

Shen Haijuan
(Hangzhou Vocational Technology Institute, Hangzhou 310015)

Abstract Sniffer is a network manage tool, and it is also used by hacker. This article states its mechanism and some methods for metwork protection.

Key words sniffer network management network safety hacker